

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

H.764

Introduced by Committee on Commerce and Economic Development

Date:

Subject: Commerce and trade; consumer protection; data brokers

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

An act relating to data brokers and consumer protection

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

~~Sec. 1. FINDINGS AND INTENT~~

~~(a) The General Assembly finds the following:~~

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

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

~~(B) A data broker collects many hundreds or thousands of data points
about consumers from multiple sources, including: Internet browsing history;
online purchases; public records; location data; loyalty programs; and
subscription information. The data broker then scrubs the data to ensure~~

1 ~~accuracy; analyzes the data to assess content; and packages the data for sale to~~
2 ~~a third party.~~

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

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

14 (E) There are important differences between "data brokers" and
15 businesses with whom consumers have a direct relationship.

16 (i) Consumers who have a direct relationship with traditional and
17 e-commerce businesses may have some level of knowledge about and control
18 over the collection of data by those business, including: the choice to use the
19 business's products or services; the ability to review and consider data
20 collection policies; the ability to opt out of certain data collection practices, the
21 ability to identify and contact customer representatives, the ability to pursue

1 contractual remedies through litigation; and the knowledge necessary to
2 complain to law enforcement.

3 (ii) By contrast, consumers may not be aware that data brokers
4 exist, who the companies are, or what information they collect, and may not be
5 aware of available recourse.

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

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

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

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

21 (B) While neither government nor industry can prevent every

1 ~~security breach, the State of Vermont has the authority and the duty to enact~~
2 ~~legislation to protect its consumers where possible.~~

3 ~~(C) One approach to protecting consumer data has been to require~~
4 ~~government agencies and certain regulated businesses to adopt an “information~~
5 ~~security program” that has “appropriate administrative, technical, and physical~~
6 ~~safeguards to ensure the security and confidentiality of records” and “to~~
7 ~~protect against any anticipated threats or hazards to their security or integrity~~
8 ~~which could result in substantial harm.” *Federal Privacy Act*, 5 U.S.C. §~~
9 ~~552a.~~

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

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

21 ~~(S) Prohibiting the acquisition of personal information through~~

1 ~~fraudulent means or with the intent to commit wrongful acts.~~

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

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

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

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

13 (A) In one of several major security breaches that have occurred in
14 recent years, the names, Social Security numbers, birth dates, addresses,
15 driver's license numbers, and credit card numbers of over 145 million
16 Americans were exposed, including over 247,000 Vermonters.

17 (B) In response to concerns about data security, identity theft, and
18 consumer protection, the Vermont Attorney General and the Department of
19 Financial Regulation have outlined steps a consumer should take to protect his
20 or her identity and credit information. One important step a consumer can take
21 is to place a security freeze on his or her credit file with each of the national

1 credit reporting agencies.

2 (C) Under State law, when a consumer places a security freeze, a
3 credit reporting agency issues a unique personal identification number or
4 password to the consumer. The consumer must provide the PIN or password,
5 and his or her express consent, to allow a potential creditor to access his or her
6 credit information.

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

10 (E) Vermont should exercise its authority to prohibit these fees to
11 eliminate any financial barrier to placing or removing a security freeze.

12 (b) Intent.

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

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

19 (i) includes only those businesses that aggregate and sell the
20 personal information of consumers with whom they do not have a direct
21 relationship, and

1 ~~(ii) excludes businesses that collect information from their own~~
2 ~~customers, employees, users, or donors, including: banks and other financial~~
3 ~~institutions; utilities; insurers; retailers and grocers; restaurants and hospitality~~
4 ~~businesses; social media websites and mobile “apps”; search websites; and~~
5 ~~businesses that provide services for consumer-facing businesses and~~
6 ~~maintain a direct relationship with those consumers, such as website, “app,”~~
7 ~~and e-commerce platforms; and~~

8 (B) requiring a data broker to register annually with the Secretary of
9 State and make certain disclosures in order to provide consumers, policy
10 makers, and regulators with relevant information.

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

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

20 (4) Removing financial barriers to protect consumer credit information.
21 It is the intent of the General Assembly to remove any financial barrier for

1 ~~Vermonters who wish to place a security freeze on their credit report by~~
2 ~~prohibiting credit reporting agencies from charging a fee to place or remove a~~
3 ~~freeze.~~

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

5 CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

6 Subchapter 1. General Provisions

7 § 2430. DEFINITIONS

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

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

18 (2) "Consumer" means an individual residing in this State.

19 (3)(A) "Data broker" means a business that collects and licenses or sells
20 to one or more third parties the personal information of a consumer with
21 whom the business does not have a direct relationship.

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

3 (i) customer, client, subscriber, or user of the business's goods or
4 services;

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

6 (iii) donor to the business.

7 (C) The term "data broker" does not include a vendor acting solely
8 on behalf of the State, a State agency, or a political subdivision of the State.

9 (4)(A) "Data broker security breach" means an unauthorized acquisition
10 or a reasonable belief of an unauthorized acquisition of more than one element
11 of personal information maintained by a data broker when the personal
12 information is not encrypted, redacted, or protected by another method that
13 renders the information unreadable or unusable by an unauthorized person.

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

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

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

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

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

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

10 ~~(3)(5) "Data collector" may include the State, State agencies, political~~
11 ~~subdivisions of the State, public and private universities, privately and publicly~~
12 ~~held corporations, limited liability companies, financial institutions, retail~~
13 ~~operators, and any other entity that, means a person who, for any purpose,~~
14 ~~whether by automated collection or otherwise, handles, collects, disseminates,~~
15 ~~or otherwise deals with nonpublic personal information personally identifiable~~
16 ~~information, and includes the State, State agencies, political subdivisions of~~
17 ~~the State, public and private universities, privately and publicly held~~
18 ~~corporations, limited liability companies, financial institutions, and retail~~
19 ~~operators.~~

20 ~~(4)(6) "Encryption" means use of an algorithmic process to transform~~
21 ~~data into a form in which the data is rendered unreadable or unusable without~~

1 ~~use of a confidential process or key~~

2 ~~(5)(7)(A) "Personally identifiable information" means an individual's a~~
3 ~~consumer's first name or first initial and last name in combination with any~~
4 ~~one or more of the following digital data elements, when either the name or~~
5 ~~the data elements are not encrypted or redacted or protected by another method~~
6 ~~that renders them unreadable or unusable by unauthorized persons:~~

7 ~~(i) Social Security number;~~

8 ~~(ii) motor vehicle operator's license number or nondriver~~
9 ~~identification card number;~~

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

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

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

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

20 ~~(A) name;~~

21 ~~(B) address,~~

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

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

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

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

10 ~~(6)(9) "Records Record" means any material on which written, drawn,~~
11 ~~spoken, visual, or electromagnetic information is recorded or preserved,~~
12 ~~regardless of physical form or characteristics.~~

13 ~~(7)(10) "Redaction" means the rendering of data so that it is the data are~~
14 ~~unreadable or is are truncated so that no more than the last four digits of the~~
15 ~~identification number are accessible as part of the data.~~

16 ~~(8)(11)(A) "Security breach" means unauthorized acquisition of,~~
17 ~~electronic data or a reasonable belief of an unauthorized acquisition of,~~
18 ~~electronic data that compromises the security, confidentiality, or integrity of a~~
19 ~~consumer's personally identifiable information maintained by the a data~~
20 ~~collector.~~

21 ~~(B) "Security breach" does not include good faith but unauthorized~~

1 ~~acquisition of personally identifiable information by an employee or agent of~~
2 the data collector for a legitimate purpose of the data collector, provided that
3 the personally identifiable information is not used for a purpose unrelated to
4 the data collector's business or subject to further unauthorized disclosure.

5 (C) In determining whether personally identifiable information has
6 been acquired or is reasonably believed to have been acquired by a person
7 without valid authorization, a data collector may consider the following
8 factors, among others:

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

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

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

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

18 § 2433. ACQUISITION OF PERSONAL INFORMATION; PROHIBITIONS

19 (a) Prohibited acquisition and use.

20 (1) A person shall not acquire personal information through fraudulent

21 means.

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

3 (A) stalking or harassing another person;

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

6 (C) engaging in unlawful discrimination, including employment
7 discrimination and housing discrimination.

8 (b) 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 section and to conduct civil investigations,
13 enter into assurances of discontinuance, bring civil actions, and take other
14 enforcement actions as provided under chapter 63, subchapter 1 of this title.

15 Subchapter 2. Security Breach Notice Act

16 § 2435. NOTICE OF SECURITY BREACHES

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

18 (b) Notice of breach.

19 (1)(A) Except as set forth in subsection (d) of this section, ~~any a~~ data
20 collector that owns or licenses ~~computerized~~ personally identifiable

21 ~~information that includes personal information concerning a consumer shall~~

1 ~~notify the consumer that there has been of a security breach following~~

2 ~~discovery or notification to the data collector of the breach.~~

3 ~~(B) Notice A data collector shall provide notice of the security~~

4 ~~breach shall be made to consumers pursuant to subdivision (A) of this~~

5 ~~subdivision (b)(1) in the most expedient time possible and without~~

6 ~~unreasonable delay, but not later than 45 days after the discovery or~~

7 ~~notification, consistent with the legitimate needs of the law enforcement~~

8 ~~agency, as provided in subdivisions (3) and (4) of this subsection (b), or with~~

9 ~~any measures necessary to determine the scope of the security breach and~~

10 ~~restore the reasonable integrity, security, and confidentiality of the data system,~~

11 ~~but not later than 45 days after the discovery or notification of the breach,~~

12 ~~unless a law enforcement agency, as provided in subdivisions (3) and requests~~

13 ~~a delay pursuant to subdivision (4) of this subsection (b).~~

14 ~~(2) Any A data collector that maintains or possesses computerized data~~

15 ~~containing personally identifiable information of a consumer that the data~~

16 ~~collector does not own or license, or any a data collector that acts or conducts~~

17 ~~business in Vermont that maintains or possesses records or data containing~~

18 ~~personally identifiable information that the data collector does not own or~~

19 ~~license, shall notify the owner or licensee of the information of any security~~

20 ~~breach immediately following discovery of the breach, consistent with the~~

21 ~~legitimate needs of law enforcement as provided in subdivisions (3) and~~

1 ~~subdivision (4) of this subsection (b)~~

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

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

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

17 (ii) Notwithstanding subdivision ~~(B)~~(i) of this subdivision
18 (b)(3)(B), a data collector ~~who~~ that, prior to the date of the security breach, on
19 a form and in a manner prescribed by the Attorney General, had sworn in
20 writing to the Attorney General that it maintains written policies and
21 ~~procedures to maintain the security of personally identifiable information and~~

1 ~~respond to a breach in a manner consistent with Vermont law shall notify the~~
2 Attorney General of the date of the security breach and the date of discovery
3 of the breach and shall provide a description of the breach prior to providing
4 notice of the breach to consumers pursuant to subdivision (1) of this subsection
5 (b).

6 (iii) If the date of the security breach is unknown at the time
7 notice is sent to the Attorney General or to the Department, the data collector
8 shall send the Attorney General or the Department the date of the breach as
9 soon as it is known.

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

18 (C)(i) When the data collector provides notice of the security breach
19 to consumers pursuant to subdivision (1) of this subsection (b), the data
20 collector shall notify the Attorney General or the Department, as applicable, of
21 ~~the number of Vermont consumers affected, if known to the data collector, and~~

1 ~~shall provide a copy of the notice provided to consumers under subdivision (1)~~
2 ~~of this subsection (b).~~

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

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

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

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

19 (iv) A law enforcement agency shall promptly notify the data
20 collector in writing when the law enforcement agency no longer believes that
21 ~~notification may impede a law enforcement investigation, or a national or~~

1 ~~Homeland Security investigation, or jeopardize public safety or national or~~
2 ~~Homeland Security interests.~~

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

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

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

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

19 (5) The notice to a consumer shall be clear and conspicuous. The notice
20 shall include a description of each of the following, if known to the data
21 collector.

1 (A) the incident in general terms;

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

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

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

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

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

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

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

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

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

17 (I) the data collector's primary method of communication with
18 the consumer is by electronic means, the electronic notice does not request or
19 contain a hypertext link to a request that the consumer provide personal
20 information, and the electronic notice conspicuously warns consumers not to
21 provide personal information in response to electronic communications

1 regarding security breaches; or

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

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

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

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

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

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

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

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

16 (II) notifying major statewide and regional media.

17 (c) ~~In the event~~ If a data collector provides notice to more than 1,000
18 consumers at one time pursuant to this section, the data collector shall notify,
19 without unreasonable delay, all consumer reporting agencies that compile and
20 maintain files on consumers on a nationwide basis, as defined in 15 U.S.C.

21 § 1681a(p), of the timing, distribution, and content of the notice. This

1 ~~subsection shall not apply to a person who is licensed or registered under Title~~
2 ~~8 by the Department of Financial Regulation.~~

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

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

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

21 ~~(2) If a data collector established that misuse of personal information~~

1 ~~personally identifiable information was not reasonably possible under~~
2 subdivision (1) of this subsection (d) and subsequently obtains facts indicating
3 that misuse of the personal information personally identifiable information has
4 occurred or is occurring, the data collector shall provide notice of the security
5 breach pursuant to subsection (b) of this section.

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

8 (f) Except as provided in subdivision (3) of this subsection (~~¶~~), a financial
9 institution that is subject to the following guidances, and any revisions,
10 additions, or substitutions relating to an interagency guidance₂ shall be exempt
11 from this section:

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

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

20 (3) A financial institution regulated by the Department of Financial
21 ~~regulation that is subject to subdivision (1) or (2) of this subsection (~~¶~~) shall~~

1 ~~notify the Department as soon as possible after it becomes aware of an incident~~
2 ~~involving unauthorized access to or use of personally identifiable information~~
3 ~~a security breach.~~

4 (g) Enforcement.

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

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

1 title or any other applicable law or regulation

2 Subchapter 3. Social Security Number Protection Act

3 § 2440. SOCIAL SECURITY NUMBER PROTECTION

4 * * *

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

1 ~~license number, State identification number, passport number, checking~~
2 account number, savings account number, credit card number, or debit card
3 number, or personal identification number (PIN) code or passwords to be
4 redacted. The request for redaction shall be considered a public record with
5 access restricted to the town clerk, the clerk of court, their staff, or upon order
6 of the court. The town clerk or clerk of court shall have no duty to inquire
7 beyond the written request to verify the identity of a person requesting
8 redaction and shall have no duty to remove redaction for any reason upon
9 subsequent request by an individual or by order of the court, if impossible to
10 do so. No fee will be charged for the redaction pursuant to such request. Any
11 person who requests a redaction without proper authority to do so shall be
12 guilty of an infraction, punishable by a fine not to exceed \$500.00 for each
13 violation.

14 * * *

15 Subchapter 4. Document Safe Destruction Act

16 § 2445. SAFE DESTRUCTION OF DOCUMENTS CONTAINING
17 PERSONAL CONFIDENTIAL INFORMATION

18 (a) As used in this section:

19 (1) "Business" ~~means sole proprietorship, partnership, corporation,~~
20 ~~association, limited liability company, or other group, however organized and~~
21 ~~whether or not organized to operate at a profit, including a financial institution~~

1 ~~organized, chartered, or holding a license or authorization certificate under the~~
2 ~~laws of this State, any other state, the United States, or any other country, or~~
3 ~~the parent, affiliate, or subsidiary of a financial institution, but in no case shall~~
4 ~~it include the State, a State agency, or any political subdivision of the State.~~

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

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

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

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

21 ~~(B) "Record" does not include publicly available directories~~

1 ~~containing information an individual has voluntarily consented to have~~

2 ~~publicly disseminated or listed, such as name, address, or telephone number.~~

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

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

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

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

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

1 ~~confidential information during or after the collection and transportation and~~
2 ~~disposing of such information.~~

3 * * *

4 Subchapter 5. Data Brokers

5 § 2446. ANNUAL REGISTRATION

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

9 (1) register with the Secretary of State;

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

11 (3) provide the following information:

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

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

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

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

20 (iii) whether the data broker permits a consumer to authorize a
21 third party to perform the opt out on the consumer's behalf,

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

3 ~~(D) a statement whether the data broker implements a purchaser~~
4 ~~credentialing process;~~

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

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

12 ~~(G) any additional information or explanation the data broker~~
13 ~~chooses to provide concerning its data collection practices.~~

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

16 ~~(1) a civil penalty of \$50.00 for each day, not to exceed a total of~~
17 ~~\$10,000.00 for each year, it fails to register pursuant to this section;~~

18 ~~(2) an amount equal to the fees due under this section during the period~~
19 ~~it failed to register pursuant to this section; and~~

20 ~~(3) other penalties imposed by law.~~

21 ~~(c) The Attorney General may maintain an action in the Civil Division of~~

1 ~~the Superior Court to collect the penalties imposed in this section and to seek~~
2 appropriate injunctive relief.

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
16 identifiable 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:~~

21 ~~(A) taking reasonable steps to select and retain third-party service~~

1 providers that are capable of maintaining appropriate security measures to
2 protect personally identifiable information consistent with applicable law; and

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

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

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

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

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

15 (A) at least annually; or

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

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

21 (B) mandatory post-incident review of events and actions taken, if

1 ~~any to make changes in business practices relating to protection of personally~~
2 ~~identifiable information.~~

3 ~~(c) Information security program; computer system security requirements.~~

4 ~~A comprehensive information security program required by this section shall~~
5 ~~at minimum, and to the extent technically feasible, have the following~~
6 ~~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 (A) of this subdivision (C)(1).~~

- 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
21 integrity of the personally identifiable information or a protocol that provides a

1 higher degree of security:

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

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

11 (d) Enforcement.

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

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

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

19 § 2480b. DISCLOSURES TO CONSUMERS

20 (a) A credit reporting agency shall, upon request and proper identification
21 of any consumer, clearly and accurately disclose to the consumer all

1 information available to users at the time of the request pertaining to the

2 consumer, including:

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

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

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

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

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

19 "NOTICE TO VERMONT CONSUMERS

20 (1) Under Vermont law, you are allowed to receive one free copy of
21 your credit report every 12 months from each credit reporting agency. If you

1 would like to obtain your free credit report from [INSERT NAME OF
2 COMPANY], you should contact us by [[writing to the following address:
3 [INSERT ADDRESS FOR OBTAINING FREE CREDIT REPORT]] or
4 [calling the following number: [INSERT TELEPHONE NUMBER FOR
5 OBTAINING FREE CREDIT REPORT]],² or both].

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

8 (A) in response to a court order;

9 (B) for direct mail offers of credit;

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

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

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

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

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

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

5 Vermont Consumers Have the Right to Obtain a Security Freeze

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

13 The security freeze is designed to help prevent credit, loans, and services
14 from being approved in your name without your consent. However, you
15 should be aware that using a security freeze to take control over who gains
16 access to the personal and financial information in your credit report may
17 delay, interfere with, or prohibit the timely approval of any subsequent request
18 or application you make regarding new loans, credit, mortgage, insurance,
19 government services or payments, rental housing, employment, investment,
20 license, cellular phone, utilities, digital signature, ~~internet~~ Internet credit card
21 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, or~~
3 ~~other equally or more secure method of authentication to use if you choose to~~
4 ~~remove the freeze on your credit report or authorize the release of your credit~~
5 ~~report for a specific party, parties, or period of time after the freeze is in place.~~
6 ~~To provide that authorization, you must contact the credit reporting agency and~~
7 ~~provide all of the following:~~

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

10 (2) ~~Proper identification to verify your identity.~~

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

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

21 ~~A credit reporting agency that receives a request from a consumer to lift~~

1 temporarily a freeze on a credit report shall comply with the request no later
2 than three business days after receiving the request.

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

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

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

17 (d) The information required to be disclosed by this section shall be
18 disclosed in writing. The information required to be disclosed pursuant to
19 subsection (c) of this section shall be disclosed on one side of a separate
20 document, with text no smaller than that prescribed by the Federal Trade
21 Commission for the notice required under 15 U.S.C. § 1681g § 1681g. The

1 ~~information required to be disclosed pursuant to subsection (c) of this section~~
2 may accurately reflect changes in numerical items that change over time (such
3 as the phone telephone number or address of Vermont State agencies), and
4 remain in compliance.

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

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

9 § 2480h. SECURITY FREEZE BY CREDIT REPORTING AGENCY; TIME
10 IN EFFECT

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

17 (2) A consumer who has been the victim of identity theft may place a
18 security freeze on his or her credit report by making a request in writing by
19 certified mail to a credit reporting agency with a valid copy of a police report,
20 investigative report, or complaint the consumer has filed with a law
21 enforcement agency about unlawful use of his or her personal information by

1 ~~another person. All other Vermont consumers may place a security freeze on~~
2 ~~his or her credit report by making a request in writing by certified mail to a~~
3 ~~credit reporting agency.~~

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

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

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

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

1 ~~her credit for a specific party, parties, or period of time.~~

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

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

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

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

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

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

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

1 (1) Upon consumer request pursuant to subsection (d) or (i) of this
2 section.

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

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

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

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

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

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

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

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

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

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

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

1 ~~(4) The Office of Child Support when investigating a child support case~~
2 pursuant to Title IV-D of the Social Security Act (42 U.S.C. et seq.) and
3 33 V.S.A. § 4102.

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

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

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

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

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

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

20 Sec. 5. REPORTS

21 ~~(a) On or before March 1, 2019, the Attorney General, the Department of~~

1 ~~Financial Regulation, and Secretary of State shall submit a preliminary report~~
2 concerning the implementation of this act to the House Committee on
3 Commerce and Economic Development and the Senate Committee on
4 Economic Development, Housing and General Affairs.

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

11 Sec. 6. EFFECTIVE DATES

12 (a) This section, Secs. 1 (findings and intent), 3–4 (eliminating fees for
13 placing or removing a credit freeze), and 5 (reports) shall take effect on
14 passage.

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

Sec. 1. FINDINGS AND INTENT

(a) The General Assembly finds the following:

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

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

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

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

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

(E) There are important differences between “data brokers” and

businesses with whom consumers have a direct relationship.

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

(ii) By contrast, consumers may not be aware that data brokers exist, who the companies are, or what information they collect, and may not be aware of available recourse.

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

(G) To provide consumers with necessary information about data brokers, Vermont should adopt a narrowly tailored definition of "data broker" and require data brokers to register annually with the Secretary of State and provide information about their data collection activities, opt-out policies,

purchaser credentialing practices, and security breaches.

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

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

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

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

(D) The requirement to adopt such an information security program currently applies to “financial institutions” subject to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq; to certain entities regulated by the Vermont Department of Financial Regulation pursuant to rules adopted by the Department; to persons who maintain or transmit health information regulated

by the Health Insurance Portability and Accountability Act; and to various types of businesses under laws in at least 13 other states.

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

(3) Prohibiting the acquisition of personal information through fraudulent means or with the intent to commit wrongful acts.

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

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

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

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

(A) In one of several major security breaches that have occurred in recent years, the names, Social Security numbers, birth dates, addresses,

driver's license numbers, and credit card numbers of over 145 million Americans were exposed, including over 247,000 Vermonters.

(B) In response to concerns about data security, identity theft, and consumer protection, the Vermont Attorney General and the Department of Financial Regulation have outlined steps a consumer should take to protect his or her identity and credit information. One important step a consumer can take is to place a security freeze on his or her credit file with each of the national credit reporting agencies.

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

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

(E) Vermont should exercise its authority to prohibit these fees to eliminate any financial barrier to placing or removing a security freeze.

(b) Intent.

(1) Providing consumers with more information about data brokers, their data collection practices, and the right to opt out. It is the intent of the

General Assembly to provide Vermonters with access to more information about the data brokers that collect consumer data and their collection practices by:

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

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

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

(B) requiring a data broker to register annually with the Secretary of State and make certain disclosures in order to provide consumers, policy makers, and regulators with relevant information.

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

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

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

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

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

Subchapter 1. General Provisions

§ 2430. DEFINITIONS

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

(1)(A) "Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(i) name;

(ii) address;

(iii) date of birth;

(iv) place of birth;

(v) mother's maiden name;

(vi) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vii) name or address of a member of the consumer's immediate family or household;

(viii) Social Security number or other government-issued identification number; or

(ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

(B) "Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.

(2) "Business" means a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to

operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of a financial institution, but ~~in no case shall it~~ does not include the State, a State agency, ~~or~~ any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State.

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

(4)(A) “Data broker” means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

(B) Examples of a direct relationship with a business include if the consumer is a past or present:

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

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

(iii) investor in the business; or

(iv) donor to the business.

(C) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker:

(i) developing or maintaining third-party e-commerce or application platforms;

(ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;

(iii) providing publicly available information related to a consumer's business or profession; or

(iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes.

(D) The phrase "sells or licenses" does not include:

(i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or

(ii) a sale or license of data that is merely incidental to the business.

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

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

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

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

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

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

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

~~(3)(6) “Data collector” may include the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly~~

~~held corporations, limited liability companies, financial institutions, retail operators, and any other entity that, means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information personally identifiable information, and includes the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.~~

~~(4)(7) “Encryption” means use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.~~

~~(8) “License” means a grant of access to, or distribution of, data by one person to another in exchange for consideration. A use of data for the sole benefit of the data provider, where the data provider maintains control over the use of the data, is not a license.~~

~~(5)(9)(A) “Personally identifiable information” means an individual’s a consumer’s first name or first initial and last name in combination with any one or more of the following digital data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:~~

~~(i) Social Security number;~~

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

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

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

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

~~(6)~~(10) "~~Records~~ Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(7)~~(11) "Redaction" means the rendering of data so that ~~it is~~ the data ~~are unreadable or is~~ are truncated so that no more than the last four digits of the identification number are accessible as part of the data.

~~(8)~~(12)(A) "Security breach" means unauthorized acquisition of, electronic data or a reasonable belief of an unauthorized acquisition of, electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by ~~the~~ a data collector.

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

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

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

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

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

(iv) that the information has been made public.

§ 2433. ACQUISITION OF BROKERED PERSONAL INFORMATION;

PROHIBITIONS

(a) Prohibited acquisition and use.

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

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

(A) stalking or harassing another person;

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

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

(b) Enforcement.

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

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

* * *

Subchapter 5. Data Brokers

§ 2446. ANNUAL REGISTRATION

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

data broker shall:

(1) register with the Secretary of State;

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

(3) provide the following information:

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

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

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

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

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

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

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

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

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

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

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

(1) a civil penalty of \$50.00 for each day, not to exceed a total of \$10,000.00 for each year; it fails to register pursuant to this section;

(2) an amount equal to the fees due under this section during the period it failed to register pursuant to this section; and

(3) other penalties imposed by law.

(c) The Attorney General may maintain an action in the Civil Division of the Superior Court to collect the penalties imposed in this section and to seek appropriate injunctive relief.

§ 2447. DATA BROKER DUTY TO PROTECT INFORMATION;

STANDARDS; TECHNICAL REQUIREMENTS

(a) Duty to protect personally identifiable information.

(1) A data broker shall develop, implement, and maintain a comprehensive information security program that is written in one or more

readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

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

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

(C) the amount of stored data; and

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

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

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

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

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

current safeguards for limiting such risks, including:

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

(B) employee compliance with policies and procedures; and

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

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

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

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

(6) supervision of service providers, by:

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

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

(7) reasonable restrictions upon physical access to records containing personally identifiable information and storage of the records and data in

locked facilities, storage areas, or containers;

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

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

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

(A) at least annually; or

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

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

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

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

(1) secure user authentication protocols, as follows:

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

(i) control of user IDs and other identifiers;

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

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

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

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

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

(2) secure access control measures that:

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

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

security;

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

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

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

(6) for files containing personally identifiable information on a system that is connected to the Internet, reasonably up-to-date firewall protection and operating system security patches that are reasonably designed to maintain the integrity of the personally identifiable information or a protocol that provides a higher degree of security;

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

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

(d) Enforcement.

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

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

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

§ 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

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

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

“NOTICE TO VERMONT CONSUMERS

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

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

- (A) in response to a court order;*
- (B) for direct mail offers of credit;*
- (C) if you have given ongoing permission and you have an existing relationship with the person requesting a copy of your credit report;*
- (D) where the request for a credit report is related to an education loan made, guaranteed, or serviced by the Vermont Student Assistance Corporation;*
- (E) where the request for a credit report is by the Office of Child Support Services when investigating a child support case;*
- (F) where the request for a credit report is related to a credit transaction entered into prior to January 1, 1993; ~~and~~ or*
- (G) where the request for a credit report is by the Vermont State Tax Department of Taxes and is used for the purpose of collecting or investigating delinquent taxes.*

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

Vermont Consumers Have the Right to Obtain a Security Freeze

You have a right to place a "security freeze" on your credit report pursuant to 9 V.S.A. § 2480h at no charge if you are a victim of identity theft. ~~All other~~

~~Vermont consumers will pay a fee to the credit reporting agency of up to \$10.00 to place the freeze on their credit report. The security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail.~~

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

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

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

(2) Proper identification to verify your identity.

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

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

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

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

A security freeze does not apply to a person or entity, or its affiliates, or

collection agencies acting on behalf of the person or entity with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account, provided you have previously given your consent to this use of your credit reports. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

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

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

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

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

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

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

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

(3) A security freeze shall prohibit, subject to the exceptions in subsection (l) of this section, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. ~~When a security freeze is in place, information~~

~~from a consumer's credit report shall not be released to a third party without prior express authorization from the consumer.~~

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

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

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

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

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

~~(2) The the unique personal identification number ~~or~~, password, or~~

other method of authentication provided by the credit reporting agency pursuant to subsection (c) of this section-; and

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

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

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

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

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

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

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

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

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

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

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

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

(l) The provisions of this section, including the security freeze, do not apply

to the use of a consumer report by the following:

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

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

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

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

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

(6) The Department of Taxes, municipal taxing authorities, or the

Department of Motor Vehicles, or any of their agents or assignees, acting to investigate or collect delinquent taxes or assessments, including interest and penalties, unpaid court orders, or acting to fulfill any of their other statutory or charter responsibilities.

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

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

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

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

Sec. 5. REPORTS

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

(b) On or before January 15, 2020, the Attorney General and Secretary of State shall update its preliminary report and provide additional information concerning the implementation of this act to the House Committee on Commerce and Economic Development and the Senate Committee on

Economic Development, Housing and General Affairs.

(c) On or before January 15, 2019, the Attorney General shall:

(1) review and consider the necessity of additional legislative and regulatory approaches to protecting the data security and privacy of Vermont consumers, including:

(A) whether to create or designate a Chief Privacy Officer and if so, the appropriate duties for, and the resources necessary to support, that position; and

(B) whether to expand or reduce the scope of regulation to businesses with direct relationships to consumers; and

(2) report its findings and recommendations to the House Committees on Commerce and Economic Development and on Energy and Technology and to the Senate Committee on Economic Development, Housing and General Affairs.

Sec. 6. ONE-STOP FREEZE NOTIFICATION

(a) The Attorney General, in consultation with industry stakeholders, shall consider one or more methods to ease the burden on consumers when placing or lifting a credit security freeze, including the right to place a freeze with a single nationwide credit reporting agency and require that agency to initiate a freeze with other agencies.

(b) On or before January 15, 2019, the Attorney General shall report his or

her findings and recommendations to the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing and General Affairs.

Sec. 7. EFFECTIVE DATES

(a) This section, Secs. 1 (findings and intent), 3–4 (eliminating fees for placing or removing a credit freeze), and 5–6 (reports) shall take effect on passage.

(b) Sec. 2 (data brokers) shall take effect on January 1, 2019.