

1 KEY (Note these shadings are not intended to have any legal affect, nor do
2 they reflect any sort of judgment or assessment by the AGO other than to
3 simply clarify what is new and what isn't new in the current bill, as requested):

4 1. [NO SHADING] Language that is included primarily for clean-up

5 2. Explanatory Language

6 3. Language that doesn't create new obligations

7 4. New regulation with new obligations

8 5. Adjustments to existing regulation, or creating regulation in line with

9 other states with new obligations.

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, there are also risks
14 associated with the widespread aggregation and sale of data about consumers,
15 including 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.

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

1 (i) Consumers who have a direct relationship with traditional and
2 e-commerce businesses typically have some level of knowledge and control
3 over 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; the
6 ability to identify and contact customer representatives; the ability to pursue
7 contractual remedies through litigation; and the knowledge necessary to
8 complain to law enforcement if other methods fail.

9 (ii) By contrast, consumers may not be aware that data brokers
10 exist, who the companies are, or what information they collect. Typically
11 consumers do not have a direct relationship with a data broker and have little
12 recourse to address grievances.

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

1 (G) At this time, comprehensive regulation of the data broker
2 industry would be premature. However, to give Vermont consumers access to
3 the information necessary to know who may be collecting or selling their data,
4 and whether and how to opt out of certain of these practices, Vermont should
5 adopt a narrowly-tailored definition of “data broker” and require data brokers
6 to annually register with the Secretary of State and provide information about
7 their data collection activities, including specific information about activities
8 relating to minors.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 (5) Removing financial barriers to protect consumer credit information.

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

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

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

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

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

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

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

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

10 (b) Intent.

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

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

17 (i) includes only those businesses that aggregate and sell the
18 personal information of consumers with whom they do not have a direct
19 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 maintain a
6 direct relationship with those consumers, such as website, “app,” and e-
7 commerce platforms; and

8 (B) requiring data brokers to annually register with the Secretary of
9 State and file certain disclosures concerning the opt out rights of their data
10 collection practices, including specific information about activities relating to
11 minors.

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

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

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

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

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

12 CHAPTER 62: PROTECTION OF PERSONAL INFORMATION

13 Subchapter 1: General Provisions

14 § 2430. DEFINITIONS

15 ~~The following definitions shall apply throughout this chapter unless~~
16 ~~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 has a direct relationship with a business if the consumer is a past or present:

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

15 (B) employee, contractor, or agent of the business; or

16 (C) donor to the business.

17 (4)(A) “Data broker security breach” means an unauthorized acquisition
18 or a reasonable belief of an unauthorized acquisition of personal information
19 maintained by a data broker when the personal information is not encrypted,
20 redacted, or protected by another method that renders the information
21 unreadable or unusable by an unauthorized person.

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.

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

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

16 (A) stalking or harassing another person;

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

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

21 (b) Enforcement.

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

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

7 [Criminal; rulemaking]

8 Subchapter 2: Security Breach Notice Act

9 § 2435. NOTICE OF SECURITY BREACHES

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

11 (b) Notice of breach.

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

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), or any later
16 supplemental information provided by the data collector, other than notice to
17 consumer or the number of Vermont consumers affected, shall not be disclosed
18 to any person other than the Department, the authorized agent or representative
19 of the Attorney General, a State's Attorney, or another law enforcement officer
20 engaged in legitimate law enforcement activities without the consent of the
21 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 personally identifiable information was not reasonably possible under
15 subdivision (1) of this subsection (d) and subsequently obtains facts indicating
16 that misuse of the ~~personal information~~ personally identifiable information has
17 occurred or is occurring, the data collector shall provide notice of the security
18 breach pursuant to subsection (b) of this section.

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

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

Subchapter 3: Social Security Number Protection Act

§ 2440. SOCIAL SECURITY NUMBER PROTECTION

* * *

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 (a) A data broker that collects and sells the personal information of a
13 Vermont consumer shall:

14 (1) register with the Secretary of State on or before January 31
15 following the year of the sale; and

16 (2) renew its registration annually thereafter for each year in which the
17 data broker collects and sells the personal information of a Vermont consumer.

18 (b) A data broker shall provide with its registration the following
19 information:

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

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

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

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

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

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

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

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

17 § 2447. DATA BROKER DUTY TO PROTECT PERSONAL

18 INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS

19 (a) Duty to protect personally identifiable information.

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

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

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

9 (C) the amount of stored data; and

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

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

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

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

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

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

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

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

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

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

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

17 (6) supervision of service providers, including:

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

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

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

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

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

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

13 (A) at least annually; or

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

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

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

1 (c) Information security program; computer system security requirements.

2 A comprehensive information security program required by this section shall at
3 minimum, and to the extent technically feasible, include the following
4 elements:

5 (1) secure user authentication protocols, including:

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

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

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

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

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

15 (F) an authentication protocol that provides a higher level of security
16 than those specified in subdivisions (A)–(E) of this subdivision (1).

17 (2) secure access control measures that:

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

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

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

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

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

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

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, or a protocol that provides a higher degree
6 of security; and

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

10 (d) Enforcement.

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

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

17 § 2448. DATA BROKER SECURITY BREACH NOTICE

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

20 (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), or any later
3 supplemental information provided by the data collector, other than notice to
4 consumer or the number of Vermont consumers affected shall not be disclosed
5 to any person other than the Attorney General, a State’s Attorney, or another
6 law enforcement officer engaged in legitimate law enforcement activities
7 without the consent of the data broker.

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

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

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

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

5 (iii) If law enforcement requests a delay in a manner other than in
6 writing, the data broker shall document the request contemporaneously in
7 writing, including the name of the law enforcement officer making the request
8 and the officer's law enforcement agency engaged in the investigation.

9 (iv) A law enforcement agency shall promptly notify the data
10 broker in writing when the law enforcement agency no longer believes that
11 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 (v) The data broker shall provide notice required by this section
15 without unreasonable delay upon receipt of a written communication, which
16 includes facsimile or electronic communication, from the law enforcement
17 agency withdrawing its request for delay.

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

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

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

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

12 (A) the incident in general terms;

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

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

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

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

21 (F) the approximate date of the breach.

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

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

4 (i) written notice mailed to the consumer’s residence;

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

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

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

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

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

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

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

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

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

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

6 (II) notifying major statewide and regional media.

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

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

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

5 (ii) The data broker may designate its notice and detailed
6 explanation to the Attorney General as a “trade secret” if the notice and
7 detailed explanation meet the definition of trade secret contained in 1 V.S.A.
8 § 317(c)(9).

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

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

1 (f) Enforcement. The Attorney General and State’s Attorney have sole and
2 full authority to investigate potential violations of this section and to enforce,
3 prosecute, obtain, and impose remedies for a violation of this section or any
4 rules or regulations made pursuant to this section as the Attorney General and
5 State’s Attorney have under chapter 63 of this title. The Attorney General may
6 refer the matter to the State’s Attorney in an appropriate case. The Superior
7 Courts shall have jurisdiction over any enforcement matter brought by the
8 Attorney General or a State’s Attorney under this subsection.

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

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

11 § 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

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

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

11 “NOTICE TO VERMONT CONSUMERS

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

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

21 (A) in response to a court order;

1 (B) for direct mail offers of credit;

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

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

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

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

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

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

18 Vermont Consumers Have the Right to Obtain a Security Freeze

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

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

1 When you place a security freeze on your credit report, within ten business
2 days you will be provided a personal identification number, ~~or~~ password, or
3 other equally 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 consumer
15 ~~who is not a victim of identity theft~~ to remove the freeze on your credit report
16 or authorize the release of your credit report for a specific party, parties, or
17 period of time after the freeze is in place. ~~For a victim of identity theft, there is~~
18 ~~no charge when the victim submits a copy of a police report, investigative~~
19 ~~report, or complaint filed with a law enforcement agency about unlawful use of~~
20 ~~the victim's personal information by another person.~~

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14 **Sec. 5. REPORTS**

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

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

7 Sec. 6. EFFECTIVE DATES

8 (a) This section, Sec. 1 (Findings and Intent), and Secs. 3–4 (eliminating
9 fees for placing or removing a credit freeze), and Sec. 5 (Reports) of this act
10 shall take effect on passage.

11 (b) Sec 2 of this act (amending 9 V.S.A. chapter 62) shall take effect on
12 July 1, 2018, except that 9 V.S.A. § 2447 (data broker information security
13 program) shall take effect on January 1, 2019.