

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

7 An act relating to data brokers and consumer protection

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

9 Sec. 1. FINDINGS AND INTENT

10 (a) The General Assembly finds the following:

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

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

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

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

13 (D) While data brokers offer many benefits, the risks associated with
14 the widespread aggregation and sale of data about consumers are extensive,
15 and include risks related to consumers' ability to know and control information
16 held and sold about them, and risks arising from the unauthorized or harmful
17 acquisition and use of consumer information.

1 (E) Consumers who choose to engage with traditional and e-
2 commerce businesses typically have some level of knowledge and control over
3 the collection of data by those business, including: the choice to use the
4 business’s products or services; the ability to review and consider data
5 collection policies; the ability to opt out of certain data collection practices;
6 and the ability to identify and contact customer representatives.

7 (F) By contrast, most consumers are not aware that data brokers
8 exist, who the companies are, how many operate in Vermont, or what
9 information they collect. In most cases consumers do not have a direct
10 relationship with a data broker and have little legal recourse to address
11 grievances arising from the collection or sale of personal information by a data
12 broker.

13 (G) Given this distinction, an appropriately narrow definition of the
14 term “data broker” for regulatory purposes should:

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

1 (ii) exclude 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 maintain a
6 direct relationship with those consumers, such as website, “app,” and e-
7 commerce platforms.

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

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

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

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

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

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

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

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

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

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

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

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

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

12 (4) Prohibiting the acquisition of personal information **through**
13 **fraudulent means or** with the intent to commit wrongful acts.

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

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

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

7 (5) Protecting Vermont’s children.

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

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

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

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

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

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

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

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

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

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

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

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

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

18 (b) Intent.

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

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

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

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

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

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

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

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

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

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

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

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

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

11 CHAPTER 62: PROTECTION OF PERSONAL INFORMATION

12 Subchapter 1: General Provisions

13 § 2430. DEFINITIONS

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

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

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

9 (3) “Data broker” means a business that collects and sells to one or more
10 third parties the personal information of a consumer with whom the business
11 does not have a direct relationship. For purposes of this definition, a consumer
12 does not have a direct relationship with a business if the consumer is a past,
13 present, or prospective:

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

16 (B) employee of the business; or

17 (C) donor to the business.

18 (4)(A) “Data broker security breach” means an unauthorized acquisition
19 or a reasonable belief of an unauthorized acquisition of personal information
20 maintained by a data broker.

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

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

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

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

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

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

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

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

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

18 (i) Social Security number;

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

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

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

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

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

11 (A) name;

12 (B) address;

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

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

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

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

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

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

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

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

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

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

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

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

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

10 § 2433. ACQUISITION OF PERSONAL INFORMATION; PROHIBITIONS

11 (a) Prohibited acquisition and use. A person shall not acquire **personal**
12 **information through fraudulent means**, or acquire or use personal information
13 for the purpose of:

14 (1) stalking or harassing another person;

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

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

1 (b) Personal information of certain teenagers. A person shall not sell or
2 offer for sale [collect, maintain, use, or disclose?] personal information
3 collected from or about a consumer who is 13 years of age or older and under
4 18 years of age, unless the person:

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

8 (2) following notice, provides the child’s parent or legal guardian the
9 opportunity to opt out of the sale or offer for sale of personal information.

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

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

18 (2) following notice, provides the child’s parent or legal guardian the
19 opportunity to opt out of the collection or disclosure of the personal
20 information.

21 (d) Enforcement.

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

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

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

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

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

1 (ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a
2 data collector ~~who~~ that, prior to the date of the security breach, on a form and
3 in a manner prescribed by the Attorney General, had sworn in writing to the
4 Attorney General that it maintains written policies and procedures to maintain
5 the security of personally identifiable information and respond to a breach in a
6 manner consistent with Vermont law shall notify the Attorney General of the
7 date of the security breach and the date of discovery of the breach and shall
8 provide a description of the breach prior to providing notice of the breach to
9 consumers pursuant to subdivision (1) of this subsection (b).

10 (iii) If the date of the security breach is unknown at the time notice
11 is sent to the Attorney General or to the Department, the data collector shall
12 send the Attorney General or the Department the date of the breach as soon as
13 it is known.

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

1 (C)(i) When the data collector provides notice of the security breach
2 to consumers pursuant to subdivision (1) of this subsection (b), the data
3 collector shall notify the Attorney General or the Department, as applicable, of
4 the number of Vermont consumers affected, if known to the data collector, and
5 shall provide a copy of the notice provided to consumers under subdivision (1)
6 of this subsection (b).

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

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

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

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

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

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

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

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

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

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

13 (A) the incident in general terms;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 (II) notifying major statewide and regional media.

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

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

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

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

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

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

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

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

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

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

18 (g) Enforcement.

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

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

10 * * *

11 Subchapter 4: Document Safe Destruction Act

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

14 (a) As used in this section:

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

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

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

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

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

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

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

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

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

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

9 * * *

10 Subchapter 5: Data Brokers

11 § 2446. ANNUAL REGISTRATION

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

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

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

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

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

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

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

7 § 2447. DATA BROKER DUTY TO PROTECT PERSONAL

8 INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS

9 (a) Duty to protect personal information.

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

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

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

18 (C) the amount of stored data; and

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

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

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

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

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

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

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

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

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

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

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

3 (6) supervision of service providers, including:

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

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

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

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

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

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

17 (A) at least annually; or

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

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

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

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

10 (1) secure user authentication protocols, including:

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

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

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

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

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

21 (2) secure access control measures that:

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

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

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

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

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

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

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

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

8 (d) Enforcement.

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

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

15 § 2448. DATA BROKER SECURITY BREACH NOTICE

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

18 (b) Notice of breach.

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

5 (B) A data broker shall provide notice of the data broker security
6 breach to consumers pursuant to subdivision (A) of this subdivision (b)(1) in
7 the most expedient time possible and without unreasonable delay, consistent
8 with measures necessary to determine the scope of the breach and restore the
9 reasonable integrity, security, and confidentiality of the data system, but not
10 later than 45 days after the discovery or notification, unless a law enforcement
11 agency requests a delay pursuant to subdivision (4) of this subsection (b).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8 (A) the incident in general terms;

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

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

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

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

17 (F) the approximate date of the breach.

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

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

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

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

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

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

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

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

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

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

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

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

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

3 (II) notifying major statewide and regional media.

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

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

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

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

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

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

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

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

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

2 § 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

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

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

4 “NOTICE TO VERMONT CONSUMERS

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

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

14 (A) in response to a court order;

15 (B) for direct mail offers of credit;

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

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

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

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

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

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

12 Vermont Consumers Have the Right to Obtain a Security Freeze

13 You have a right to place a “security freeze” on your credit report pursuant
14 to 9 V.S.A. § 2480h at no charge ~~if you are a victim of identity theft. All other~~
15 ~~Vermont consumers will pay a fee to the credit reporting agency of up to~~
16 ~~\$10.00 to place the freeze on their credit report.~~ The security freeze will
17 prohibit a credit reporting agency from releasing any information in your credit
18 report without your express authorization. A security freeze must be requested
19 in writing by certified mail.

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

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

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

19 (2) Proper identification to verify your identity.

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

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

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

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

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

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

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

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

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

5 § 2480h. SECURITY FREEZE BY CREDIT REPORTING AGENCY; TIME
6 IN EFFECT

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

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

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

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

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

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

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

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

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

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

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

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

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

1 (1) Upon consumer request, pursuant to subsection (d) or (j) 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 treat
12 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. EFFECTIVE DATE

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