

1 TO THE HOUSE OF REPRESENTATIVES:

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

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

8 CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

9 Subchapter 1. General Provisions

10 § 2430. DEFINITIONS

11 As used in this chapter:

12 (1) “Authorized agent” means:

13 (A) a person designated by a consumer to act on the consumer’s
14 behalf;

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

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

19 (2)(A) “Biometric data” means that data generated from the
20 technological processing of an individual’s unique biological, physical, or
21 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) “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 (10) “Identified or identifiable individual” means an individual who can
5 be readily identified, directly or indirectly.

6 ~~(8)~~(11) “License” means a grant of access to, or distribution of, data by
7 one person to another in exchange for consideration. A use of data for the sole
8 benefit of the data provider, where the data provider maintains control over the
9 use of the data, is not a license.

10 ~~(9)~~(12) “Login credentials” means a consumer’s user name or ~~e-mail~~
11 email address, in combination with a password or an answer to a security
12 question, that together permit access to an online account.

13 ~~(10)~~(13)(A) “Personally identifiable information” means a consumer’s
14 first name or first initial and last name in combination with one or more of the
15 following digital data elements, when the data elements are not encrypted,
16 redacted, or protected by another method that renders them unreadable or
17 unusable by unauthorized persons, subject to the exception in subdivision (C)
18 of this subdivision (13):

19 (i) a Social Security number;
20 (ii) a driver license or nondriver State identification card number,
21 individual taxpayer identification number, passport number, military

1 identification card number, or other identification number that originates from
2 a government identification document that is commonly used to verify identity
3 for a commercial transaction;

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

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

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

14 (vi) genetic information; and

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

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

19 (III) a health insurance policy number.

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

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

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

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

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

17 (i) is made available:

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

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

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

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

1 ~~(11)~~(17) “Record” means any material on which written, drawn, spoken,
2 visual, or electromagnetic information is recorded or preserved, regardless of
3 physical form or characteristics.

4 ~~(12)~~(18) “Redaction” means the rendering of data so that the data are
5 unreadable or are truncated so that ~~no~~ not more than the last four digits of the
6 identification number are accessible as part of the data.

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

10 (B) “Sale” does not include:

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

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

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

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

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

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

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

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

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

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

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

17 ~~(13)(20)~~(A) “Security breach” means unauthorized acquisition of
18 electronic data, or a reasonable belief of an unauthorized acquisition of
19 electronic data, that compromises the security, confidentiality, or integrity of a
20 consumer’s personally identifiable information or login credentials maintained
21 by a data collector or data broker.

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

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

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

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

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

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

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

(a) Prohibited acquisition and use.

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

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

(A) stalking or harassing another person;

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

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

(b) Disclosure. A data broker shall:

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

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

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

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

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

7 (c) Enforcement.

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

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

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

15 § 2435. NOTICE OF SECURITY BREACHES

16 * * *

17 (b) Notice of breach.

18 * * *

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

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

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

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

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

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

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

19 * * *

20 (c) Notice to consumer reporting agencies. In the event a data collector
21 provides notice to more than 1,000 consumers at one time pursuant to this

1 section, the data collector shall notify, without unreasonable delay, all
2 consumer reporting agencies that compile and maintain files on consumers on
3 a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing,
4 distribution, and content of the notice. This subsection shall not apply to a
5 person who is licensed or registered under Title 8 by the Department of
6 Financial Regulation.

7 (d) Exception to notice requirement.

8 (1) Notice of a security breach pursuant to subsection (b) of this section
9 is not required if the data collector establishes that misuse of personally
10 identifiable information or login credentials is not reasonably possible and the
11 data collector provides notice of the determination that the misuse of the
12 personally identifiable information or login credentials is not reasonably
13 possible pursuant to the requirements of this subsection. If the data collector
14 establishes that misuse of the personally identifiable information or login
15 credentials is not reasonably possible, the data collector shall provide notice of
16 its determination that misuse of the personally identifiable information or login
17 credentials is not reasonably possible and a detailed explanation for said
18 determination to the Vermont Attorney General or to the Department of
19 Financial Regulation in the event that the data collector is a person or entity
20 licensed or registered with the Department under Title 8 or this title. The data
21 collector may designate its notice and detailed explanation to the Vermont

1 Attorney General or the Department of Financial Regulation as “trade secret”
2 if the notice and detailed explanation meet the definition of trade secret
3 contained in 1 V.S.A. § 317(c)(9).

4 * * *

5 (e) HIPAA compliance. A data collector that is subject to the privacy,
6 security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant
7 to the federal Health Insurance Portability and Accountability Act, P.L. 104-
8 191 (1996) is deemed to be in compliance with this subchapter if the data
9 collector:

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

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

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

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

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

(h) Enforcement.

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

§ 2436. NOTICE OF DATA BROKER SECURITY BREACHES

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

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

11 (A)(i) The data broker shall notify the Attorney General of the date of
12 the security breach and the date of discovery of the breach and shall provide a
13 preliminary description of the breach within 14 business days, consistent with
14 the legitimate needs of the law enforcement agency, as provided in
15 subdivisions (3) and (4) of this subsection (b), after the data broker's discovery
16 of the security breach.

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

20 (iii) Unless otherwise ordered by a court of this State for good
21 cause shown, a notice provided under this subdivision (2)(A) shall not be

1 disclosed, without the consent of the data broker, to any person other than the
2 authorized agent or representative of the Attorney General, a State’s Attorney,
3 or another law enforcement officer engaged in legitimate law enforcement
4 activities.

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

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

14 (3) The notice to the Attorney General and a consumer required by this
15 subsection shall be delayed upon request of a law enforcement agency. A law
16 enforcement agency may request the delay if it believes that notification may
17 impede a law enforcement investigation or a national or Homeland Security
18 investigation or jeopardize public safety or national or Homeland Security
19 interests. In the event law enforcement makes the request for a delay in a
20 manner other than in writing, the data broker shall document the request
21 contemporaneously in writing and include the name of the law enforcement

1 officer making the request and the officer's law enforcement agency engaged
2 in the investigation. A law enforcement agency shall promptly notify the data
3 broker in writing when the law enforcement agency no longer believes that
4 notification may impede a law enforcement investigation or a national or
5 Homeland Security investigation or jeopardize public safety or national or
6 Homeland Security interests. The data broker shall provide notice required by
7 this subsection without unreasonable delay upon receipt of a written
8 communication, which includes facsimile or electronic communication, from
9 the law enforcement agency withdrawing its request for delay.

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

14 (A) the incident in general terms;

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

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

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

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

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

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

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

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

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

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

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

20 or

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

3 (c) Exception to notice requirement.

4 (1) Notice of a security breach pursuant to subsection (b) of this section
5 is not required if the data broker establishes that misuse of brokered personal
6 information is not reasonably possible and the data broker provides notice of
7 the determination that the misuse of the brokered personal information is not
8 reasonably possible pursuant to the requirements of this subsection. If the data
9 broker establishes that misuse of the brokered personal information is not
10 reasonably possible, the data broker shall provide notice of its determination
11 that misuse of the brokered personal information is not reasonably possible and
12 a detailed explanation for said determination to the Attorney General. The data
13 broker may designate its notice and detailed explanation to the Attorney
14 General as a trade secret if the notice and detailed explanation meet the
15 definition of trade secret contained in 1 V.S.A. § 317(c)(9). Upon review of
16 the data broker's notice and detailed explanation, the Attorney General may
17 request additional information from the data broker and may accept or reject
18 the data broker's determination. If the Attorney General rejects the data
19 broker's determination, the data broker shall provide notice of the security
20 breach pursuant to subsection (b) of this section.

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

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

(e) Enforcement.

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

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

* * *

Subchapter 3A. Student Privacy

* * *

§ 2443f. ENFORCEMENT

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

1 title.

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

6 * * *

7 Subchapter 5. Data Brokers

8 § 2446. DATA BROKERS; ANNUAL REGISTRATION

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20 (G)(E) whether the data broker:

21 (i) collects the:

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

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

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

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

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

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

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

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

14 ~~(1) a civil penalty of \$50.00 for each day, not to exceed a total of~~
15 ~~\$10,000.00 for each year, it fails to register pursuant to this section;~~

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

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

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

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

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

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

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

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

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

17 (B) correct the materially incorrect information by filing an
18 amendment pursuant to subdivision (a)(5) of this section not later than 30 days
19 after discovering or receiving notification of the incorrect information, and, if
20 it fails to correct the information, the data broker shall be liable for an

1 additional civil penalty of \$1,000.00 per day for each day the data broker fails
2 to correct the information.

3 (c) Deleting brokered personal information.

4 (1) A data broker shall:

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

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

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

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

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

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

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

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

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

13 (B) the brokered personal information is:

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

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

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

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

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

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

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

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

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

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

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

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

1 (B) is conspicuously available to the consumer;

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

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

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

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

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

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

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

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

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

12 (e) Enforcement.

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

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

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

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

* * *

(d) Enforcement.

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

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

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

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

(1) establishing an accessible deletion mechanism that:

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

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

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

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

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

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

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

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

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

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

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

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

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

10 (N) provides a description of the following:

11 (i) the deletion permitted by this section;

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

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

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

19 (b) Reporting. The Secretary of State shall, based on the study set forth in
20 subsection (a) of this section, submit to the House Committee on Commerce
21 and Economic Development and the Senate Committee on Economic

1 Development, Housing and General Affairs an interim report on or before
2 December 1, 2027, and a final report on or before December 1, 2028, including
3 its findings and any proposed legislation for the General Assembly's
4 consideration. The interim report shall provide the General Assembly with any
5 recommended actions to pursue in the 2028 legislative session.

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

9 Sec. 3. EFFECTIVE DATE

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

11
12 (Committee vote: _____)

13 _____

14 Representative _____

15 FOR THE COMMITTEE