

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

H.764

Representative Browning of Arlington moves to amend the bill by striking out all after the enacting clause and inserting in lieu thereof the following:

Sec. 1. 9 V.S.A. chapter 62 is amended to read:

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

Subchapter 1. General Provisions

§ 2430. DEFINITIONS

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

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

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

(3) “Data collector” ~~may include the State, State agencies, political subdivisions of the State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, retail~~

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

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

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

15 (i) Social Security number;

16 (ii) motor vehicle operator’s license number or nondriver
17 identification card number;

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

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

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

6 (6) “Personal information” means one or more of the following digital
7 data elements about a consumer:

8 (A) name;

9 (B) address;

10 (C) name or address of a member of his or her immediate family or
11 household;

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

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

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

19 ~~(6)~~(7) “Records Record” means any material on which written, drawn,
20 spoken, visual, or electromagnetic information is recorded or preserved,
21 regardless of physical form or characteristics.

1 ~~(7)~~(8) “Redaction” means the rendering of data so that ~~it is~~ the data are
2 unreadable or ~~is~~ are truncated so that no more than the last four digits of the
3 identification number are accessible as part of the data.

4 ~~(8)~~(9)(A) “Security breach” means unauthorized acquisition of,
5 ~~electronic data~~ or a reasonable belief of an unauthorized acquisition of,
6 ~~electronic data that compromises the security, confidentiality, or integrity of a~~
7 ~~consumer’s~~ personally identifiable information maintained by ~~the~~ a data
8 collector.

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

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

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

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

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

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

7 § 2431. DATA COLLECTORS; REGISTRATION; INFORMATION

8 When filing its annual registration with the Secretary of State pursuant to an
9 applicable provision of Titles 11-11C of the Vermont Statutes Annotated, a
10 business organization doing business in this State shall specify on its
11 registration form whether it collects personally identifiable information of
12 Vermont consumers as one of its business activities, and if so, it shall further
13 specify:

14 (1) whether it uses industry best practice security systems to protect
15 consumer personally identifiable information; and

16 (2) whether it notifies customers of security breaches that result in stolen
17 personally identifiable information.

18 § 2433. ACQUISITION OF PERSONAL INFORMATION; PROHIBITIONS

19 (a) Prohibited acquisition and use.

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

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

3 (A) stalking or harassing another person;

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

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

8 (b) Enforcement.

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

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

15 Subchapter 2. Security Breach Notice Act

16 § 2435. NOTICE OF SECURITY BREACHES

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

18 (b) Notice of breach.

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

1 notify the consumer ~~that there has been~~ of a security breach following
2 discovery or notification to the data collector of the breach.

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

14 (2) ~~Any~~ A data collector that maintains or possesses ~~computerized data~~
15 ~~containing~~ personally identifiable information ~~of a consumer~~ that the data
16 collector does not own or license, ~~or any~~ a data collector that acts or conducts
17 business in Vermont that maintains or possesses ~~records or data containing~~
18 personally identifiable information that the data collector does not own or
19 license, shall notify the owner or licensee of the information of any security
20 breach immediately following discovery of the breach, consistent with the

1 legitimate needs of law enforcement as provided in ~~subdivisions (3) and~~
2 subdivision (4) of this subsection (b).

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

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

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

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

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

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

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

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

1 the number of Vermont consumers affected, if known to the data collector, and
2 shall provide a copy of the notice provided to consumers under subdivision (1)
3 of this subsection (b).

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

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

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

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

20 (iv) A law enforcement agency shall promptly notify the data
21 collector in writing when the law enforcement agency no longer believes that

1 notification may impede a law enforcement investigation, or a national or
2 Homeland Security investigation, or jeopardize public safety or national or
3 Homeland Security interests.

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

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

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

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

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

4 (A) the incident in general terms;

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

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

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

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

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

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

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

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

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

20 (I) the data collector's primary method of communication with
21 the consumer is by electronic means, the electronic notice does not request or

1 contain a hypertext link to a request that the consumer provide personal
2 information, and the electronic notice conspicuously warns consumers not to
3 provide personal information in response to electronic communications
4 regarding security breaches; or

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

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

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

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

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

14 (III) the data collector does not have sufficient contact
15 information.

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

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

19 (II) notifying major statewide and regional media.

20 (c) ~~In the event~~ If a data collector provides notice to more than 1,000
21 consumers at one time pursuant to this section, the data collector shall notify,

1 without unreasonable delay, all consumer reporting agencies that compile and
2 maintain files on consumers on a nationwide basis, as defined in 15 U.S.C.
3 § 1681a(p), of the timing, distribution, and content of the notice. This
4 subsection shall not apply to a person who is licensed or registered under Title
5 8 by the Department of Financial Regulation.

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

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

20 (ii) The data collector may designate its notice and detailed
21 explanation to the Vermont Attorney General or the Department of Financial

1 Regulation as “trade secret” if the notice and detailed explanation meet the
2 definition of trade secret contained in 1 V.S.A. § 317(c)(9).

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

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

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

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

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

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

9 (g) Enforcement.

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

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

8 Subchapter 3. Social Security Number Protection Act

9 § 2440. SOCIAL SECURITY NUMBER PROTECTION

10 * * *

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

1 requester, and delivered by mail, facsimile, or electronic transmission, or
2 delivered in person to the town clerk or clerk of court. The request must
3 specify the ~~personal~~ information to be redacted, information that identifies the
4 document that contains the ~~personal~~ information to be redacted, and unique
5 information that identifies the location within the document that contains the
6 Social Security number, employer taxpayer identification number, driver's
7 license number, State identification number, passport number, checking
8 account number, savings account number, credit card number, or debit card
9 number, or personal identification number (PIN) code or passwords to be
10 redacted. The request for redaction shall be considered a public record with
11 access restricted to the town clerk, the clerk of court, their staff, or upon order
12 of the court. The town clerk or clerk of court shall have no duty to inquire
13 beyond the written request to verify the identity of a person requesting
14 redaction and shall have no duty to remove redaction for any reason upon
15 subsequent request by an individual or by order of the court, if impossible to
16 do so. No fee will be charged for the redaction pursuant to such request. Any
17 person who requests a redaction without proper authority to do so shall be
18 guilty of an infraction, punishable by a fine not to exceed \$500.00 for each
19 violation.

20 * * *

1 Subchapter 4. Document Safe Destruction Act

2 § 2445. SAFE DESTRUCTION OF DOCUMENTS CONTAINING

3 PERSONAL CONFIDENTIAL INFORMATION

4 (a) As used in this section:

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

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

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

1 account number, credit card number, debit card number, or any other financial
2 information.

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

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

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

16 (1) ensuring the security and confidentiality of customer ~~personal~~
17 confidential information;

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

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

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

12 * * *

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

14 § 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

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

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

14 “NOTICE TO VERMONT CONSUMERS

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

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

3 (A) in response to a court order;

4 (B) for direct mail offers of credit;

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

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

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

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

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

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

21 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.

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

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

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

5 (2) Proper identification to verify your identity.

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

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

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

19 A security freeze will not apply to “preauthorized approvals of credit.” If
20 you want to stop receiving preauthorized approvals of credit, you should call

1 [INSERT PHONE NUMBERS] [ALSO INSERT ALL OTHER CONTACT
2 INFORMATION FOR PRESCREENED OFFER ~~OPT-OUT~~ OPT-OUT.]

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

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

13 (d) The information required to be disclosed by this section shall be
14 disclosed in writing. The information required to be disclosed pursuant to
15 subsection (c) of this section shall be disclosed on one side of a separate
16 document, with text no smaller than that prescribed by the Federal Trade
17 Commission for the notice required under 15 U.S.C. ~~§ 1681g~~ § 1681g. The
18 information required to be disclosed pursuant to subsection (c) of this section
19 may accurately reflect changes in numerical items that change over time (such
20 as the ~~phone~~ telephone number or address of Vermont State agencies), and
21 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. 3. 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.

20 (d) If the consumer wishes to allow his or her credit report to be accessed
21 for a specific party, parties, or period of time while a freeze is in place, he or

1 she shall contact the credit reporting agency, request that the freeze be
2 temporarily lifted, and provide the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20 (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. 4. EFFECTIVE DATE

21 This act shall take effect on passage.