

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:

1                   (i) iris or retina scans;

2                   (ii) fingerprints;

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

4                   (iv) vein patterns;

5                   (v) voice prints; and

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

7                   (B) “Biometric data” does not include:

8                   (i) a digital or physical photograph;

9                   (ii) an audio or video recording; or

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

13                   ~~(3)(A) “Brokered personal information” means one or more of the~~  
14                   ~~following computerized data elements about a consumer, if categorized or~~  
15                   ~~organized for dissemination to third parties:~~

16                   ~~(i) name;~~

17                   ~~(ii) address;~~

18                   ~~(iii) date of birth;~~

19                   ~~(iv) place of birth;~~

20                   ~~(v) mother’s maiden name;~~

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

6                   ~~(vii) name or address of a member of the consumer’s immediate~~  
7                   ~~family or household;~~

8                   ~~(viii) Social Security number or other government issued~~  
9                   ~~identification number; or~~

10                  ~~(ix) other information that, alone or in combination with the other~~  
11                  ~~information sold or licensed, would allow a reasonable person to identify the~~  
12                  ~~consumer with reasonable certainty~~ any information, including derived data  
13                  and unique identifiers, that is linked or reasonably linkable, alone or in  
14                  combination with other information, to an identified or identifiable individual  
15                  or to a device that identifies, is linked to, or is reasonably linkable to one or  
16                  more identified or identifiable individuals in a household.

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

20                  ~~(2)(4)~~ (4) “Business” means a commercial entity, including a sole  
21                  proprietorship, partnership, corporation, association, limited liability company,

1 or other group, however organized and whether or not organized to operate at a  
2 profit, including a financial institution organized, chartered, or holding a  
3 license or authorization certificate under the laws of this State, any other state,  
4 the United States, or any other country, or the parent, affiliate, or subsidiary of  
5 a financial institution, but does not include the State, a State agency, any  
6 political subdivision of the State, or a vendor acting solely on behalf of, and at  
7 the direction of, the State.

8 ~~(3)~~(5) “Consumer” means an individual residing in this State.

9 ~~(4)~~(6)(A) “Data broker” means a business, or unit or units of a business,  
10 separately or together, that knowingly collects and sells or licenses to third  
11 parties the brokered personal information of a consumer with whom the  
12 business does not have a direct relationship.

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

15 ~~(i) customer, client, subscriber, user, or registered user of the~~  
16 ~~business’s goods or services;~~

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

18 ~~(iii) investor in the business; or~~

19 ~~(iv) donor to the business~~ As used in this subdivision (6), “direct  
20 relationship” means that a consumer has intentionally interacted with a  
21 business for the purpose of accessing, purchasing, using, requesting, or

1 obtaining information about the business’s products or services. A consumer  
2 does not have a direct relationship with a business if the purpose of the  
3 consumer’s engagement is to exercise a consumer right or for the business to  
4 verify the consumer’s identity. A business does not have a direct relationship  
5 with a consumer simply because the business collects brokered personal  
6 information directly from the consumer; the consumer must intend to interact  
7 with the business. A business is still a data broker and does not have a direct  
8 relationship with a consumer as to the brokered personal information the  
9 business sells about the consumer that it collected outside of a first-party  
10 interaction with the consumer.

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

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

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

19 ~~(iii) providing publicly available information related to a~~  
20 ~~consumer’s business or profession; or~~

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

3                   ~~(D)(C)~~ The phrase “sells or licenses” does not include:

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

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

9                   ~~(5)(A) “Data broker security breach” means an unauthorized acquisition~~  
10 ~~or a reasonable belief of an unauthorized acquisition of more than one element~~  
11 ~~of brokered personal information maintained by a data broker when the~~  
12 ~~brokered personal information is not encrypted, redacted, or protected by~~  
13 ~~another method that renders the information unreadable or unusable by an~~  
14 ~~unauthorized person.~~

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

20                   ~~(C) In determining whether brokered personal information has been~~  
21 ~~acquired or is reasonably believed to have been acquired by a person without~~

1 ~~valid authorization, a data broker may consider the following factors, among~~  
2 ~~others:~~

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

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

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

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

13 ~~(6)(7)~~ “Data collector” means a person who, for any purpose, whether  
14 by automated collection or otherwise, handles, collects, disseminates, or  
15 otherwise deals with personally identifiable information, and includes the  
16 State, State agencies, political subdivisions of the State, public and private  
17 universities, privately and publicly held corporations, limited liability  
18 companies, financial institutions, and retail operators.

19 ~~(7)(8)~~ “Encryption” means use of an algorithmic process to transform  
20 data into a form in which the data is rendered unreadable or unusable without  
21 use of a confidential process or key.

1           (9)(A) “GenAI system” means an artificial intelligence system that can  
2           generate derived synthetic content, including text, images, video, and audio,  
3           that emulates the structure and characteristics of the system’s training data.

4           (B) As used in subdivision (A) of this subdivision (9), “artificial  
5           intelligence system” means an engineered or machine-based system that varies  
6           in its level of autonomy and that can, for explicit or implicit objectives, infer  
7           from the input it receives how to generate outputs that can influence physical  
8           or virtual environments.

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

11          ~~(8)~~(11) “License” means a grant of access to, or distribution of, data by  
12          one person to another in exchange for consideration. A use of data for the sole  
13          benefit of the data provider, where the data provider maintains control over the  
14          use of the data, is not a license.

15          ~~(9)~~(12) “Login credentials” means a consumer’s user name or e-mail  
16          email address, in combination with a password or an answer to a security  
17          question, that together permit access to an online account.

18          ~~(10)~~(13)(A) “Personally identifiable information” means a consumer’s  
19          first name or first initial and last name in combination with one or more of the  
20          following digital data elements, when the data elements are not encrypted,  
21          redacted, or protected by another method that renders them unreadable or

1 unusable by unauthorized persons, subject to the exception in subdivision (C)  
2 of this subdivision (13):

3 (i) a Social Security number;

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

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

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

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

19 (vi) genetic information; and

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

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

3 (III) a health insurance policy number.

4 (B) “Personally identifiable information” does not ~~mean~~ include  
5 publicly available information ~~that is lawfully made available to the general~~  
6 ~~public from federal, State, or local government records.~~

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

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

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

19 (16)(A) “Publicly available information” means information that:

20 (i) is made available:

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

- 1                    (II) to the general public from widely distributed media; or
- 2                    (ii) a data broker has a reasonable basis to believe that the
- 3                    consumer has lawfully made available to the general public.
- 4                    (B) “Publicly available information” does not include:
- 5                    (i) biometric data collected by a business about a consumer
- 6                    without the consumer’s knowledge;
- 7                    (ii) information that is collated and combined to create a consumer
- 8                    profile that is made available to a user of a publicly available website either in
- 9                    exchange for payment or free of charge;
- 10                   (iii) information that is made available for sale;
- 11                   (iv) an inference about a consumer that is generated from the
- 12                   information described in subdivision (ii) or (iii) of this subdivision (16)(B);
- 13                   (v) any obscene visual depiction, as defined in 18 U.S.C. § 1460;
- 14                   (vi) brokered personal information that is created through the
- 15                   combination of brokered personal information with publicly available
- 16                   information;
- 17                   (vii) genetic data, unless otherwise made publicly available by the
- 18                   consumer to whom the information pertains;
- 19                   (viii) information provided by a consumer on a website or online
- 20                   service made available to all members of the public, for free or for a fee, where

1 the consumer has maintained a reasonable expectation of privacy in the  
2 information, such as by restricting the information to a specific audience; or

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

5 ~~(11)~~(17) “Record” means any material on which written, drawn, spoken,  
6 visual, or electromagnetic information is recorded or preserved, regardless of  
7 physical form or characteristics.

8 ~~(12)~~(18) “Redaction” means the rendering of data so that the data are  
9 unreadable or are truncated so that ~~no~~ not more than the last four digits of the  
10 identification number are accessible as part of the data.

11 ~~(19)~~(A) “Sale” means the exchange of a consumer’s brokered personal  
12 information by the data broker to a third party for monetary or other valuable  
13 consideration.

14 (B) “Sale” does not include:

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

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

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

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

5                   (v) the disclosure of publicly available information; or

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

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

14                  (D) As used in subdivision (C) of this subdivision (19), “control” or  
15                  “controlled” means:

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

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

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

1           ~~(13)~~(20)(A) “Security breach” means unauthorized acquisition of  
2           electronic data, or a reasonable belief of an unauthorized acquisition of  
3           electronic data, that compromises the security, confidentiality, or integrity of a  
4           consumer’s personally identifiable information or login credentials maintained  
5           by a data collector or data broker.

6           (B) “Security breach” does not include good faith but unauthorized  
7           acquisition of personally identifiable information or login credentials by an  
8           employee or agent of the data collector or data broker for a legitimate purpose  
9           of the data collector or data broker, provided that the personally identifiable  
10          information or login credentials are not used for a purpose unrelated to the data  
11          collector’s or data broker’s business or subject to further unauthorized  
12          disclosure.

13          (C) In determining whether personally identifiable information or  
14          login credentials have been acquired or ~~is~~ are reasonably believed to have been  
15          acquired by a person without valid authorization, a data collector or data  
16          broker may consider the following factors, among others:

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

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

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

4 (iv) that the information has been made public.

5 § 2431. ACQUISITION AND DISCLOSURE OF BROKERED PERSONAL  
6 INFORMATION; PROHIBITIONS

7 (a) Prohibited acquisition and use.

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

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

12 (A) stalking or harassing another person;

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

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

17 (b) Disclosure. A data broker shall:

18 (1) maintain procedures that require prospective users of the data  
19 broker's brokered personal information to identify themselves, state the  
20 purposes for which the information is sought, and certify that the information  
21 shall be used for no other purpose;



\* \* \*

(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

1 attempts to contact the consumer for a live conversation before the data  
2 collector may leave a voicemail providing information about the breach.

3 \* \* \*

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

12 (d) Exception to notice requirement.

13 (1) Notice of a security breach pursuant to subsection (b) of this section  
14 is not required if the data collector establishes that misuse of personally  
15 identifiable information or login credentials is not reasonably possible and the  
16 data collector provides notice of the determination that the misuse of the  
17 personally identifiable information or login credentials is not reasonably  
18 possible pursuant to the requirements of this subsection. If the data collector  
19 establishes that misuse of the personally identifiable information or login  
20 credentials is not reasonably possible, the data collector shall provide notice of  
21 its determination that misuse of the personally identifiable information or login

1 credentials is not reasonably possible and a detailed explanation for said  
2 determination to the Vermont Attorney General or to the Department of  
3 Financial Regulation in the event that the data collector is a person or entity  
4 licensed or registered with the Department under Title 8 or this title. The data  
5 collector may designate its notice and detailed explanation to the Vermont  
6 Attorney General or the Department of Financial Regulation as “trade secret”  
7 if the notice and detailed explanation meet the definition of trade secret  
8 contained in 1 V.S.A. § 317(c)(9).

9 \* \* \*

10 (e) HIPAA compliance. A data collector that is subject to the privacy,  
11 security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant  
12 to the federal Health Insurance Portability and Accountability Act, P.L. 104-  
13 191 (1996) is deemed to be in compliance with this subchapter if the data  
14 collector:

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

18 (2) ~~the data collector~~ provides notice to affected consumers pursuant to  
19 the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart  
20 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.

\* \* \*

1     § 2436. NOTICE OF DATA BROKER SECURITY BREACHES

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

4           (b) Notice of breach.

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

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

17           (A)(i) The data broker shall notify the Attorney General of the date of  
18    the security breach and the date of discovery of the breach and shall provide a  
19    preliminary description of the breach within 14 business days, consistent with  
20    the legitimate needs of the law enforcement agency, as provided in

1 subdivisions (3) and (4) of this subsection (b), after the data broker's discovery  
2 of the security breach.

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

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

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

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

1           (3) The notice to the Attorney General and a consumer required by this  
2           subsection shall be delayed upon request of a law enforcement agency. A law  
3           enforcement agency may request the delay if it believes that notification may  
4           impede a law enforcement investigation or a national or Homeland Security  
5           investigation or jeopardize public safety or national or Homeland Security  
6           interests. In the event law enforcement makes the request for a delay in a  
7           manner other than in writing, the data broker shall document the request  
8           contemporaneously in writing and include the name of the law enforcement  
9           officer making the request and the officer's law enforcement agency engaged  
10           in the investigation. A law enforcement agency shall promptly notify the data  
11           broker in writing when the law enforcement agency no longer believes that  
12           notification may impede a law enforcement investigation or a national or  
13           Homeland Security investigation or jeopardize public safety or national or  
14           Homeland Security interests. The data broker shall provide notice required by  
15           this subsection without unreasonable delay upon receipt of a written  
16           communication, which includes facsimile or electronic communication, from  
17           the law enforcement agency withdrawing its request for delay.

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

1           (A) the incident in general terms;

2           (B) the categories of brokered personal information that was subject  
3 to the security breach;

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

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

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

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

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

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

15           (B) electronic notice, for those consumers for whom the data broker  
16 has a valid email address, if:

17            (i) the data broker's primary method of communication with the  
18 consumer is by electronic means, the electronic notice does not request or  
19 contain a hypertext link to a request that the consumer provide personal  
20 information, and the electronic notice conspicuously warns consumers not to

1 provide personal information in response to electronic communications  
2 regarding security breaches; or

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

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

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

10 (c) Exception to notice requirement.

11 (1) Notice of a security breach pursuant to subsection (b) of this section  
12 is not required if the data broker establishes that misuse of brokered personal  
13 information is not reasonably possible and the data broker provides notice of  
14 the determination that the misuse of the brokered personal information is not  
15 reasonably possible pursuant to the requirements of this subsection. If the data  
16 broker establishes that misuse of the brokered personal information is not  
17 reasonably possible, the data broker shall provide notice of its determination  
18 that misuse of the brokered personal information is not reasonably possible and  
19 a detailed explanation for said determination to the Attorney General. The data  
20 broker may designate its notice and detailed explanation to the Attorney

1 General as a trade secret if the notice and detailed explanation meet the  
2 definition of trade secret contained in 1 V.S.A. § 317(c)(9).

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

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

11 (e) Enforcement.

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

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

18 \* \* \*

19 Subchapter 3A. Student Privacy

20 \* \* \*

21 § 2443f. ENFORCEMENT

(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

(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:~~

- VT LEG #386584 v.6

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

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

6 (i) ~~the method for requesting an opt out;~~

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

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

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

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

15 (E)(C) pursuant to section 2436 of this chapter, the number of data  
16 broker security breaches that the data broker has experienced during the prior  
17 year, and if known, the total number of consumers affected by the breaches;

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

- 1           ~~(G)~~(E) whether the data broker:
- 2               (i) collects the:
- 3                   (I) precise geolocation of consumers;
- 4                   (II) reproductive health care data of consumers;
- 5                   (III) biometric data of consumers;
- 6                   (IV) immigration status of consumers;
- 7                   (V) sexual orientation of consumers;
- 8                   (VI) union membership status of consumers;
- 9                   (VII) name, date of birth, zip code, email address, or phone
- 10           number of consumers;
- 11               (VIII) account login or account number of consumers in
- 12           combination with any required security code, access code, or password that
- 13           would permit access to a consumer’s account with a third party;
- 14               (IX) driver’s license number, State identification card number,
- 15           Social Security number, passport number, military identification number, or
- 16           other unique identification number of consumers issued on a government
- 17           document commonly used to verify the identity of a specific individual; or
- 18               (X) mobile advertising identification number, connected
- 19           television identification number, or vehicle identification number of
- 20           consumers; and

- 1                    (ii) in the past year, has shared or sold consumers’ data to:
- 2                    (I) a foreign actor;
- 3                    (II) the federal government;
- 4                    (III) to other state or local governments;
- 5                    (IV) to law enforcement, unless the data was shared pursuant to
- 6 a subpoena or other court order; or
- 7                    (V) to a developer of a GenAI system or model;
- 8                    (F) the three most common types of personal information that the
- 9 data broker collects, if the data broker does not collect the information set forth
- 10 in subdivisions (E)(i)(VII) and (E)(i)(IX) of this subdivision (4);
- 11                    (G) an electronic copy of the data broker’s:
- 12                    (i) bond, pursuant to subdivision (3) of this subsection (a); and
- 13                    (ii) current privacy policy;
- 14                    (H) any additional information or explanation the data broker
- 15 chooses to provide concerning its data collection practices;
- 16                    (I) the URL of a page on the data broker’s website that:
- 17                    (i) pursuant to subsection (c) of this section, allows a consumer to
- 18 request that a data broker delete the brokered personal information of the
- 19 consumer; and
- 20                    (ii) informs consumers about the rights of consumers to opt out of
- 21 the collection of the consumer’s brokered personal information, including:

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

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

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

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

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

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

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

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

17                   ~~(1) a civil penalty of \$50.00 for each day, not to exceed a total of~~  
18                   ~~\$10,000.00 for each year, it fails to register pursuant to this section;~~

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

21                   ~~(3) other penalties imposed by law.~~

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

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

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

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

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

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

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

19                   (B) correct the materially incorrect information by filing an  
20           amendment pursuant to subdivision (a)(5) of this section not later than 30 days  
21           after discovering or receiving notification of the incorrect information, and, if

1 it fails to correct the information, the data broker shall be liable for an  
2 additional civil penalty of \$1,000.00 per day for each day the data broker fails  
3 to correct the information.

4 (c) ~~The Attorney General may maintain an action in the Civil Division~~  
5 ~~of the Superior Court to collect the penalties imposed in this section and to~~  
6 ~~seek appropriate injunctive relief.~~ Deleting brokered personal information.

7 (1) A data broker shall:

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

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

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

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

20 (A) describe how a consumer may exercise the consumer's right to  
21 delete the consumer's brokered personal information, including the process for

1 the consumer to appeal the denial of a deletion request pursuant to subdivision  
2 (5) of this subsection (c);

3 (B) adhere to the accessibility and usability guidelines recommended  
4 pursuant to 42 U.S.C. chapter 126 (the Americans with Disabilities Act) and  
5 29 U.S.C. § 794d (section 508 of the Rehabilitation Act of 1973); and

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

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

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

15 (B) the brokered personal information is:

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

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

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

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

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

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

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

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

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

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

19                   (5) A data broker shall provide the consumer with the ability to appeal  
20                   an instance where the data broker denies the consumer’s request to delete the

1 consumer's brokered personal information pursuant to subdivision (3) of this  
2 subsection (c) with a process that:

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

5 (B) is conspicuously available to the consumer;

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

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

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

15 (6)(A) If a data broker is unable to authenticate a deletion request made  
16 pursuant to subdivision (1) of this subsection (c), the data broker shall not be  
17 required to comply with the request and shall provide notice to the consumer or  
18 the consumer's agent that the data broker is unable to authenticate the request.  
19 The data broker shall provide the consumer with the additional information the  
20 data broker requires in order to authenticate the consumer.

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

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

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

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

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

16           (e) Enforcement.

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

19           (2) The Attorney General has the same authority to adopt rules to  
20           implement the provisions of this section and to conduct civil investigations.

1 enter into assurances of discontinuance, and bring civil actions as provided  
2 under chapter 63, subchapter 1 of this title.

3 § 2447. DATA BROKER DUTY TO PROTECT INFORMATION;  
4 STANDARDS; TECHNICAL REQUIREMENTS

5 \* \* \*

6 (d) Enforcement.

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

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

13 Sec. 2. STUDY OF ACCESSIBLE DELETION MECHANISM; REPORT;  
14 APPROPRIATION

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

16 (1) establishing an accessible deletion mechanism that:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13          (N) provides a description of the following:

14               (i) the deletion permitted by this section;

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

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

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

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

9        (c) Appropriation. In fiscal year 2027, X is appropriated from the General  
10       Fund to the Secretary of State to fund the cost of a consultant to provide  
11       support to the Secretary in the study pursuant to subsection (a) of this section.

1       Sec. 3. EFFECTIVE DATE

2       This act shall take effect on January 1, 2027.

3

4

5

6

7

8       (Committee vote: \_\_\_\_\_)

9

10

\_\_\_\_\_  
Representative \_\_\_\_\_

11

FOR THE COMMITTEE