TO THE HOUSE OF REPRESENTATIVES:

The Committee on Commerce and Economic Development to which was referred House Bill No. 121 entitled "An act relating to enhancing consumer privacy" respectfully reports that it has considered the same and recommends that the bill be amended by striking out all after the enacting clause and inserting in lieu thereof the following:

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

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

Subchapter 1. General Provisions

§ 2430. DEFINITIONS

As used in this chapter:

(1) "Biometric identifier" means unique biometric data generated from measurements or technical analysis of an individual's biological characteristics, including a fingerprint, voiceprint, retina, iris, or other unique biological characteristics, which is used to identify a specific individual.

(2)(A) "Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties:

(i) name;

(ii) address;

(iii) date of birth;

(iv) place of birth;

(v) mother's maiden name;

(vi) ~~unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data~~ biometric identifier;

(vii) name or address of a member of the consumer's immediate family or household;

(viii) Social Security number or other government-issued identification number; or

(ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty.

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

~~(2)~~(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 does not include the State, a State agency, any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State.

~~(3)~~(4) "Consumer" means an individual residing in this State.

~~(4)~~(5)(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

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

(i) customer, client, subscriber, user, or registered 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.

(C) The following activities conducted by a business, and the collection and sale or licensing of brokered personal information incidental to conducting these activities, do not qualify the business as a data broker:

(i) developing or maintaining third-party e-commerce or application platforms;

(ii) providing 411 directory assistance or directory information services, including name, address, and telephone number, on behalf of or as a function of a telecommunications carrier;

(iii) providing publicly available information related to a consumer's business or profession; or

(iv) providing publicly available information via real-time or near-real-time alert services for health or safety purposes.

(D) The phrase "sells or licenses" does not include:

(i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; or

(ii) a sale or license of data that is merely incidental to the business.

~~(5)~~(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.

~~(6)~~(7) "Data collector" means a person who, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or

otherwise deals with 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.

(8) "De-identified data means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or to a device linked to the individual, if the data collector or data broker that possesses the data:

(A) takes reasonable measures to ensure that the data cannot be associated with an individual;

(B) publicly commits to process the data in a de-identified fashion and not attempt to re-identify the data; and

(C) contractually obligates a recipient of the data to satisfy the criteria established in subdivisions (8)(A) and (B) of this section.

~~(7)~~(9) "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.

(10) "Identified or identifiable individual" means an individual who can be readily identified, directly or indirectly.

~~(8)~~(11) "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.

~~(9)~~(12) "Login credentials" means a consumer's user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account.

~~(10)~~(13)(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) a Social Security number;

(ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;

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

(iv) a password, personal identification number, or other access code for a financial account;

(v) ~~unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data~~ a biometric identifier;

(vi) genetic information; and

(vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention;

(II) a health care professional's medical diagnosis or treatment of the consumer; or

(III) a health insurance policy number.

(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.

(14) "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with a particular consumer, and includes personally identifiable information, brokered personal information, login credentials, and covered information as defined in the Health Insurance Portability and Accountability Act of 1996.

(15) "Predictive analytics" means any form of automated processing of personal information to evaluate, analyze, or predict personal aspects

concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(16) "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal information or on sets of personal information, including the collection, use, storage, disclosure, analysis, deletion, or modification of personal information.

(17) "Publicly available information" means information that:

(A) is lawfully made available through federal, state, or municipal government records or widely-distributed media; and

(B) a data collector or a data broker has a reasonable basis to believe a consumer has lawfully made available to the general public.

~~(11)~~(18) "Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(12)~~(19) "Redaction" means the rendering of data so that the data are unreadable or are truncated so that no more than the last four digits of the identification number are accessible as part of the data.

~~(13)~~(20)(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 or login credentials maintained by a data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are 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 or login credentials have 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.

(21) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means personal information by the business to another business or a third party for monetary or other valuable consideration.

(22)(A) "Targeted advertising" means the targeting of advertisements to a consumer based on the consumer's activities with one or more businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

(B) "Targeted advertising" does not include advertising:

(i) based on activities within a data collector or data broker's own commonly-branded websites for online applications;

(ii) based on the context of a consumer's current search query or visit to a website or online application; or

(iii) to a consumer in response to the consumer's request for information or feedback.

* * *

§ 2432. APPLICATION AND SCOPE

The provisions of this chapter apply to a person that conducts business in this State or that produce products or services that are targeted to residents of this State.

§ 2433. GENERAL REQUIREMENTS FOR COLLECTION AND USE OF DATA

(a) Data minimization. A data collector's collection, use, retention, and sharing of personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed.

(b) Duties.

(1) A data collector that controls the collection of a consumer's personal information shall, at or before the point of collection, inform the consumers of the categories of personal information to be collected and the purposes for which the categories of personal information are collected or used and whether that information is sold or shared.

(2) A data collector that obtains personal information from a consumer shall not use that information for an additional purpose that is inconsistent with the purpose for which it was initially collected without providing the consumer notice consistent with this subsection.

(3) A data collector shall not retain personal information if it is unable to determine the initial purpose, notice, or consent described in this subsection.

(c) Non-discrimination. A data collector shall not discriminate against a consumer for exercising a right provided in subsection (e) of this section, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer.

(d) Rights of consumers. A consumer shall have the right to:

(1) confirm whether a data collector or data broker is processing the consumer's personal information and to access the consumer's personal information, unless the confirmation or access would require the data collector or data broker to reveal a trade secret;

(2) correct inaccuracies in the consumer's personal information, taking into account the nature of the personal information and the purposes of the processing of the consumer's personal information;

(3) delete personal information provided by, or obtained about, the consumer;

(4) obtain a copy of the consumer's personal information processed by a data collector, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another data collector without hindrance, where the processing is carried out by automated means, provided such data collector shall not be required to reveal any trade secret; and

(5) opt out of the processing of the personal information for purposes of targeted advertising, the sale of personal information, or profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

(e) Do not track.

(1) On or after July 1, 2023, a data collector that processes for purposes of targeted advertising, predictive analytics, tracking, or the sale of personal information or that is a data broker shall allow consumers to exercise the right to opt out of the processing of personal information concerning the consumer for purposes of targeted advertising, predictive analytics, tracking, or the sale of personal information through a user-selected universal opt-out mechanism.

(2)(A) A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to opt out of the processing of the consumer's personal data for one or more of the purposes specified in subdivision (1) of this subsection.

(B) The consumer may designate an authorized agent by one or more methods, including an Internet link or a browser setting, browser extension, or global device setting, indicating the consumer's intent to opt out of processing.

(C) A data collector or data broker shall comply with an opt out request received from an authorized agent if the data collector or data broker is

able to verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

(f) Exemptions. Nothing in this section shall be construed to restrict a data collector or data broker's ability to:

(1) comply with federal, state, or municipal law;

(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal or other governmental authorities;

(3) cooperate with law enforcement agencies concerning conduct or activity that the data collector or data broker reasonably and in good faith believes may violate federal, state, or municipal law;

(4) investigate, establish, exercise, prepare for, or defend legal claims;

(5) provide a product or service specifically requested by a consumer;

(6) perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) take steps at the request of a consumer prior to entering into a contract;

(8) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;

(9) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action;

(10) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws;

(11) assist another data collector, data broker, or third party with any of the obligations under this section; or

(12) process personal information for reasons of public interest in the area of public health, community health or population health, but solely to the extent that such processing is:

(A) subject to suitable and specific measures to safeguard the rights of the consumer whose personal information is being processed; and

(B) under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law.

(g) Exceptions. This [section] [subchapter] [chapter] does not apply to the following purposes or laws, as may be amended from time to time:

(1) protected health information under the Health Insurance Portability and Accountability Act of 1996. 42 U.S.C. 1320d et. seq., as amended;

(2) patient-identifying information for purposes of 42 U.S.C. 290dd-2, as amended;

(3) identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal information used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law;

(4) information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11101 et seq.;

(5) patient safety work product for purposes of the federal Patient Safety and Quality Improvement Act, 42 U.S.C. § 299b-21 et seq.;

(6) information derived from any of the health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to the Health Insurance Portability and Accountability Act of 1996.;

(7) information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as

information exempt under this subsection that is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996. or a program or a qualified service organization as defined by 42 U.S.C. § 290dd-2;

(8) information used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996.;

(9) the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.;

(10) personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act, Public Law 106-102;

(11) personal information collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994,18 U.S.C. § 2721 et seq.;

(12) personal information regulated by the federal Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g et seq.;

(13) personal information collected, processed, sold, or disclosed in compliance with the federal Farm Credit Act, 12 U.S.C. § 2001 et seq.;

(14) personal information regulated by the federal Children's Online Privacy Protection Act of 1998, 15 U.S.C. Secs. 6501 to 6506, if collected, processed, and maintained in compliance with that law; and

(15) data processed:

(A) in the course of an individual applying to, employed by, or acting as an agent or independent contractor of a data collector, data broker, or third party, to the extent that the data is collected and used within the context of that role;

(B) as the emergency contact information of an individual under this chapter used for emergency contact purposes; or

(C) that is necessary to retain to administer benefits for another individual relating to the individual under subdivision (B) of this subdivision (15) and used for the purposes of administering those benefits.

Subchapter 2. ~~Security Breach Notice Act~~ Data Security Breaches

* * *

§ 2436. NOTICE OF DATA BROKER SECURITY BREACH

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

(b) Notice of breach.

(1) Except as otherwise provided in subsection (d) of this section, any data broker shall notify the consumer that there has been a data broker security breach following discovery or notification to the data broker of the breach. Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) A data broker shall provide notice of a breach to the Attorney General as follows:

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

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

(iii) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (2)(A) shall not be disclosed to any person other than the authorized agent or representative of the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data broker.

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

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

(3) The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation or a national or Homeland Security investigation or jeopardize public safety or national or Homeland Security interests. In the event law enforcement makes the request for a delay in a manner other than in

writing, the data broker shall document such request contemporaneously in writing and include the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data broker in writing when the law enforcement agency no longer believes that notification may impede a law enforcement investigation or a national or Homeland Security investigation, or jeopardize public safety or national or Homeland Security interests. The data broker shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.

(4) The notice to a consumer required in subdivision (1) of this subsection shall be clear and conspicuous. A notice to a consumer of a security breach involving brokered personal information shall include a description of each of the following, if known to the data broker:

(A) the incident in general terms;

(B) the type of brokered personal information that was subject to the security breach;

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

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

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

(F) the approximate date of the data broker security breach.

(5) A data broker may provide notice of a security breach involving brokered personal information to a consumer by one or more of the following methods:

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

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

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

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

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

(c) Exception.

(1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data broker establishes that misuse of brokered personal information is not reasonably possible and the data broker provides notice of the determination that the misuse of the brokered personal information is not reasonably possible pursuant to the requirements of this subsection. If the data broker establishes that misuse of the brokered personal information is not reasonably possible, the data broker shall provide notice of its determination that misuse of the brokered personal information is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General. The data broker may designate its notice and detailed explanation to the Vermont Attorney General as a trade secret if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).

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

(d) Waiver. Any waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

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

Subchapter 4. Document Safe Destruction Act

§ 2445. SAFE DESTRUCTION OF DOCUMENTS CONTAINING ~~PERSONAL~~ PERSONALLY IDENTIFIABLE INFORMATION

(a) As used in this section:

(1) "Business" means 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 include the State, a State agency, or any political subdivision of the State. The term includes an entity that destroys records.

(2) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

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

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

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

(b) A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing ~~personal~~ personally identifiable information that is no longer to be retained by

the business by shredding, erasing, or otherwise modifying the ~~personal~~ personally identifiable information in those records to make it unreadable or indecipherable through any means for the purpose of:

(1) ensuring the security and confidentiality of customer ~~personal~~ personally identifiable information;

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

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

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

(d) This section does not apply to any of the following:

(1) any bank, credit union, or financial institution as defined under the federal ~~Gramm Leach Bliley law~~ Gramm-Leach-Bliley Act that is subject to

the regulation of the Office of the Comptroller of the Currency, the Federal Reserve, the National Credit Union Administration, the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision of the U.S. Department of the Treasury, or the Department of Financial Regulation and is subject to the privacy and security provisions of the ~~Gramm Leach Bliley~~ Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq.;

(2) any health insurer or health care facility that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996; or

(3) any consumer reporting agency that is subject to and in compliance with the Federal Credit Reporting Act, 15 U.S.C. § 1681 et seq., as amended.

(e) Enforcement.

(1) With respect to all businesses subject to this section, other than a person ~~or entity~~ licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this section~~,~~ and to prosecute, obtain, and impose remedies for a violation of this section, or any rules adopted pursuant to this section, and to adopt rules under

this chapter, as the Attorney General and State's Attorney have under chapter 63 of this title. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(2) With respect to a person ~~or entity~~ licensed or registered with the Department of Financial Regulation under Title 8 or this title to do business in this State, the Department of Financial Regulation shall have full authority to investigate potential violations of this chapter~~,~~ and to prosecute, obtain, and impose remedies for a violation of this chapter, or any rules or regulations made pursuant to this chapter, as the Department has under Title 8 and this title, or any other applicable law ~~or regulation~~.

Subchapter 5. Data Brokers

§ 2446. DATA BROKERS; 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) ~~if the data broker permits~~ the method for 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;

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

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

~~(E) 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;~~

~~(F)~~ 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, and sales activities~~, and opt-out policies~~ that are applicable to the brokered personal information of minors; and

~~(G)~~(D) 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~~ $100.00 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) A data broker that omits required information from its registration shall file an amendment to include the omitted information within five business days following notification of the omission and is liable to the State for a civil penalty of $1,000.00 per day for each day thereafter.

(d) A data broker that files materially incorrect information in its registration:

(1) is liable to the State for a civil penalty of $25,000.00; and

(2) if it fails to correct the false information within five business days after discovery or notification of the incorrect information, an additional civil penalty of $1,000.00 per day for each day thereafter that it fails to correct the information.

(e) 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.

* * *

§ 2448. DATA BROKERS; ADDITIONAL DUTIES

(a) Individual opt-out.

(1) A consumer may request that a data broker do any of the following:

(A) stop collecting the consumer's data;

(B) delete all data in its possession about the consumer; or

(C) stop selling the consumer's data.

(2) A data broker shall establish a simple procedure for consumers to submit such a request and shall comply with such a request from a consumer within 10 days of receiving such a request.

(3) A data broker shall clearly and conspicuously describe the opt-out procedure in its annual registration and on its website.

(b) General opt-out.

(1) A consumer may request that all data brokers registered with the State of Vermont honor an opt-out request by filing the request with the Secretary of State.

(2) The Secretary of State shall develop an online form to facilitate the general opt-out by a consumer and shall maintain a Data Broker Opt-Out List of consumers who have requested a general opt-out, with the specific type of opt-out.

(3) The Data Broker Opt-Out List shall contain the minimum amount of information necessary for a data broker to identify the specific consumer making the opt-out.

(4) Once every 31 days, any data broker registered with the State of Vermont shall review the Data Broker Opt-Out List in order to comply with the opt-out requests contained therein.

(5) Data contained in the Data Broker Opt-Out List shall not be used for any purpose other than to effectuate a consumer's opt-out request.

(c) Credentialing.

(1) A data broker shall maintain reasonable procedures designed to ensure that the brokered personal information it discloses is used for a legitimate and legal purpose.

(2) These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information shall be used for no other purpose.

(3) A data broker shall make a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user prior to furnishing such user brokered personal information.

(4) A data broker shall not furnish brokered personal information to any person if it has reasonable grounds for believing that the consumer report will not be used for a legitimate and legal purpose.

(d) Exemption. Nothing in this section applies to brokered personal information that is regulated as a consumer report pursuant to the Fair Credit Reporting Act, if the data broker is fully complying with the Fair Credit Reporting Act.

Subchapter 6. Biometric Information

§ 2449. PROTECTION OF BIOMETRIC INFORMATION

(a) Collection, use, and retention of biometric identifiers.

(1) A person shall not collect or retain a biometric identifier without first providing clear and conspicuous notice, obtaining consent, and providing a mechanism to prevent the subsequent use of a biometric identifier.

(2)(A) A person who collects or retains biometric identifiers shall establish a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within one year of the consumer's last interaction with the person, whichever occurs first.

(B) Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a person who possesses biometric identifiers or biometric information shall comply with its established retention schedule and destruction guidelines.

(3) A person providing notice pursuant to subdivision (1) or (5)(B) of this subsection shall include:

(A) a description of the biometric identifiers being collected or retained;

(B) the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, or used;

(C) the third parties to which the biometric identifier may be sold, leased, or otherwise disclosed to and the purpose of such disclosure; and

(D) the mechanism by which the consumer may prevent the subsequent use of the biometric identifier.

(4) A person who has collected or stored a consumer's biometric identifier may not use, sell, lease, or otherwise disclose the biometric identifier to another person for a specific purpose unless:

(A) consent has been obtained from the consumer for the specific purpose;

(B) it is necessary to provide a product or service subscribed to, requested, or expressly authorized by the consumer, and the person has notified the consumer of:

(i) the purpose; and

(ii) any third parties to which the identifier is disclosed to effectuate that purpose;

(C)(i) it is necessary to effect, administer, enforce, or complete a financial transaction that the consumer requested, initiated, or authorized;

(ii) the third party to whom the biometric identifier is disclosed maintains confidentiality of the biometric identifier and does not further disclose the biometric identifier except as otherwise permitted under this subdivision (4); and

(iii) the business has notified the consumer of any third parties to which the identifier is disclosed to effectuate that purpose; or

(D) it is required or expressly authorized by a federal or state statute, or court order.

(5)(A) Consent under subdivisions (1) or (4)(A) of this subsection (a) shall be opt-in and may be accomplished in writing by indicating assent through an electronic form, through a recording of verbal assent, or in any other way that is reasonably calculated to collect informed, confirmable consent.

(B) Where biometric information is collected in a physical, offline location and consent would be impossible to collect, consent is not necessary if the person collecting the information posts clear and conspicuous notice of the collection at a location likely to be seen by the consumer, provides notice on its website, and complies with all other requirements of this section.

(6) A person who possesses a biometric identifier of a consumer:

(A) shall take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the person;

(B) shall comply with the data security standard set forth in section 2447 of this title; and

(C) may retain the biometric identifier not longer than is reasonably necessary to:

(i) comply with a court order, statute, or public records retention schedule specified under federal, state, or local law;

(ii) protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and

(iii) provide the services for which the biometric identifier was collected or stored.

(7) A person who collects or stores a biometric identifier of a consumer or obtains a biometric identifier of a consumer from a third party pursuant to this section may not use or disclose it in a manner that is materially inconsistent with the terms under which the biometric identifier was originally provided without obtaining consent for the new terms of use or disclosure.

(8) Nothing in this section requires a person to provide notice and obtain consent to collect, use, or retain a biometric identifier where:

(A) the biometric identifier will be used solely to authenticate the consumer for the purpose of securing the goods or services provided by the business;

(B) the biometric identifier will not be leased or sold to any third party; and

(C) the biometric identifier will only be disclosed to a third party for the purpose of effectuating subdivision (8)(A) of this subsection (a), and the third party is contractually obligated to maintain the confidentiality of the biometric identifier and to not further disclose the biometric identifier.

(b) Enforcement.

(1)(A) The Attorney General and State's Attorney shall have authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(B) In determining appropriate civil penalties, the courts shall consider each instance in which a person violates this subchapter with respect to each consumer as a separate violation and shall base civil penalties on the

seriousness of the violation, the size and sophistication of the business violating the subchapter, and the business's history of respecting or failing to respect the privacy of consumers, with maximum penalties imposed where appropriate.

(C) A person who possesses a biometric identifier of a consumer that was not acquired in accordance with the requirements of this subchapter as of the effective date of this law shall either obtain consent or delete the biometric information within 180 days after enactment of this law or shall be liable for $10,000.00 per day thereafter until the business has complied with this subdivision (1)(c).

(2) A consumer aggrieved by a violation of this subchapter or rules adopted under this subchapter may bring an action in Superior Court for the consumer's damages, injunctive relief, punitive damages, and reasonable costs and attorney's fees. The court, in addition, may issue an award for the greater of the consumer's actual damages or $1,000.00 a negligent violation or $5,000.00 for a willful or reckless violation.

(c) Exclusions. Nothing in this chapter expands or limits the authority of a law enforcement officer acting within the scope of the officer's authority, including the authority of a State law enforcement officer in executing lawful searches and seizures.

Sec. 2. EFFECTIVE DATE

This act shall take effect on July 1, 2023.

(Committee vote: _____)

_____

Representative _____

FOR THE COMMITTEE