H.211

Introduced by Representatives Priestley of Bradford, Marcotte of Coventry, Arsenault of Williston, Austin of Colchester, Berbeco of Winooski, Bos-Lun of Westminster, Bosch of Clarendon, Boutin of Barre City, Boyden of Cambridge, Brown of Richmond, Burke of Brattleboro, Burrows of West Windsor, Campbell of St. Johnsbury, Carris-Duncan of Whitingham, Casey of Montpelier, Chapin of East Montpelier, Cina of Burlington, Cole of Hartford, Cordes of Bristol, Donahue of Northfield, Duke of Burlington, Eastes of Guilford, Goldman of Rockingham, Graning of Jericho, Greer of Bennington, Harple of Glover, Headrick of Burlington, Holcombe of Norwich, Krasnow of South Burlington, Lalley of Shelburne, Lipsky of Stowe, Masland of Thetford, McCann of Montpelier, McGill of Bridport, Micklus of Milton, Mihaly of Calais, Minier of South Burlington, Mrowicki of Putney, Nugent of South Burlington, O'Brien of Tunbridge, Ode of Burlington, Olson of Starksboro, Pezzo of Colchester, Pouech of Hinesburg, Rachelson of Burlington, Satcowitz of Randolph, Sibilia of Dover, Stevens of Waterbury, Surprenant of Barnard, Tomlinson of Winooski,

Torre of Moretown, Waszazak of Barre City, and White of Bethel

Referred to Committee on

Date:

Subject: Commerce and trade; protection of personal information; data brokers

Statement of purpose of bill as introduced: This bill proposes to add various provisions to Vermont's laws that protect the personal information of its residents, including requiring data brokers to provide notice of security breaches, to certify that the personal information it discloses will be used for a legitimate purpose, and to delete the personal information of consumers who make such a request through the use of an accessible deletion mechanism.

An act relating to data brokers and personal information

It is hereby enacted by the General Assembly of the State of Vermont:

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) "Authorized agent" means:

(A) a person designated by a consumer to act on the consumer's behalf;

(B) a parent or legal guardian that acts on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility; or

(C) a guardian or conservator that acts on behalf of a consumer that is subject to a guardianship, conservatorship, or other protective arrangement.

(2)(A) "Biometric data" means data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including:

(i) iris or retina scans;

(ii) fingerprints;

(iii) facial or hand mapping, geometry, or templates;

(iv) vein patterns;

(v) voice prints; and

(vi) gait or personally identifying physical movement or patterns.

(B) "Biometric data" does not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

(iii) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(3)(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;

(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) phone number; or

(x) 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)~~(4) "Business" means a controller, a consumer health data controller, a processor, or 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)~~(5) "Consumer" means an individual residing in this State.

(6) "Consumer health data controller" means any controller that, alone or jointly with others, determines the purpose and means of processing consumer health data.

(7) "Controller" means a person who, alone or jointly with others, determines the purpose and means of processing personal data.

~~(4)~~(8)(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 within the last five calendar years;

(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)~~(9)(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)~~(10) "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.

~~(7)~~(11) "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.

~~(8)~~(12) "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)~~(13) "Login credentials" means a consumer's user name or ~~e-mail~~ email address, in combination with a password or an answer to a security question, that together permit access to an online account.

~~(10)~~(14)(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;

(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.

(15) "Precise geolocation" means information derived from technology that can precisely and accurately identify the specific location of a consumer within a radius of 1,850 feet.

(16) "Processor" means a person who processes personal data on behalf of a controller.

~~(11)~~(17) "Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(12)~~(18) "Redaction" means the rendering of data so that the data are unreadable or are truncated so that ~~no~~ not more than the last four digits of the identification number are accessible as part of the data.

~~(13)~~(19)(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.

* * *

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

§ 2435. NOTICE OF SECURITY BREACHES

* * *

(h) Enforcement.

(1) ~~With respect to all data collectors and other entities subject to this subchapter, 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 subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this subchapter as the Attorney General and State's Attorney~~

~~have under chapter 63 of this title. With respect to a controller or processor~~ other than a controller or processor licensed or registered with the Department of Financial Regulation under Title 8 or this title, 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. 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.

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

* * *

§ 2436. NOTICE OF DATA BROKER SECURITY BREACHES

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

(b) Notice of breach to consumers.

(1) Except as otherwise provided in subsection (c) of this section, a data broker shall, following discovery or notification to the data broker of a security breach affecting a consumer, notify the consumer that there has been a data broker security 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 subdivisions (3) and (4) of this subsection (b), after the data broker's discovery of the security breach.

(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, without the consent of the data broker, 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.

(B)(i) When the data broker provides notice of the breach pursuant to subdivision (1) of this subsection, 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 the Attorney General and 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 the 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 subsection 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 categories 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 two 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 email 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;

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

(D) notice by publication in a newspaper of statewide circulation in the event the data broker cannot effectuate notice by any other means.

(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 Attorney General. The data broker may designate its notice and detailed explanation to the 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.

(1) With respect to a controller or processor other than a controller or processor licensed or registered with the Department of Financial Regulation under Title 8 or this title, 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. 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.

~~(2) With respect to a controller or processor that is licensed or registered~~ with the Department of Financial Regulation under Title 8 or this title, the Department of Financial Regulation 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 Title 8 or this title or any other applicable law or regulation.

* * *

Subchapter 5. Data Brokers

§ 2446. DATA BROKERS; ANNUAL REGISTRATION

(a) Registration. 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~~ pay a registration fee in an amount determined by the Secretary of State which shall:

(A) not exceed the reasonable costs of:

(i) establishing and maintaining the informational website set forth in subsection (f) of this section; and

(ii) establishing, maintaining, and providing access to the ~~accessible deletion mechanism set forth in section 2446b of this title; and~~

(B) be deposited by the Secretary of State into the Data Brokers Registry Fund established in section 2446b of this title; and

(3) provide the following information to the Secretary of State:

(A) the name and primary physical, ~~e-mail~~ email, phone number, and ~~Internet~~ internet addresses of the data broker;

(B) 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~~ an authorized agent 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;

(E) 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~~

(G) whether the data broker collects:

(i) precise geolocation of consumers;

(ii) reproductive health care data of consumers;

(iii) Social Security numbers of consumers;

(iv) driver's license information of consumers;

(v) biometric data of consumers;

(vi) immigration status of consumers;

(vii) sexual orientation of consumers; or

(viii) union membership status of consumers;

(H) beginning on January 1, 2031, whether the data broker has undergone an audit pursuant to subsection 2449a(e) of this title and if so, the most recent year that the data broker has submitted a report resulting from the audit to the Secretary of State;

(I) beginning on January 1, 2029, the following annual metrics pursuant to section 2449a of this title:

(i) the number of deletion requests received;

(ii) the number of deletion requests processed;

(iii) the number of deletion requests denied because the consumer request cannot be verified; and

(iv) the number of deletion requests denied because retention of the consumer's brokered personal information is required by law; and

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

(b) Penalties. 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.

(1) A data broker that fails to register as required by subsection (a) of this section is liable to the State for:

(A) an administrative fine of $200.00 for each day the data broker fails to register;

(B) an amount equal to the fees that were due during the period the data broker failed to register; and

(C) any reasonable costs incurred by the State in the investigation and administration of the action as the court deems appropriate.

(2) A data broker that fails to provide all registration information required in subdivision (a)(3) of this section shall file an amendment that includes any omitted information not later than 30 days after receiving notification of the omission from the Secretary of State and is liable to the State for a civil penalty of $1,000.00 per day for each day thereafter that the data broker does not file an amendment providing the omitted information.

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

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

(B) shall correct the incorrect information not later than 30 days after notification of the incorrect information, and, if it fails to correct the information, the data broker shall be liable for an additional civil penalty of $1,000.00 per day for each day the data broker fails to correct the information.

(4) All penalties, fines, fees, and expenses recovered in an action pursuant to this section shall be deposited in the Data Brokers Registry Fund.

(c) Enforcement. The Attorney General and the Secretary of State 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.

(d) Public web page. The Secretary of State shall create a publicly accessible page on its website where it lists the registration information

provided by data brokers pursuant to this section and the accessible deletion mechanism set forth in section 2446a of this title.

§ 2446a. ACCESSIBLE DELETION MECHANISM

(a) Creation of mechanism. On or before January 1, 2028, the Secretary of State shall establish an accessible deletion mechanism that:

(1) implements and maintains reasonable security procedures and practices, including administrative, physical, and technical safeguards appropriate to the nature of the information and the purposes for which the brokered personal information will be used and to protect a consumer's brokered personal information from unauthorized use, disclosure, access, destruction, or modification;

(2) allows a consumer, through a single verifiable consumer request, to request that every data broker that maintains any brokered personal information about the consumer delete the brokered personal information;

(3) allows a consumer to selectively exclude specific data brokers from a request made under subdivision (2) of this subsection;

(4) allows a consumer to alter a previous request made pursuant to subdivision (2) of this subsection after at least 45 days have passed since the consumer last made a request;

(5) allows a consumer to request the deletion of all brokered personal information related to that consumer all at once through a single deletion request;

(6) permits a consumer to securely submit information in one or more privacy-protecting ways, as determined by the Secretary of State, to aid in the deletion request;

(7) allows a data broker registered with the Secretary of State to determine whether a consumer has submitted a verifiable request to delete the brokered personal information related to that consumer as described in subdivision (2) of this subsection;

(8) does not allow the disclosure of any additional brokered personal information of a consumer when the data broker accesses the accessible deletion mechanism, unless otherwise specified in this subchapter;

(9) allows a consumer to make a request described in subdivision (2) of this subsection using a website operated by the Secretary of State;

(10) does not charge a consumer to make a request described in subdivision (2) of this subsection;

(11) is readily accessible and usable by consumers with disabilities;

(12) supports the ability of a consumer's authorized agents to aid in the deletion request;

(13) allows the consumer or their authorized agent to verify the status of the consumer's deletion request; and

(14) provides a description of the following:

(A) the deletion permitted by this section;

(B) the process for submitting a deletion request pursuant to this section; and

(C) examples of the types of information that may be deleted.

(b) Data broker access.

(1) Beginning on August 1, 2028, a data broker shall access the accessible deletion mechanism established in subsection (a) of this section at least once every 45 days and shall:

(A) process all verifiable deletion requests the data broker has received from consumers in the previous 45 days and delete such brokered personal information;

(B) process a request as an opt-out of the sale or sharing of the consumer's brokered personal information;

(C) direct all service providers and contractors associated with the data broker to:

(i) delete all brokered personal information related to a consumer who has made a verifiable deletion request; and

(ii) process a request as an opt-out of the sale or sharing of the consumer's brokered personal information; and

(D) not use or disclose any information submitted by a consumer through the accessible deletion mechanism for any other purpose besides the authority provided in this subsection (b), including for marketing purposes.

(2) A data broker may deny a consumer's request to delete a consumer's brokered personal information made pursuant to this section if retention of the consumer's brokered personal information is required by law.

(3) The Secretary of State may charge an access fee to a data broker to use the accessible deletion mechanism that does not exceed the reasonable costs of providing access.

(4) Any fees collected pursuant to subdivision (3) of this subsection shall be deposited into the Data Brokers Registry Fund.

(c) Continuing obligation to consumers. Beginning on August 1, 2028, once a data broker has processed a verifiable consumer request to delete a consumer's brokered personal information, the data broker shall:

(1) delete all brokered personal information of the consumer at least once every 45 days unless:

(A) the consumer alters the consumer's decision pursuant to subdivision (a)(4) of this section; or

(B) retention of the consumer's brokered personal information is required by law; and

(2) not sell or share new brokered personal information of the consumer unless the consumer expressly requests otherwise in writing;

(d) Audits.

(1) A data broker shall undergo an audit by an independent third party to determine compliance with this section at least once every three years, with the first audit taking place on or before December 31, 2030.

(2) For an audit completed pursuant to subdivision (1) of this subsection, the data broker shall submit the report resulting from the audit and any related materials to the Secretary of State within five business days of a written request from the Secretary of State.

(3) A data broker shall maintain all reports and materials resulting from audits conducted pursuant to this subsection for at least six years.

(e) Rules. The Secretary of State may adopt rules to implement the provisions of this subchapter, except it shall not be permitted to create a rule that establishes a new fee that is not authorized in this section.

(f) Penalties.

(1) A data broker that fails to comply with the requirements of this section is liable to the State for:

(A) an administrative fine of $200.00 per day for each deletion request the data broker fails to complete as required by subsection (b) of this section; and

(B) reasonable expenses incurred by the State in the investigation and administration of the action.

(2) All penalties, fines, fees, and expenses recovered in an action pursuant to subdivision (1) of this subsection shall be deposited in the Data Brokers Registry Fund.

§ 2446b. DATA BROKERS REGISTRY FUND

There is established the Data Brokers Registry Fund within the State Treasury. The Fund shall be administered by the Secretary of State. All moneys collected or received by the Secretary of State and the Attorney General pursuant to this subchapter shall be deposited into the Fund and shall be made available for expenditure by the Secretary of State upon appropriation by the General Assembly to offset the following costs:

(1) the reasonable costs of establishing and maintaining the informational website as set forth in subsection 2446(d) of this title;

(2) the costs incurred by State courts and the Secretary of State in connection with enforcing this subchapter; and

(3) the reasonable costs of establishing, maintaining, and providing access to the accessible deletion mechanism described in section 2446a of this title.

§ 2446c. CREDENTIALING

(a) 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.

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

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

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

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

* * *

Sec. 3. EFFECTIVE DATE

~~This act shall take effect on July 1, 2025.~~

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) "Authorized agent" means:

(A) a person designated by a consumer to act on the consumer's behalf;

(B) a parent or legal guardian that acts on behalf of the parent's child or on behalf of a child for whom the guardian has legal responsibility; or

(C) a guardian or conservator that acts on behalf of a consumer that is subject to a guardianship, conservatorship, or other protective arrangement.

(2)(A) "Biometric data" means that data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics can be used to identify an individual, including:

(i) iris or retina scans;

(ii) fingerprints;

(iii) facial or hand mapping, geometry, or templates;

(iv) vein patterns;

(v) voice prints; and

(vi) gait or personally identifying physical movement or patterns.

(B) "Biometric data" does not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

(iii) any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

(3)(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;~~

~~*(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*~~ *any information, including derived data and unique identifiers, that is linked or reasonably linkable, alone or in combination with other information, to an identified or identifiable individual or to a device that identifies, is linked to, or is reasonably linkable to one or more identified or identifiable individuals in a household.*

(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)*~~*(4) "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)~~(5) "Consumer" means an individual residing in this State.

~~(4)~~(6)(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~~ As used in this subdivision (6), "direct relationship" means that a consumer has intentionally interacted with a business for the purpose of accessing, purchasing, using, requesting, or obtaining information about the business's products or services. A consumer does not have a direct relationship with a business if the purpose of the consumer's engagement is to exercise a consumer right or for the business to verify the consumer's identity. A business does not have a direct relationship with a consumer simply because the business collects brokered personal

information directly from the consumer; the consumer must intend to interact with the business. A business is still a data broker and does not have a direct relationship with a consumer as to the brokered personal information the business sells about the consumer that it collected outside of a first-party interaction with the consumer.

~~*(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)*~~*(C) 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)(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.*

~~*(7)*~~*(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)(A) "GenAI system" means an artificial intelligence system that can generate derived synthetic content, including text, images, video, and audio, that emulates the structure and characteristics of the system's training data.

(B) As used in subdivision (A) of this subdivision (9), "artificial intelligence system" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer

from the input it receives how to generate outputs that can influence physical or virtual environments.

(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~~ email 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, subject to the exception in subdivision (C) of this subdivision (13):

(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;*

(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~~ include publicly available information ~~that is lawfully made available to the general public from federal, State, or local government records~~.

(C) "Personally identifiable information" does not require a consumer's first name or first initial and last name if any of the data elements contained in subdivisions (A)(i)–(vii) of this subdivision (13) is sufficient to perform or attempt to perform identity theft against the consumer.

(14) "Precise geolocation" means information derived from technology that can precisely and accurately identify the specific location of a consumer within a radius of 1,850 feet.

(15) "Processor" means a person who performs any operation or set of operations, whether by manual or automated means, on brokered personal information or on sets of brokered personal information, such as the collection, use, storage, disclosure, analysis, deletion, or modification of brokered personal information on behalf of a business.

(16)(A) "Publicly available information" means information that:

(i) is made available:

(I) through federal, state, or local government records; or

(II) to the general public from widely distributed media; or

(ii) a data broker has a reasonable basis to believe that the consumer has lawfully made available to the general public.

(B) "Publicly available information" does not include:

(i) biometric data collected by a business about a consumer without the consumer's knowledge;

(ii) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available website either in exchange for payment or free of charge;

(iii) information that is made available for sale;

(iv) an inference about a consumer that is generated from the information described in subdivision (ii) or (iii) of this subdivision (16)(B);

(v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

(vi) brokered personal information that is created through the combination of brokered personal information with publicly available information;

(vii) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains;

(viii) information provided by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has maintained a reasonable expectation of privacy in the information, such as by restricting the information to a specific audience; or

(ix) intimate images, authentic or computer-generated, known to be nonconsensual.

(B) "Publicly available information" does not include:

(i) biometric data collected by a business about a consumer without the consumer's knowledge;

(ii) any obscene visual depiction, as defined in 18 U.S.C. § 1460;

(iii) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains; or

(iv) intimate images, authentic or computer-generated, known to be nonconsensual.

~~(11)~~(17) "Record" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

~~(12)~~(18) "Redaction" means the rendering of data so that the data are unreadable or are truncated so that ~~no~~ not more than the last four digits of the identification number are accessible as part of the data.

(19)(A) "Sale" means the exchange of a consumer's brokered personal information by the data broker to a third party for monetary or other valuable consideration.

(B) "Sale" does not include:

(i) the disclosure of brokered personal information to a processor that processes the brokered personal information on behalf of the data broker;

(ii) the disclosure of brokered personal information to a third party for purposes of providing a product or service requested by the consumer;

(iii) the disclosure or transfer of brokered personal information to an affiliate of the data broker;

(iv) the disclosure, with the consumer's consent, of brokered personal information where the consumer directs the data broker to disclose the brokered personal information or intentionally uses the data broker to interact with a third party;

(v) the disclosure of publicly available information; or

(vi) the disclosure or transfer of brokered personal information to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction, in which the third party assumes control of all or part of the data broker's assets.

(C) As used in subdivision (B) of this subdivision (19), "affiliate" means a legal entity that shares common branding with another legal entity or controls, is controlled by, or is under common control with another legal entity.

(D) As used in subdivision (C) of this subdivision (19), "control" or "controlled" means:

(i) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company;

(ii) control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or

(iii) the power to exercise controlling influence over the management of a company.

~~(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~~ are 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.

§ 2431. ACQUISITION AND DISCLOSURE 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~~ email fraud; or

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

(b) Disclosure. A data broker shall:

(1) maintain procedures that require prospective users of the data broker's brokered personal information to identify themselves, state the

purposes for which the information is sought, and certify that the information shall be used for no other purpose;

(2) prior to disclosing brokered personal information to a prospective user and pursuant to subdivision (1) of this subsection:

(A) make a reasonable effort to verify the identity of the prospective user of the information; and

(B) review the user's stated purposes for which the information is sought; and

(3) not disclose brokered personal information to a prospective user if the data broker has reasonable grounds for believing that the information will be used to violate State or federal law or will not be used for the purposes stated by the user pursuant to this subsection.

(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 2. Security ~~Breach Notice Act~~ Breaches

§ 2435. NOTICE OF SECURITY BREACHES

* * *

(b) Notice of breach.

* * *

(6) A data collector may provide notice of a security breach involving personally identifiable information to a consumer by one or more of the following methods:

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

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

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

(I) the data collector'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

(iii) telephonic notice, for those consumers for whom the data collector has a valid phone number, provided that the telephonic contact is made directly with each affected consumer and not through a prerecorded message and further provided that the data collector makes not less than five attempts to contact the consumer for a live conversation before the data collector may leave a voicemail providing information about the breach.

* * *

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

(d) Exception to notice requirement.

(1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personally identifiable information or login credentials is not reasonably possible and the data collector provides notice of the determination that the misuse of the personally identifiable information or login credentials is not reasonably

possible pursuant to the requirements of this subsection. If the data collector establishes that misuse of the personally identifiable information or login credentials is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personally identifiable information or login credentials is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the Department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont Attorney General or the Department of Financial Regulation as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).

* * *

(e) HIPAA compliance. A data collector that is subject to the privacy, security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health Insurance Portability and Accountability Act, P.L. 104-191 (1996) is deemed to be in compliance with this subchapter if the data collector:

(1) ~~the data collector~~ experiences a security breach that is limited to personally identifiable information specified in subdivision 2430(10)(A)(vii) of this chapter; ~~and~~

(2) ~~the data collector~~ provides notice to affected consumers pursuant to the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart D; and

(3) provides notice to the Attorney General or to the Department of Financial Regulation pursuant to subdivision (b)(3)(B) of this section along with a written certification of compliance with 45 C.F.R. Part 164, Subpart D.

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

(g) Financial institutions. Except as provided in subdivision (3) of this subsection, a financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to an interagency guidance, shall be exempt from this section:

* * *

(h) Enforcement.

* * *

(2) With respect to a data collector that is a person or entity ~~licensed or registered with~~ regulated by the Department of Financial Regulation under Title 8 or this title, the Department of Financial Regulation shall have the full authority to investigate potential violations of this subchapter and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations adopted pursuant to this subchapter, as the

Department has under Title 8 or this title or any other applicable law or regulation.

* * *

§ 2436. NOTICE OF DATA BROKER SECURITY BREACHES

(a) Short title and definitions.

(1) This section shall be known as the "Data Broker Security Breach Notice Act."

(2)(A) As used in this section, "data broker security breach" means an unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one instance 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.

(b) Notice of breach.

(1) Except as otherwise provided in subsection (c) of this section, a data broker shall, following discovery or notification to the data broker of a security breach affecting a consumer, notify the consumer that there has been a data broker security 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 subdivisions (3) and (4) of this subsection (b), after the data broker's discovery of the security breach.

(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, without the consent of the data broker, 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.

(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 the Attorney General and 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 the 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 subsection 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 categories 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 two 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 email 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;

(C) telephonic notice, for those consumers for whom the data broker has a valid phone number, provided that the telephonic contact is made directly with each affected consumer and not through a prerecorded message and further provided that the data broker makes not less than five attempts to contact the consumer for a live conversation before the data broker may leave a voicemail providing information about the breach; or

(D) notice by publication in a newspaper of statewide circulation in the event the data broker cannot effectuate notice by any other means.

(c) Exception to notice requirement.

(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 Attorney General. The data broker may designate its notice and detailed explanation to the 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). Upon review of the data broker's notice and detailed explanation, the Attorney General may request additional information from the data broker and may accept or reject the data broker's determination. If the Attorney General rejects the data broker's determination, the data broker shall provide notice of the security breach pursuant to subsection (b) of this section.

(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.

(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, and bring civil actions as provided under chapter 63, subchapter 1 of this title.

* * *

Subchapter 3A. Student Privacy

* * *

§ 2443f. ENFORCEMENT

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

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

* * *

Subchapter 5. Data Brokers

§ 2446. DATA BROKERS; ANNUAL REGISTRATION

(a) ~~Annually, on or before January 31 following a year in which a~~ Registration. A person ~~meets~~, not more than 30 days after meeting the definition of a data broker ~~as provided in section 2430 of this title, a data broker~~ and then once annually thereafter on or before July 1 of each year, shall:

(1) register with the Secretary of State as a data broker;

(2) pay a registration fee of ~~$100.00~~ $900.00;

(3) maintain a bond in the amount of $20,000.00 that shall run to the State for any liability arising under this subchapter, provided that the action on the bond is brought within two years after accrual of the cause of action; ~~and~~

(4) provide the following information about the data broker to the Secretary of State:

~~*(A) the name and primary physical, e-mail email, phone number, and Internet internet addresses of the data broker;*~~

(A) the name and primary physical, ~~e-mail, and Internet addresses~~ email, and internet addresses and phone number of the data broker;

(B) ~~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;*~~

~~*(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)*~~*(C) pursuant to section 2436 of this chapter, 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)*~~*(D) 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*~~

~~*(G)*~~*(E) whether the data broker:*

(i) collects the:

(I) precise geolocation of consumers;

(II) reproductive health care data of consumers;

(III) biometric data of consumers;

(IV) immigration status of consumers;

(V) sexual orientation of consumers;

(VI) union membership status of consumers;

(VII) name, date of birth, zip code, email address, or phone number of consumers;

(VIII) account login or account number of consumers in combination with any required security code, access code, or password that would permit access to a consumer's account with a third party;

(IX) driver's license number, State identification card number, Social Security number, passport number, military identification number, or other unique identification number of consumers issued on a government document commonly used to verify the identity of a specific individual; or

(X) mobile advertising identification number, connected television identification number, or vehicle identification number of consumers; and

(ii) in the past year has shared or sold consumers' data to:

(I) a foreign actor;

(II) the federal government;

(III) to other state or local governments;

(IV) to law enforcement, unless the data was shared pursuant to a subpoena or other court order; or

~~(V) to a developer of a GenAI system or model;~~

(ii) in the past year, has shared consumers' data with or sold consumers' data to:

(I) a foreign actor;

(II) the federal government;

(III) other state or local governments;

(IV) law enforcement, unless the data was shared pursuant to a subpoena or other court order; or

(V) a developer of a GenAI system or model;

(F) the three most common types of personal information that the data broker collects, if the data broker does not collect the information set forth in subdivisions (E)(i)(VII) and (E)(i)(IX) of this subdivision (4);

(G) an electronic copy of the data broker's:

(i) bond, pursuant to subdivision (3) of this subsection (a); and

(ii) current privacy policy;

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

(I) the URL of a page on the data broker's website that:

(i) ~~pursuant to subsection (c) of this section~~ if the data broker permits deletion, allows a consumer to request that a data broker delete the brokered personal information of the consumer; and

(ii) informs consumers about the rights of consumers to opt out of the collection of the consumer's brokered personal information, including:

(I) whether the data broker permits a consumer to opt out of its databases, or opt out of certain sales of data;

(II) the procedure for requesting an opt-out;

(III) if the opt-out applies to only certain activities or sales, which activities or sales it applies to;

(IV) whether the data broker permits a consumer to authorize an authorized agent to perform the opt out on the consumer's behalf; and

(V) the data collection, databases, or sales activities from which a consumer may not opt out; and

(J) whether and to what extent the data broker or any of its subsidiaries is regulated by the Fair Credit Reporting Act; and

(5) amend an existing registration the data broker has with the Secretary of State if required by this section or by the State upon the payment of an administrative fee of $100.00.

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

~~(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.*~~

(1) A data broker that fails to register as required by subsection (a) of this section is liable to the State for:

(A) an administrative fine of $200.00 for each day the data broker fails to register;

(B) an amount equal to the fees that were due during the period the data broker failed to register; and

(C) any reasonable costs incurred by the State in the investigation and administration of the action as the court deems appropriate.

(2) A data broker that fails to provide all registration information required in subdivision (a)(4) of this section shall file an amendment pursuant to subdivision (a)(5) of this section that includes any omitted information not later than 30 days after discovering or receiving notification of the omission and is liable to the State for a civil penalty of $1,000.00 per day for each day thereafter that the data broker does not file an amendment providing the omitted information.

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

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

(B) correct the materially incorrect information by filing an amendment pursuant to subdivision (a)(5) of this section not later than 30 days after discovering or receiving notification of the incorrect information, and, if it fails to correct the information, the data broker shall be liable for an additional civil penalty of $1,000.00 per day for each day the data broker fails to correct the information.

~~*(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.*~~ *Deleting brokered personal information.*

(1) A data broker shall:

(A) maintain a conspicuous page on its website where a consumer or an authorized agent of a consumer has the ability to request that the data broker delete the consumer's brokered personal information free of charge;

(B) delete the consumer's brokered personal information not later than 30 days after the consumer makes a deletion request pursuant to subdivision (A) of this subdivision (1), unless the data broker denies the request pursuant to subdivision (3) of this subsection (c); and

(C) notify the consumer that the consumer's brokered personal information has been deleted not later than five days after the information has been deleted.

(2) The web page maintained by a data broker pursuant to subdivision (1) of this subsection shall:

(A) describe how a consumer may exercise the consumer's right to delete the consumer's brokered personal information, including the process for the consumer to appeal the denial of a deletion request pursuant to subdivision (5) of this subsection (c);

(B) adhere to the accessibility and usability guidelines recommended pursuant to 42 U.S.C. chapter 126 (the Americans with Disabilities Act) and 29 U.S.C. § 794d (section 508 of the Rehabilitation Act of 1973); and

(C) employ design practices that facilitate easy comprehension and navigation for all users and that are free of any dark patterns.

(3) A data broker may deny a consumer's request to delete the consumer's brokered personal information pursuant to subdivision (1) of this subsection to the extent that:

(A) the retention of the consumer's brokered personal information is required by law or is required to comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, state, municipal, or other governmental authority; or

(B) the brokered personal information is:

(i) used by a consumer reporting agency to furnish a consumer report pursuant to the Fair Credit Reporting Act;

(ii) necessary to investigate, establish, exercise, prepare for, or defend a legal claim;

(iii) strictly necessary to fulfill a specific legal requirement on behalf of a business to which the data broker is bound by a written contract to fulfill that legal requirement;

(iv) used to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or to preserve the technical integrity or physical security of systems or investigate, report, or prosecute those responsible for any such action;

(v) data that is collected or used for purposes of the National Precursor Log Exchange, or its equivalent, pursuant to State or federal law;

(vi) processed solely in the data broker's capacity as a processor to a business with which the consumer has a direct relationship, as that term is defined in subdivision 2430(a)(6)(B) of this chapter; or

(vii) used in connection with underwriting, issuing title insurance, or completing an appraisal.

(4) Brokered personal information retained pursuant to subdivision (3) of this subsection shall be:

(A) separated or segregated from data used for any other purpose;

(B) deleted immediately upon the expiration of the legal or contractual requirement; and

(C) not used, sold, shared, or processed for any other purpose.

(5) A data broker shall provide the consumer with the ability to appeal an instance where the data broker denies the consumer's request to delete the consumer's brokered personal information pursuant to subdivision (3) of this subsection (c) with a process that:

(A) gives the consumer 45 days after the consumer receives notice that the data broker has denied the deletion request to initiate the appeal;

(B) is conspicuously available to the consumer;

(C) is similar to the manner in which a consumer submits a deletion request pursuant to subdivision (1) of this subsection (c);

(D) requires the data broker to approve or deny the appeal within 45 days after the date on which the data broker received the appeal and to notify the consumer in writing of the data broker's decision and the reasons for the decision; and

(E) requires a data broker that denies a consumer's appeal to provide information that enables the consumer to contact the Attorney General to submit a complaint.

(6)(A) If a data broker is unable to authenticate a deletion request made pursuant to subdivision (1) of this subsection (c), the data broker shall not be required to comply with the request and shall provide notice to the consumer or the consumer's agent that the data broker is unable to authenticate the

~~request. The data broker shall provide the consumer with the additional information the data broker requires in order to authenticate the consumer.~~

~~(B) As used in this subdivision (6), "authenticate" means the use of reasonable measures to determine whether a deletion request is being made by, or on behalf of, the consumer who is entitled to exercise that request with respect to the brokered personal information at issue.~~

~~(b)~~(c) ~~Consumer rights web page. The Secretary of State shall create and maintain~~ a publicly accessible page on its website that provides consumers with the following:

(1) a downloadable spreadsheet of data brokers that have registered with the State along with the information a data broker provides during registration pursuant to subsection (a) of this section;

(2) the URL of a page on each registered data broker's website that allows a consumer to delete the consumer's brokered personal information, pursuant to subdivision (c)(1) of this section; and

(3) any additional information about the rights consumers have ~~pursuant to this subchapter.~~

(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.~~ Consumer rights web page. The Secretary of

State shall create and maintain a publicly accessible page on its website that provides consumers with the following:

(1) a downloadable spreadsheet of data brokers that have registered with the State along with the information a data broker provides during registration pursuant to subsection (a) of this section; and

(2) any additional information about the rights consumers have pursuant to this subchapter.

~~(c)~~*(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 section and to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided under chapter 63, subchapter 1 of this title.

(e) Definitions. As used in this subchapter, "consumer" means an individual residing in this State and does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit organization, or government agency whose communications or transactions with the data broker occur solely within the context of that individual's role

with the company, partnership, sole proprietorship, nonprofit organization, or government agency.

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

* * *

(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~~ section 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. 2. STUDY OF ACCESSIBLE DELETION MECHANISM; REPORT; ~~APPROPRIATION~~

(a) The Secretary of State shall study the feasibility of:

(1) establishing an accessible deletion mechanism that:

(A) implements and maintains reasonable security procedures and practices, including administrative, physical, and technical safeguards appropriate to the nature of the information and the purposes for which brokered personal information will be used and to protect a consumer's

brokered personal information from unauthorized use, disclosure, access, destruction, or modification;

(B) allows a consumer, through a single verifiable consumer request, to request that every data broker that maintains any brokered personal information about the consumer delete the brokered personal information;

(C) allows a consumer to selectively exclude specific data brokers from a request made under subdivision (B) of this subdivision (1);

(D) allows a consumer to alter a previous request made pursuant to subdivision (B) of this subdivision (1) after at least 45 days have passed since the consumer last made a request;

(E) allows a consumer to request the deletion of all brokered personal information related to that consumer all at once through a single deletion request;

(F) permits a consumer to securely submit information in one or more privacy-protecting ways to aid in the deletion request;

(G) allows a data broker registered with the Secretary of State to determine whether a consumer has submitted a verifiable request to delete the brokered personal information related to that consumer as described in subdivision (B) of this subdivision (1);

(H) does not allow the disclosure of any additional brokered personal information of a consumer when the data broker accesses the accessible deletion mechanism, unless otherwise specified in this subchapter;

(I) allows a consumer to make a request described in subdivision (B) of this subdivision (1) using a website operated by the Secretary of State;

(J) does not charge a consumer to make a request described in subdivision (B) of this subdivision (1);

(K) is readily accessible and usable by consumers with disabilities;

(L) supports the ability of a consumer's authorized agents to aid in the deletion request;

(M) allows the consumer or their authorized agent to verify the status of the consumer's deletion request; and

(N) provides a description of the following:

(i) the deletion permitted by this section;

(ii) the process for submitting a deletion request pursuant to this section; and

(iii) examples of the types of information that may be deleted; and

(2) utilizing a data broker's registry fund to hold monies received for transactions pursuant to 9 V.S.A. § 2446 and to disburse for the purpose of supporting and offsetting the costs of the accessible deletion mechanism set forth in subdivision (1) of this subsection.

(b) Reporting. The Secretary of State shall, based on the study set forth in subsection (a) of this section, submit to the House Committee on Commerce and Economic Development and the Senate Committee on Economic Development, Housing and General Affairs an interim report on or before December 1, 2027, and a final report on or before December 1, 2028, including its findings and any proposed legislation for the General Assembly's consideration. The interim report shall provide the General Assembly with any recommended actions to pursue in the 2028 legislative session.

~~*(c) Appropriation. In fiscal year 2027, $50,000.00 is appropriated from the General Fund to the Secretary of State for the purpose of hiring a consultant that will provide support to the Secretary in the study pursuant to subsection (a) of this section.*~~

~~*Sec. 2. EFFECTIVE DATE*~~

~~*This act shall take effect on January 1, 2027.*~~

** * * Cybersecurity Advisory Council * * **

Sec. 3. 20 V.S.A. § 4662 is amended to read:

§ 4662. CYBERSECURITY ADVISORY COUNCIL

(a) Creation. There is created the Cybersecurity Advisory Council to advise on the State's cybersecurity infrastructure, best practices, communications protocols, standards, training, and safeguards.

(b) Membership. The Council shall be composed of the following members:

(1) the Chief Information Officer, who shall serve as the Chair or appoint a designee from the Council to serve as the Chair;

(2) the Chief Information Security Officer;

(3) a representative from a distribution or transmission utility, appointed by the Commissioner of Public Service;

(4) a representative from a State municipal water system, appointed by the Secretary of Natural Resources;

(5) a representative from a Vermont hospital, appointed by the President of the Vermont Association of Hospitals and Health Systems;

(6) a person representing a Vermont business related to an essential supply chain, appointed by the Chair of the Vermont Business Roundtable;

(7) the Director of Vermont Emergency Management or designee;

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

(9) the Vermont Adjutant General or designee;

(10) the Attorney General or designee; ~~and~~

(11) the President of Vermont Information Technology Leaders or designee;

(12) the Chair of the House Committee on Energy and Digital Infrastructure;

(13) the Chair of the Senate Committee on Institutions; and

(14) a representative from the Judiciary, appointed by the Chief Justice of the Supreme Court.

* * *

Sec. 3a. 2023 Acts and Resolves No. 71, Sec. 4 is amended to read:

Sec. 4. REPEAL

20 V.S.A. chapter 208 (cybersecurity) is repealed on June 30, ~~2028~~ 2033.

** * * Educational Technology * * **

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

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

* * *

Subchapter 3A. Student Privacy

* * *

§ 2443f. ENFORCEMENT

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

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

Subchapter 3B. Educational Technology

§ 2444a. REGISTRATION

(a) Definitions. As used in this section:

(1)(A) "Educational technology product" and "product" mean any software, application, or platform that may collect, process, or transmit student data and that is used for teaching and learning purposes in a school in Vermont.

(B) "Educational technology product" and "product" does not include:

(i) hardware or other physical devices; or

(ii) a product that is being used in a school without the knowledge of the provider.

(2) "Filing" means an initial registration, amendment, periodic report, or other filing with the Secretary of State as the Secretary may require.

(3) "Provider of an educational technology product" and "provider" mean a person that provides an educational technology product that is in use at a school.

(4) "School" means a public school or an independent school approved pursuant to 16 V.S.A. § 166 and includes school districts.

(5) "School district" has the same meaning as in 16 V.S.A. § 11(a).

(b) Mandatory data reporting. In addition to all other requirements of a person registering with the Secretary of State pursuant to State law, a person doing business in this State as a provider of an educational technology product shall, at the time of a filing, provide the following:

(1) the name and primary physical, email, and internet addresses of the person;

(2) a link to the most recent version of the privacy policy and terms and conditions of each product in use in any school;

(3) the name of each school in which the provider is operating pursuant to a paid contract;

(4) the name and a brief description of each product of the provider, or a URL that provides the same information;

(5) which products may be in use in any school; and

(6) an attestation that each product meets:

(A) the standards set forth in subchapter 3A of this chapter (student privacy) and subchapter 6 of this chapter (the Vermont Age-Appropriate Design Code Act); and

(B) all relevant federal and State privacy laws, including the federal Children's Online Privacy Protection Act.

** * * Effective Dates * * **

Sec. 5. EFFECTIVE DATES

(a) Secs. 1 and 4 shall take effect on January 1, 2027.

(b) This section and Secs. 2 and 3 shall take effect on July 1, 2026.