

1 Introduced by Committee on Commerce and Economic Development

2 Date:

3 Subject: Commerce and trade; consumer protection; data brokers

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

6 An act relating to data brokers and consumer protection

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

8 Sec. 1. FINDINGS AND INTENT

9 (a) The General Assembly finds the following:

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

12 (A) While many different types of business collect data about  
13 consumers, a “data broker” is in the business of aggregating and selling data  
14 about consumers with whom the business does not have a direct relationship.

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

1           (C) Data brokers provide information that is critical to services  
2           offered in the modern economy, including: targeted marketing and sales;  
3           credit reporting; background checks; government information; risk mitigation  
4           and fraud detection; people search; decisions by banks, insurers, or others  
5           whether to provide services; ancestry research; and voter targeting and strategy  
6           by political campaigns.

7           (D) While data brokers offer many benefits, there are also risks  
8           associated with the widespread aggregation and sale of data about consumers,  
9           including risks related to consumers’ ability to know and control information  
10           held and sold about them and risks arising from the unauthorized or harmful  
11           acquisition and use of consumer information.

12           (E) There are important differences between “data brokers” and  
13           businesses with whom consumers have a direct relationship.

14           (i) Consumers who have a direct relationship with traditional and  
15           e-commerce businesses may have some level of knowledge about and control  
16           over the collection of data by those business, including: the choice to use the  
17           business’s products or services; the ability to review and consider data  
18           collection policies; the ability to opt out of certain data collection practices; the  
19           ability to identify and contact customer representatives; the ability to pursue  
20           contractual remedies through litigation; and the knowledge necessary to  
21           complain to law enforcement if other methods fail.

1           (ii) By contrast, consumers may not be aware that data brokers  
2 exist, who the companies are, or what information they collect, and may have  
3 little recourse to address grievances.

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

9           (G) To provide consumers with necessary information about data  
10 brokers, Vermont should adopt a narrowly tailored definition of “data broker”  
11 and require data brokers to register annually with the Secretary of State and  
12 provide information about their data collection activities, opt out policies,  
13 purchaser credentialing practices, and security breaches.

14           (2) Ensuring that data brokers have adequate security standards.

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

19           (B) While neither government nor industry can prevent every  
20 security breach, the State of Vermont has the authority and the duty to enact  
21 legislation 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           (3) Prohibiting the acquisition of personal information through  
19           fraudulent means or with the intent to commit wrongful acts.

20           (A) One of the significant dangers of the broad availability of  
21           sensitive personal information is that it can be used with malicious intent to

1 commit wrongful acts, such as stalking, harassment, fraud, discrimination, and  
2 identity theft.

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

6 (C) Vermont should create new causes of action to prohibit the  
7 acquisition of personal information through fraudulent means, or for the  
8 purpose of committing a wrongful act, to enable authorities and consumers to  
9 take action before harm occurs.

10 (4) Removing financial barriers to protect consumer credit information.

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

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

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

20 (D) In the aftermath of the breach, members of the General Assembly  
21 held hearings throughout the State to take testimony from Vermont consumers

1 concerned about the breach, gather information about their experiences, and  
2 disseminate guidance from the Vermont Attorney General and the Department  
3 of Financial Regulation on steps consumers should take to protect their  
4 identities and credit information.

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

8 (F) Under State law, when a consumer places a security freeze, the  
9 credit reporting agency issues a unique personal identification number or  
10 password to the consumer. The consumer must provide the PIN or password,  
11 and his or her express consent, to allow a potential creditor to access his or her  
12 credit information.

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

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

1        (b) Intent.

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

7            (A) adopting a narrowly tailored definition of “data broker” that:

8            (i) includes only those businesses that aggregate and sell the  
9        personal information of consumers with whom they do not have a direct  
10       relationship; and

11           (ii) excludes businesses that collect information from their own  
12       customers, employees, users, or donors, including: banks and other financial  
13       institutions; utilities; insurers; retailers and grocers; restaurants and hospitality  
14       businesses; social media websites and mobile “apps;” search websites; and  
15       businesses that provide services for consumer-facing businesses and  
16       maintain a direct relationship with those consumers, such as website, “app,”  
17       and e-commerce platforms; and

18           (B) requiring a data broker to register annually with the Secretary of  
19       State and **make certain disclosures in order to provide consumers and**  
20       **regulators with relevant information about its business practices.**

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

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

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

15           Sec. 2. 9 V.S.A. chapter 62 is amended to read:

16           CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

17                           Subchapter 1. General Provisions

18           § 2430. DEFINITIONS

19           ~~The following definitions shall apply throughout this chapter unless~~  
20           ~~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 does not include the State, a State agency, or any political subdivision of the  
8           State.

9           (2) “Consumer” means an individual residing in this State.

10           (3)(A) “Data broker” means a business that collects and licenses or sells  
11           to one or more third parties the personal information of a consumer with whom  
12           the business does not have a direct relationship.

13           (B) For purposes of this definition a consumer has a direct  
14           relationship with a business if the consumer is a past or present:

15           (i) customer, client, subscriber, or user of the business’s goods or  
16           services;

17           (ii) employee, contractor, or agent of the business; or

18           (iii) donor to the business.

19           (C) The term “data broker” does not include a vendor acting solely  
20           on behalf of the State, a State agency, or a political subdivision of the State.

1           (4)(A) “Data broker security breach” means an unauthorized acquisition  
2           or a reasonable belief of an unauthorized acquisition of **more than one element**  
3           of personal information maintained by a data broker when the personal  
4           information is not encrypted, redacted, or protected by another method that  
5           renders the information unreadable or unusable by an unauthorized person.

6           (B) “Data broker security breach” does not include good faith but  
7           unauthorized acquisition of personal information by an employee or agent of  
8           the data broker for a legitimate purpose of the data broker, provided that the  
9           personal information is not used for a purpose unrelated to the data broker’s  
10           business or subject to further unauthorized disclosure.

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

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

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

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

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

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

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

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

19                    (i) Social Security number;

20                    (ii) motor vehicle operator’s license number or nondriver  
21 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 digital  
10 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,  
8 ~~electronic data~~ or a reasonable belief of an unauthorized acquisition of,  
9 ~~electronic data that compromises the security, confidentiality, or integrity of a~~  
10 ~~consumer’s~~ personally identifiable information maintained by ~~the~~ a data  
11 collector.

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

17           (C) In determining whether personally identifiable information has  
18 been acquired or is reasonably believed to have been acquired by a person  
19 without valid authorization, a data collector may consider the following  
20 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.

12 (1) A person shall not acquire personal information through fraudulent  
13 means.

14 (2) A person shall not acquire or use personal information for the  
15 purpose of:

16 (A) stalking or harassing another person;

17 (B) committing a fraud, including identity theft, financial fraud, or e-  
18 mail fraud; or

19 (C) engaging in unlawful discrimination, including employment  
20 discrimination and housing discrimination.

1 (b) Enforcement.

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

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

8 Subchapter 2. Security Breach Notice Act

9 § 2435. NOTICE OF SECURITY BREACHES

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

11 (b) Notice of breach.

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

17 ~~(B) Notice~~ A data collector shall provide notice of the security breach  
18 ~~shall be made~~ to consumers pursuant to subdivision (1)(A) of this subsection  
19 (b) in the most expedient time possible and without unreasonable delay, but not  
20 later than 45 days after the discovery or notification, consistent with the  
21 legitimate needs of the law enforcement agency, as provided in subdivisions

1 ~~(3) and (4) of this subsection (b), or with any~~ measures necessary to determine  
2 the scope of the security breach and restore the reasonable integrity, security,  
3 and confidentiality of the data system, but not later than 45 days after the  
4 discovery or notification of the breach, unless a law enforcement agency, as  
5 provided in subdivisions (3) and requests a delay pursuant to subdivision (4) of  
6 this subsection (b).

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

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

19 (A) A data collector ~~or other entity~~ regulated by the Department of  
20 Financial Regulation under Title 8 or this title shall provide notice of a breach



1 to the Department. All other data collectors or ~~other entities subject to this~~  
2 ~~subchapter~~ shall provide notice of a breach to the Attorney General.

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

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

20 (iii) If the date of the security breach is unknown at the time notice  
21 is sent to the Attorney General or to the Department, the data collector shall

1 send the Attorney General or the Department the date of the breach as soon as  
2 it is known.

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

11 (C)(i) When the data collector provides notice of the security breach  
12 to consumers pursuant to subdivision (1) of this subsection (b), the data  
13 collector shall notify the Attorney General or the Department, as applicable, of  
14 the number of Vermont consumers affected, if known to the data collector, and  
15 shall provide a copy of the notice provided to consumers under subdivision (1)  
16 of this 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           (4)(A)(i) The notice to a consumer required by this subsection shall be  
2 delayed upon request of a law enforcement agency.

3           (ii) A law enforcement agency may request the delay if it believes  
4 that notification may impede a law enforcement investigation, or a national or  
5 Homeland Security investigation, or jeopardize public safety or national or  
6 Homeland Security interests.

7           (iii) ~~In the event~~ If law enforcement ~~makes the request for requests~~  
8 a delay in a manner other than in writing, the data collector shall document  
9 ~~such~~ the request contemporaneously in writing, including the name of the law  
10 enforcement officer making the request and the officer's law enforcement  
11 agency engaged in the investigation.

12           (iv) A law enforcement agency shall promptly notify the data  
13 collector in writing when the law enforcement agency no longer believes that  
14 notification may impede a law enforcement investigation, or a national or  
15 Homeland Security investigation, or jeopardize public safety or national or  
16 Homeland Security interests.

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

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

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

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

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

16           (A) the incident in general terms;

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

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

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

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

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

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

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

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

10           (ii) electronic notice, for those consumers for whom the data  
11 collector has a valid e-mail address if:

12           (I) the data collector's primary method of communication with  
13 the consumer is by electronic means, the electronic notice does not request or  
14 contain a hypertext link to a request that the consumer provide personal  
15 information, and the electronic notice conspicuously warns consumers not to  
16 provide personal information in response to electronic communications  
17 regarding security breaches; or

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

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

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

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

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

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

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

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

11 (II) notifying major statewide and regional media.

12 (c) ~~In the event~~ If a data collector provides notice to more than 1,000  
13 consumers at one time pursuant to this section, the data collector shall notify,  
14 without unreasonable delay, all consumer reporting agencies that compile and  
15 maintain files on consumers on a nationwide basis, as defined in 15 U.S.C.  
16 § 1681a(p), of the timing, distribution, and content of the notice. This  
17 subsection shall not apply to a person who is licensed or registered under Title  
18 8 by the Department of Financial Regulation.

19 (d)(1)(A) Notice of a security breach pursuant to subsection (b) of this  
20 section is not required if the data collector establishes that misuse of ~~personal~~  
21 personally identifiable information is not reasonably possible and the data

1 collector provides notice of ~~the~~ its determination ~~that the misuse of the~~  
2 ~~personal information is not reasonably possible~~ pursuant to the requirements of  
3 this subsection (d).

4 (B)(i) If the data collector establishes that misuse of the ~~personal~~  
5 personally identifiable information is not reasonably possible, the data  
6 collector shall provide notice of its determination ~~that misuse of the personal~~  
7 ~~information is not reasonably possible~~ and a detailed explanation for said  
8 ~~determination~~ to the Vermont Attorney General or to the Department of  
9 Financial Regulation, ~~in the event that the data collector is a person or entity~~  
10 ~~licensed or registered with the Department under Title 8 or this title~~ as  
11 applicable.

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

16 (2) If a data collector established that misuse of ~~personal information~~  
17 personally identifiable information was not reasonably possible under  
18 subdivision (1) of this subsection (d) and subsequently obtains facts indicating  
19 that misuse of the ~~personal information~~ personally identifiable information has  
20 occurred or is occurring, the data collector shall provide notice of the security  
21 breach pursuant to subsection (b) of this section.

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

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

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

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

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



1 (g) Enforcement.

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

13 (2) With respect to a data collector that is a person or entity licensed or  
14 registered with the Department of Financial Regulation under Title 8 or this  
15 title, the Department of Financial Regulation shall have the full authority to  
16 investigate potential violations of this subchapter and to prosecute, obtain, and  
17 impose remedies for a violation of this subchapter or any rules or regulations  
18 adopted pursuant to this subchapter, as the Department has under Title 8 or this  
19 title or any other applicable law or regulation.

20 Subchapter 3. Social Security Number Protection Act

21 § 2440. SOCIAL SECURITY NUMBER PROTECTION

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21

\* \* \*

(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

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

11 \* \* \*

12 Subchapter 4. Document Safe Destruction Act

13 § 2445. SAFE DESTRUCTION OF DOCUMENTS CONTAINING

14 ~~PERSONAL~~ CONFIDENTIAL INFORMATION

15 (a) As used in this section:

16 (1) “Business” ~~means sole proprietorship, partnership, corporation,~~  
17 ~~association, limited liability company, or other group, however organized and~~  
18 ~~whether or not organized to operate at a profit, including a financial institution~~  
19 ~~organized, chartered, or holding a license or authorization certificate under the~~  
20 ~~laws of this State, any other state, the United States, or any other country, or~~  
21 ~~the parent, affiliate, or subsidiary of a financial institution, but in no case shall~~

1 ~~it include the State, a State agency, or any political subdivision of the State.~~

2 ~~The term~~ has the same meaning as in section 2430 of this title, and includes an  
3 entity that destroys records.

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

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

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

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

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

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

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

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

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

1 \* \* \*

2 Subchapter 5. Data Brokers

3 § 2446. ANNUAL REGISTRATION

4 (a) Annually, on or before January 31 following a year in which a person  
5 meets the definition of data broker as provided in section 2430 of this title, a  
6 data broker shall:

7 (1) register with the Secretary of State;

8 (2) pay a registration fee of \$100.00; and

9 (3) provide the following information:

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

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

15 (i) the method for requesting an opt out;

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

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

20 (C) a statement specifying the data collection, databases, or sales  
21 activities from which a consumer may not opt out;

1           (D) a statement whether the data broker implements a purchaser  
2           credentialing process;

3           (E) the number of data broker security breaches that the data broker  
4           has experienced during the prior year, and if known, the total number of  
5           consumers affected by the breaches;

6           (F) where the data broker has actual knowledge that it possesses the  
7           personal information of minors, a separate statement detailing the data  
8           collection practices, databases, sales activities, and opt out policies that are  
9           applicable to the personal information of minors; and

10           (G) any additional information or explanation the data broker  
11           chooses to provide concerning its data collection practices.

12           (b) A data broker that fails to register pursuant to subsection (a) of this  
13           section is liable to the State for:

14           (1) a civil penalty of \$50.00 for each day, not to exceed a total of  
15           \$10,000.00 for each year, it transacts business in this State without registering  
16           pursuant to this section;

17           (2) an amount equal to the fees due under this section during the period it  
18           transacted business in this State without registering; and

19           (3) other penalties imposed by law.

20           (c) The Attorney General may maintain an action in the Civil Division of  
21           the Superior Court to collect the penalties imposed in this section and to

1 restrain a data broker not in compliance with this chapter from doing business  
2 within this State.

3 § 2447. DATA BROKER DUTY TO PROTECT PERSONAL

4 INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS

5 (a) Duty to protect personally identifiable information.

6 (1) A data broker shall develop, implement, and maintain a  
7 comprehensive information security program that is written in one or more  
8 readily accessible parts and contains administrative, technical, and physical  
9 safeguards that are appropriate to:

10 (A) the size, scope, and type of business of the data broker obligated  
11 to safeguard the personally identifiable information under such comprehensive  
12 information security program;

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

14 (C) the amount of stored data; and

15 (D) the need for security and confidentiality of personally identifiable  
16 information.

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



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

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

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

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

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

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

13            (3) security policies for employees relating to the storage, access, and  
14        transportation of records containing personally identifiable information outside  
15        business premises;

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

18            (5) measures that prevent terminated employees from accessing records  
19        containing personally identifiable information;

20            (6) supervision of service providers, by:

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

4           (B) requiring third-party service providers by contract to implement  
5           and maintain appropriate security measures for personally identifiable  
6           information;

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

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

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

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

16           (A) at least annually; or

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

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

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

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

7           (1) secure user authentication protocols, as follows:

8           (A) an authentication protocol that has the following features:

9           (i) control of user IDs and other identifiers;

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

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

16           (iv) restricting access to only active users and active user  
17           accounts; and

18           (v) blocking access to user identification after multiple  
19           unsuccessful attempts to gain access; or

20           (B) an authentication protocol that provides a higher level of security  
21           than the features specified in subdivision (1)(A) of this subsection (c).

1           (2) secure access control measures that:

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

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

9                   (3) encryption of all transmitted records and files containing personally  
10 identifiable information that will travel across public networks and encryption  
11 of all data containing personally identifiable information to be transmitted  
12 wirelessly or a protocol that provides a higher degree of security;

13                   (4) reasonable monitoring of systems for unauthorized use of or access  
14 to personally identifiable information;

15                   (5) encryption of all personally identifiable information stored on  
16 laptops or other portable devices or a protocol that provides a higher degree of  
17 security;

18                   (6) for files containing personally identifiable information on a system  
19 that is connected to the Internet, reasonably up-to-date firewall protection and  
20 operating system security patches that are reasonably designed to maintain the

1 integrity of the personally identifiable information or a protocol that provides a  
2 higher degree of security;

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

9 (8) education and training of employees on the proper use of the  
10 computer security system and the importance of personally identifiable  
11 information security.

12 (d) Enforcement.

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

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

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

20 § 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

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

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

21 “NOTICE TO VERMONT CONSUMERS

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

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

10                   (A) in response to a court order;

11                   (B) for direct mail offers of credit;

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

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

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

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

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

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

#### 8           Vermont Consumers Have the Right to Obtain a Security Freeze

9           You have a right to place a “security freeze” on your credit report pursuant  
10 to 9 V.S.A. § 2480h at no charge ~~if you are a victim of identity theft. All other~~  
11 ~~Vermont consumers will pay a fee to the credit reporting agency of up to~~  
12 ~~\$10.00 to place the freeze on their credit report.~~ The security freeze will  
13 prohibit a credit reporting agency from releasing any information in your credit  
14 report without your express authorization. A security freeze must be requested  
15 in writing by certified mail.

16           The security freeze is designed to help prevent credit, loans, and services  
17 from being approved in your name without your consent. However, you  
18 should be aware that using a security freeze to take control over who gains  
19 access to the personal and financial information in your credit report may  
20 delay, interfere with, or prohibit the timely approval of any subsequent request  
21 or application you make regarding new loans, credit, mortgage, insurance,



1 government services or payments, rental housing, employment, investment,  
2 license, cellular phone, utilities, digital signature, ~~internet~~ Internet credit card  
3 transaction, or other services, including an extension of credit at point of sale.

4 When you place a security freeze on your credit report, within ten business  
5 days you will be provided a personal identification number, ~~or~~ password, or  
6 other equally or more secure method of authentication to use if you choose to  
7 remove the freeze on your credit report or authorize the release of your credit  
8 report for a specific party, parties, or period of time after the freeze is in place.

9 To provide that authorization, you must contact the credit reporting agency and  
10 provide all of the following:

11 (1) The unique personal identification number, ~~or~~ password, or other  
12 method of authentication provided by the credit reporting agency.

13 (2) Proper identification to verify your identity.

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

17 A credit reporting agency may not charge a fee ~~of up to \$5.00 to a consumer~~  
18 ~~who is not a victim of identity theft~~ to remove the freeze on your credit report  
19 or authorize the release of your credit report for a specific party, parties, or  
20 period of time after the freeze is in place. ~~For a victim of identity theft, there is~~  
21 ~~no charge when the victim submits a copy of a police report, investigative~~

1 ~~report, or complaint filed with a law enforcement agency about unlawful use of~~  
2 ~~the victim's personal information by another person.~~

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

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

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

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

20 (d) The information required to be disclosed by this section shall be  
21 disclosed in writing. The information required to be disclosed pursuant to

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

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

11 Sec. 4. 9 V.S.A. § 2480h is amended to read:

12 § 2480h. SECURITY FREEZE BY CREDIT REPORTING AGENCY; TIME  
13 IN EFFECT

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

20 (2) A consumer ~~who has been the victim of identity theft~~ may place a  
21 security freeze on his or her credit report by making a request in writing by

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

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

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

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

19 (c) The credit reporting agency shall send a written confirmation of the  
20 security freeze to the consumer within 10 business days and shall provide the  
21 consumer with a unique personal identification number or password, other than

1 the customer's Social Security number, or another method of authentication  
2 that is equally or more secure than a PIN or password, to be used by the  
3 consumer when providing authorization for the release of his or her credit for a  
4 specific party, parties, or period of time.

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

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

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

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

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

19 (f) A credit reporting agency that receives a request from a consumer to lift  
20 temporarily a freeze on a credit report pursuant to subsection (d) of this section

1 shall comply with the request ~~no~~ not later than three business days after  
2 receiving the request.

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

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

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

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

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

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

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

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

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

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

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

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

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

5           (4) The Office of Child Support when investigating a child support case  
6 pursuant to Title IV-D of the Social Security Act (42 U.S.C. et seq.) and  
7 33 V.S.A. § 4102.

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

11           (6) The Department of Taxes, municipal taxing authorities, or the  
12 Department of Motor Vehicles<sub>2</sub> or any of their agents or assignees, acting to  
13 investigate or collect delinquent taxes or assessments, including interest and  
14 penalties, unpaid court orders, or acting to fulfill any of their other statutory or  
15 charter responsibilities.

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

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

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



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

3           Sec. 5. REPORTS

4           (a) On or before March 1, 2019, the Attorney General, the Department of  
5           Financial Regulation, and Secretary of State shall submit a preliminary report  
6           concerning the implementation of this act to the House Committee on  
7           Commerce and Economic Development and the Senate Committee on  
8           Economic Development, Housing and General Affairs.

9           (b) On or before January 15, 2020, the Attorney General, the Department  
10          of Financial Regulation, and Secretary of State shall update its preliminary  
11          report and provide additional information concerning the implementation of  
12          this act to the House Committee on Commerce and Economic Development  
13          and the Senate Committee on Economic Development, Housing and General  
14          Affairs.

15          Sec. 6. EFFECTIVE DATES

16          (a) This section, Sec. 1 (Findings and Intent), Secs. 3–4 (eliminating fees  
17          for placing or removing a credit freeze), and Sec. 5 (Reports) shall take effect  
18          on passage.

19          (b) Sec 2 (amending 9 V.S.A. chapter 62) shall take effect on July 1, 2018,  
20          except that 9 V.S.A. § 2447 (data broker information security program) shall  
21          take effect on January 1, 2019.