TO THE HONORABLE SENATE:

The Committee on Economic Development, Housing and General Affairs to which was referred House Bill No. 764 entitled "An act relating to data brokers and consumer protection" respectfully reports that it has considered the same and recommends that the Senate propose to the House that

Sec. 1. FINDINGS AND INTENT

(a) The General Assembly finds the following:

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

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

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

(C) Data brokers provide information that is critical to services offered in the modern economy, including: targeted marketing and sales; credit reporting; background checks; government information; risk mitigation

and fraud detection; people search; decisions by banks, insurers, or others whether to provide services; ancestry research; and voter targeting and strategy by political campaigns.

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

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

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

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

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

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

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

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

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

(C) One approach to protecting consumer data has been to require government agencies and certain regulated businesses to adopt an "information security program" that has "appropriate administrative, technical, and physical

safeguards to ensure the security and confidentiality of records" and "to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm." Federal Privacy Act; 5 U.S.C. § 552a.

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

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

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

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

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

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

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

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

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

(C) Under State law, when a consumer places a security freeze, a credit reporting agency issues a unique personal identification number or password to the consumer. The consumer must provide the PIN or password,

and his or her express consent, to allow a potential creditor to access his or her credit information.

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

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

(b) Intent.

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

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

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

(ii) excludes businesses that collect information from their own customers, employees, users, or donors, including: banks and other financial institutions; utilities; insurers; retailers and grocers; restaurants and hospitality businesses; social media websites and mobile "apps"; search websites; and

businesses that provide services for consumer-facing businesses and maintain a direct relationship with those consumers, such as website, "app," and e-commerce platforms; and

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

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

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

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

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

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

Subchapter 1. General Provisions

§ 2430. DEFINITIONS

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

(1) "Biometric record" means an individual's psychological, biological, or behavioral characteristics that can be used, singly or in combination with each other or with other identifying data, to establish individual identity, including:

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

(B) keystroke patterns or rhythms;

(C) gait patterns or rhythms; and

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

(2)(A) "Brokered personal information" means:

(i) one or more of the following digital data elements about a consumer:

(I) name;

(II) address;

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

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

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

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

(ii) the digital data element or elements are:

(I) categorized; or

(II) combined with nonpublic information.

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

(3) "Business" means a commercial entity, including a sole proprietorship, partnership, corporation, association, limited liability company, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent, affiliate, or subsidiary of

a financial institution, but ~~in no case shall it~~ does not include the State, a State agency, ~~or~~ any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State.

~~(2)~~(4) "Consumer" means an individual residing in this State.

(5)(A) "Data broker" means:

(i) A business that:

(I) provides people search services; or

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

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

(B) "Data broker" does not include:

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

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

(C) For purposes of subdivision (3)(A)(ii) of this subsection:

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

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

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

(III) investor in the business; or

(IV) donor to the business.

(D) For purposes of subdivision (3)(A)(ii) of this subsection, a business does not sell or license brokered personal information within the meaning of the definition of "data broker" if the sale or license is merely incidental to one of its lines of business.

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

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

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

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

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

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

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

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

State, public and private universities, privately and publicly held corporations, limited liability companies, financial institutions, and retail operators.

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

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

["License" means to grant the authority to access or use in exchange for consideration.]

(10)(A) "People search services" means an Internet-based service in which an individual can pay a fee to search for a specific consumer, and which provides information about the consumer such as the consumer's address, age, maiden name, alias, name or addresses of relatives, financial records, criminal records, background reports, or property details.

[*Can* pay a fee vs. completely free vs. *pays* a fee?]

(B) "People search services" does not include a service that solely provides publicly available information related to a consumer's business or profession.

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

(i) Social Security number;

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

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

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

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

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

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

~~(8)~~(14)(A) "Security breach" means unauthorized acquisition of, ~~electronic data~~ or a reasonable belief of an unauthorized acquisition of, ~~electronic data that compromises the security, confidentiality, or integrity of a consumer's~~ personally identifiable information maintained by ~~the~~ a data collector.

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

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

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

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

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

(iv) that the information has been made public.

§ 2433. ACQUISITION OF BROKERED PERSONAL INFORMATION; PROHIBITIONS

(a) Prohibited acquisition and use.

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

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

(A) stalking or harassing another person;

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

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

(b) For purposes of this section, brokered personal information includes information acquired from people search services.

[The effect of this addition = a person cannot acquire or use for an unlawful purpose: (1) brokered personal information (as defined); or (2) any information acquired from people search services]

(c) Enforcement.

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

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

* * *

Subchapter 5. Data Brokers

§ 2446. ANNUAL REGISTRATION

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

(1) register with the Secretary of State;

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

(3) provide the following information:

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

(B) the sources of the data collected by the data broker;

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

(i) the method for requesting an opt out;

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

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

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

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

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

(G) where the data broker has actual knowledge that it possesses the brokered personal information of minors, a separate statement detailing the

data collection practices, databases, sales activities, and opt out policies that are applicable to the brokered personal information of minors; and

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

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

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

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

(3) other penalties imposed by law.

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

§ 2447. DATA BROKER DUTY TO PROTECT INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS

(a) Duty to protect personally identifiable information.

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

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

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

(C) the amount of stored data; and

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

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

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

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

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

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

(B) employee compliance with policies and procedures; and

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

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

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

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

(6) supervision of service providers, by:

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

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

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

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

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

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

(A) at least annually; or

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

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

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

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

(1) secure user authentication protocols, as follows:

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

(i) control of user IDs and other identifiers;

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

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

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

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

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

(2) secure access control measures that:

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

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

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

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

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

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

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

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

(d) Enforcement.

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

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

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

§ 2480b. DISCLOSURES TO CONSUMERS

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

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

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

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

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

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

"NOTICE TO VERMONT CONSUMERS

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

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

(A) in response to a court order;

(B) for direct mail offers of credit;

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

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

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

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

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

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

Vermont Consumers Have the Right to Obtain a Security Freeze

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

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

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

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

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

(2) Proper identification to verify your identity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b)(1) A credit reporting agency shall place a security freeze on a consumer's credit report ~~no~~ not later than five business days after receiving a written request from the consumer.

(2) If a consumer requests that a security freeze be placed on his or her credit report by a credit reporting agency, the agency shall initiate placement of the freeze with other credit reporting agencies that compile and maintain files on consumers on a nationwide basis, unless the consumer elects not to have the security freeze applied to other credit reporting agencies.

[Keep this in light of H.593?]

(c) The credit reporting agency shall send a written confirmation of the security freeze to the consumer within 10 business days and shall provide the consumer with a unique personal identification number or password, other than

the customer's Social Security number, or another method of authentication that is equally or more secure than a PIN or password, to be used by the consumer when providing authorization for the release of his or her credit for a specific party, parties, or period of time.

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

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

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

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

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

(f) A credit reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report pursuant to subsection (d) of this section

shall comply with the request ~~no~~ not later than three business days after receiving the request.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sec. 5. REPORTS

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

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

(c) On or before January 15, 2019, the Attorney General, in partnership with the Department of Financial Regulation and the Cybersecurity Advisory Team shall:

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

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

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

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

Sec. 6. 9 V.S.A. § 2431 is added to read:

§ 2431. CYBERSECURITY ADVISORY TEAM

(a) There is created the Vermont State Cybersecurity Advisory Team composed of the following members:

(1) the State Chief Information Security Officer;

(2) the State Chief Information Officer;

(3) the Governor's Homeland Security Advisor or designee;

(4) a representative from the Vermont National Guard;

(5) the Attorney General or designee;

(6) a representative from Vermont Emergency Management;

(7) four members appointed by the Governor who are leaders from the utilities sector, higher education, health care, or business.

(b) The Team may in its discretion:

(1) establish interagency working groups to support its mission, drawing membership from any agency or department of State government; and

(2) consult with private sector professionals and those from other states, the federal government, and municipalities for information and advice on issues related to its work.

(c) Powers and duties. The Council shall:

(1) develop a strategic plan for protection of Vermont public and private sector information and systems;

(2) formally evaluate statewide cybersecurity readiness and develop best practices for policies and procedures to strengthen administrative, technical, and physical cybersecurity safeguards as a resource for State government, Vermont businesses, and the public;

(3) build strong relationships and lines of communications among the State government, federal government, and the private sector designed to ensure resilience of electronic information systems;

(4) build strong partnerships with local universities and colleges in order to leverage cybersecurity resources; and

(5) identify and advise on opportunities to:

(A) ensure Vermont promotes, attracts, and retains a highly skilled cybersecurity workforce;

(B) raise citizen awareness through outreach and public service announcements;

(C) provide technical capabilities, training, and advice to local government and the private sector;

(D) provide expertise to the General Assembly regarding statutory language that could further protect critical assets, infrastructure, services, and personally identifiable information;

(E) advise on strategic, operational, and budgetary impacts to the State; and

(F) engage State and federal partners in assessing and managing risk.

(d) Assistance. The Council shall receive administrative and staff support from the Secretary of Digital Services and legal support from the Governor's Counsel and the Department of Public Safety.

(e) Compensation and reimbursement. Members of the Council who are not employees of the State of Vermont and who are not otherwise compensated or reimbursed for their attendance at meetings shall be entitled to per diem compensation and reimbursement of expenses pursuant to 32 V.S.A. § 1010. These payments shall be made from monies appropriated to the Agency of Digital Services.

Sec. 7. EFFECTIVE DATES

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

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

(c) The remaining sections shall take effect on July 1, 2018.

(Committee vote: _____)

_____

Senator _____

FOR THE COMMITTEE