TO THE HOUSE OF REPRESENTATIVES:

The Committee on Commerce and Economic Development to which was referred House Bill No. 211 entitled "An act relating to data brokers and personal information" respectfully reports that it has considered the same and recommends that the bill be amended by striking out all after the enacting clause and inserting in lieu thereof the following:

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

CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

Subchapter 1. General Provisions

§ 2430. DEFINITIONS

As used in this chapter:

(1) "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) "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.

(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:

(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~~.

(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 data broker.

(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 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.

~~(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;

(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.

~~(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 or data broker.

(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 or data broker for a legitimate purpose of the data collector or data broker, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the data collector's or data broker'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 or data broker 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. 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.

* * *

§ 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.

(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 data broker other than a data broker 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 broker 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) ~~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 January 31 of each year, shall:

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

(2) pay a registration fee ~~of $100.00~~ in an amount determined by the Secretary of State that shall 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 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;

~~(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;

(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 (3);

(G) 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;

(H) 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;

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

(J) a link to a page on the data broker's website that informs consumers about the rights of consumers to opt out, including:

(i) whether 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;

(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 from; and

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

(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)(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 of the consumer's brokered personal information;

(C) direct all processors 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 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:

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

(B) the brokered personal information is used by a consumer reporting agency to furnish a consumer report pursuant to the Fair Credit Reporting Act.

(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 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. 2. EFFECTIVE DATE

This act shall take effect on July 1, 2026.

(Committee vote: _____)

_____

Representative _____

FOR THE COMMITTEE