

1 TO THE HONORABLE SENATE:

2 The Committee on Economic Development, Housing and General Affairs to
3 which was referred House Bill No. 764 entitled “An act relating to data brokers
4 and consumer protection” respectfully reports that it has considered the same
5 and recommends that the Senate propose to the House that the bill be amended
6 by striking out all after the enacting clause and inserting in lieu thereof the
7 following:

8 Sec. 1. FINDINGS AND INTENT

9 (a) The General Assembly finds the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11 (b) Intent.

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

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

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

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

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

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

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

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

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

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

5 CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

6 Subchapter 1. General Provisions

7 § 2430. DEFINITIONS

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

10 (1) “Biometric record” means an individual’s psychological, biological,
11 or behavioral characteristics that can be used, singly or in combination with
12 each other or with other identifying data, to establish individual identity,
13 including:

14 (A) imagery of the iris, retina, fingerprint, face, hand, palm, or vein
15 patterns, and voice recordings, from which an identifier template, such as a
16 face print or a minutiae template or voiceprint, can be extracted;

17 (B) keystroke patterns or rhythms;

18 (C) gait patterns or rhythms; and

19 (D) sleep health or exercise data that contain identifying information.

1 (2)(A) “Brokered personal information” means:

2 (i) one or more of the following computerized data elements about
3 a consumer:

4 (I) name;

5 (II) address;

6 (III) a personal identifier, including a Social Security number,
7 other government-issued identification number, or biometric record;

8 (IV) an indirect identifier, including date of birth, place of
9 birth, or mother’s maiden name; or

10 (V) other information that, alone or in combination, is linked or
11 linkable to the consumer that would allow a reasonable person to identify the
12 consumer with reasonable certainty; and

13 (ii) the computerized data element or elements are:

14 (I) categorized by characteristic for dissemination to third
15 parties; or

16 (II) combined with nonpublic information.

17 (B) “Brokered personal information” does not include publicly
18 available information that is solely related to a consumer’s business or
19 profession.

20 (3) “Business” means a commercial entity, including a sole
21 proprietorship, partnership, corporation, association, limited liability company,

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

8 ~~(2)~~(4) “Consumer” means an individual residing in this State.

9 (5)(A) “Data broker” means:

10 (i) A business that:

11 (I) provides people search services; or

12 (II) collects and sells or licenses to one or more third parties the
13 brokered personal information of a consumer with whom the business does not
14 have a direct relationship.

15 (ii) “Data broker” includes each affiliated business that is under
16 common ownership or control if one business collects brokered personal
17 information and provides it to another to sell or license.

18 (B) “Data broker” does not include:

19 (i) a business that solely develops or maintains third-party e-
20 commerce or application platforms; or

1 (ii) a business that solely provides publicly available information
2 via real-time or near-real-time alert services for health or safety purposes.

3 (C) For purposes of subdivision (5)(A)(i)(II) of this subsection,
4 examples of a direct relationship with a business include if the consumer is a
5 past or present:

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

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

9 (iii) investor in the business; or

10 (iv) donor to the business.

11 (D) For purposes of subdivision (5)(A)(i)(II) of this subsection, a
12 business does not sell or license brokered personal information within the
13 meaning of the definition of “data broker” if the sale or license is merely
14 incidental to one of its lines of business.

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

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

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

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

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

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

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

20 ~~(3)(7) “Data collector” may include the State, State agencies, political~~
21 ~~subdivisions of the State, public and private universities, privately and publicly~~

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

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

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

15 (10)(A) “People search services” means an Internet-based service in
16 which an individual can pay a fee to search for a specific consumer, and which
17 provides information about the consumer such as the consumer’s address, age,
18 maiden name, alias, name or addresses of relatives, financial records, criminal
19 records, background reports, or property details, where the consumer whose
20 data is provided does not have a direct relationship with the business.

1 (B) “People search services” does not include a service that solely
2 provides publicly available information related to a consumer’s business or
3 profession.

4 ~~(5)(11)~~(A) “Personally identifiable information” means ~~an individual’s a~~
5 consumer’s first name or first initial and last name in combination with any
6 one or more of the following digital data elements, when either the name or the
7 data elements are not encrypted or redacted or protected by another method
8 that renders them unreadable or unusable by unauthorized persons:

9 (i) Social Security number;

10 (ii) motor vehicle operator’s license number or nondriver
11 identification card number;

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

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

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

1 ~~(6)~~(12) “~~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)~~(13) “Redaction” means the rendering of data so that ~~it is~~ the data are
5 unreadable or ~~is~~ are truncated so that no more than the last four digits of the
6 identification number are accessible as part of the data.

7 ~~(8)~~(14)(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 BROKERED PERSONAL INFORMATION;

11 PROHIBITIONS

12 (a) Prohibited acquisition and use.

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

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

17 (A) stalking or harassing another person;

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

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

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

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

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

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

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

11 (E) a statement whether the data broker implements a purchaser
12 credentialing process;

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

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

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

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

3 (1) a civil penalty of \$50.00 for each day, not to exceed a total of
4 \$10,000.00 for each year, it fails to register pursuant to this section;

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

7 (3) other penalties imposed by law.

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

11 § 2447. DATA BROKER DUTY TO PROTECT INFORMATION;

12 STANDARDS; TECHNICAL REQUIREMENTS

13 (a) Duty to protect personally identifiable information.

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

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

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

1 (C) the amount of stored data; and

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

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

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

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

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

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

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

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

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

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

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

8 (6) supervision of service providers, by:

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

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

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

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

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

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

3 (A) at least annually; or

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

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

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

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

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

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

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

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

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

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

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

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

10 (2) secure access control measures that:

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

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

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

- 1 (4) reasonable monitoring of systems for unauthorized use of or access
2 to personally identifiable information;
- 3 (5) encryption of all personally identifiable information stored on
4 laptops or other portable devices or a protocol that provides a higher degree of
5 security;
- 6 (6) for files containing personally identifiable information on a system
7 that is connected to the Internet, reasonably up-to-date firewall protection and
8 operating system security patches that are reasonably designed to maintain the
9 integrity of the personally identifiable information or a protocol that provides a
10 higher degree of security;
- 11 (7) reasonably up-to-date versions of system security agent software that
12 must include malware protection and reasonably up-to-date patches and virus
13 definitions, or a version of such software that can still be supported with up-to-
14 date patches and virus definitions and is set to receive the most current security
15 updates on a regular basis or a protocol that provides a higher degree of
16 security; and
- 17 (8) education and training of employees on the proper use of the
18 computer security system and the importance of personally identifiable
19 information security.

1 (d) Enforcement.

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

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

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

9 § 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

20 (b) As frequently as new telephone directories are published, the credit
21 reporting agency shall cause to be listed its name and number in each

1 telephone directory published to serve communities of this State. In
2 accordance with rules adopted by the Attorney General, the credit reporting
3 agency shall make provision for consumers to request by telephone the
4 information required to be disclosed pursuant to subsection (a) of this section
5 at no cost to the consumer.

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

9 “NOTICE TO VERMONT CONSUMERS

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

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

19 (A) in response to a court order;

20 (B) for direct mail offers of credit;

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

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

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

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

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

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

17 Vermont Consumers Have the Right to Obtain a Security Freeze

18 You have a right to place a "security freeze" on your credit report pursuant
19 to 9 V.S.A. § 2480h at no charge ~~if you are a victim of identity theft. All other~~
20 ~~Vermont consumers will pay a fee to the credit reporting agency of up to~~
21 ~~\$10.00 to place the freeze on their credit report.~~ The security freeze will

1 prohibit a credit reporting agency from releasing any information in your credit
2 report without your express authorization. A security freeze must be requested
3 in writing by certified mail.

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

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

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

1 (2) Proper identification to verify your identity.

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

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

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

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

19 A security freeze does not apply to a person or entity, or its affiliates, or
20 collection agencies acting on behalf of the person or entity with which you
21 have an existing account that requests information in your credit report for the

1 purposes of reviewing or collecting the account, provided you have previously
2 given your consent to this use of your credit reports. Reviewing the account
3 includes activities related to account maintenance, monitoring, credit line
4 increases, and account upgrades and enhancements.

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

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

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

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

2 § 2480h. SECURITY FREEZE BY CREDIT REPORTING AGENCY; TIME
3 IN EFFECT

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

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

18 (3) A security freeze shall prohibit, subject to the exceptions in
19 subsection (1) of this section, the credit reporting agency from releasing the
20 consumer's credit report or any information from it without the express
21 authorization of the consumer. ~~When a security freeze is in place, information~~

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

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

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

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

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

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

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; and

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

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

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

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

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

18 (2) If the consumer's credit report was frozen due to a material
19 misrepresentation of fact by the consumer. If a credit reporting agency intends
20 to remove a freeze upon a consumer's credit report pursuant to this

1 subdivision, the credit reporting agency shall notify the consumer in writing
2 prior to removing the freeze on the consumer's credit report.

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

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

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

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

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

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

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

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

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

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

18 (4) The Office of Child Support when investigating a child support case
19 pursuant to Title IV-D of the Social Security Act (42 U.S.C. et seq.) and
20 33 V.S.A. § 4102.

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

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

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

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

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

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

17 Sec. 5. REPORTS

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

1 the Senate Committee on Economic Development, Housing and General
2 Affairs.

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

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

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

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

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

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

1 Sec. 6. ONE-STOP FREEZE NOTIFICATION

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

7 (b) On or before January 15, 2019, the Attorney General shall report his or
8 her findings and recommendations to the House Committee on Commerce and
9 Economic Development and the Senate Committee on Economic
10 Development, Housing and General Affairs.

11 Sec. 7. EFFECTIVE DATES

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

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

16

17

18 (Committee vote: _____)

19

20

Senator _____

21

FOR THE COMMITTEE