

1 S.269

2 Introduced by Senators Kitchel and Lyons

3 Referred to Committee on

4 Date:

5 Subject: Commerce and trade; data security breach

6 Statement of purpose of bill as introduced: This bill proposes to enhance the  
7 standards and requirements for a business to be notified of a possible data  
8 security breach and to be informed that it has legal duties under current law.

9 An act relating to business consumer protection and data security breaches

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

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

12 CHAPTER 62. PROTECTION OF PERSONAL INFORMATION

13 Subchapter 1. General Provisions

14 § 2430. DEFINITIONS

15 The following definitions shall apply throughout this chapter unless  
16 otherwise required:

17 (1) ~~“Business” means a sole proprietorship, partnership, corporation,~~  
18 ~~association, limited liability company, or other group, however organized and~~  
19 ~~whether or not organized to operate at a profit, including a financial institution~~  
20 ~~organized, chartered, or holding a license or authorization certificate under the~~

1 laws of this State, any other state, the United States, or any other country, or  
2 the parent, affiliate, or subsidiary of a financial institution, but in no case shall  
3 it include the State, a State agency, or any political subdivision of the State.

4 [Repealed.]

5 (2) “Consumer” means an individual residing in this State.

6 (3) “Data collector” ~~may include the State, State agencies, political~~  
7 ~~subdivisions of the State, public and private universities, privately and publicly~~  
8 ~~held corporations, limited liability companies, financial institutions, retail~~  
9 ~~operators, and any other entity that, for any purpose, whether by automated~~  
10 ~~collection or otherwise, handles, collects, disseminates, or otherwise deals with~~  
11 ~~nonpublic personal information~~ means a person who possesses personally  
12 identifiable information in electronic format.

13 (4) “Energption” ~~means use of an algorithmic process to transform data~~  
14 ~~into a form in which the data is rendered unreadable or unusable without use of~~  
15 ~~a confidential process or key~~ “Encrypt” means to render electronic data  
16 unreadable or unusable until the operation of one or more additional processes  
17 enables the data to be read or used.

18 (5)(A) “Personally identifiable information” means ~~an individual’s a~~  
19 consumer’s first name, or first initial and last name in combination, combined  
20 ~~with any~~ one or more of the following data elements, when either the name or  
21 the data elements are not encrypted ~~or~~, redacted, or protected by another

1 method that renders them unreadable or unusable by an unauthorized ~~persons~~  
2 person:

3 (i) Social Security number;

4 (ii) ~~Motor~~ motor vehicle operator's license number or nondriver  
5 identification card number;

6 (iii) ~~Financial~~ financial account number or credit or debit card  
7 number, if ~~circumstances exist in which~~ the number could be used without  
8 additional identifying information, access codes, or passwords; or

9 (iv) ~~Account~~ account passwords or personal identification  
10 numbers or other access codes for a financial account.

11 (B) "Personally identifiable information" does not mean publicly  
12 available information that is lawfully made available to the general public from  
13 federal, State, or local government records.

14 (6) ~~"Records" means any material on which written, drawn, spoken,~~  
15 ~~visual, or electromagnetic information is recorded or preserved, regardless of~~  
16 ~~physical form or characteristics~~ "Record," used as a noun, means information  
17 that is inscribed on a tangible medium or that is stored in an electronic or other  
18 medium and is retrievable in perceivable form.

19 (7) ~~"Redaction" means the rendering of data so that it is unreadable or is~~  
20 ~~truncated so that no more than the last four digits of the identification number~~  
21 ~~are accessible as part of the data~~ "Redact" means to alter a data element

1 referenced in subdivision (5)(A) of this section so that no more than the last  
2 four digits of the data element are readable.

3 (8)(A) “Security breach” means unauthorized acquisition of electronic  
4 data, or a reasonable belief of an unauthorized acquisition of electronic data,  
5 that compromises the security, confidentiality, or integrity of a consumer’s  
6 personally identifiable information maintained by the data collector.

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

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

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

19 ~~(ii) indications that the information has been downloaded or~~  
20 ~~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                   Subchapter 2. Security Breach Notice Act

6                   § 2434. DISCOVERY AND NOTIFICATION OF A SECURITY BREACH

7                   (a) This subchapter shall be known as the Security Breach Notice Act

8                   (b) A data collector shall initiate the notice and compliance requirements of  
9 section 2435 of this chapter upon the earliest of the following:

10                   (1) the date on which a data collector discovers a security breach;

11                   (2) the date on which a similarly situated data collector reasonably  
12 should have discovered a security breach; or

13                   (3) the date on which a member of law enforcement provides written  
14 notice to a data collector that:

15                   (A) a security breach has occurred; and

16                   (B) as a result of the security breach, the data collector has a duty to  
17 inform its customers and the Vermont Attorney General's office of the security  
18 breach pursuant to the Vermont Security Breach Notice Act, section 2435 of  
19 this chapter.

20                   (c) In determining whether a security breach has occurred, a data collector  
21 shall consider the totality of the circumstances, including:

1           (1) information or evidence that suggests an unauthorized person  
2 possesses or has used personally identifiable information:

3           (2) a consumer, merchant, or other person has reported suspected  
4 identity theft to law enforcement or to the data collector; or

5           (3) personally identifiable information has been made public.

6 § 2435. NOTICE OF ~~A SECURITY BREACHES BREACH~~

7           (a) ~~This section shall be known as the Security Breach Notice Act.~~  
8 [Repealed.]

9           (b) Notice of breach.

10           (1) Except as ~~set forth~~ otherwise provided in subsection (d) of this  
11 section, ~~any~~ a data collector that owns or licenses ~~computerized~~ personally  
12 identifiable information ~~that includes personal information concerning a~~  
13 ~~consumer shall notify the consumer that there has been a security breach~~  
14 ~~following discovery or notification to the data collector of the breach. Notice~~  
15 ~~of the security breach shall be made~~ that is acquired in a security breach shall  
16 notify each consumer affected by the breach in the most expedient time  
17 possible and without unreasonable delay, ~~but not later than~~ on or before  
18 45 days after the discovery or notification of the breach consistent with  
19 section 2434 of this chapter, consistent with the legitimate needs of the ~~unless~~  
20 a law enforcement agency, as provided in subdivisions (3) and requests a delay  
21 under subdivision (4) of this subsection, or with any the data collector requires

1 additional time to take measures that he or she believes are reasonably  
2 necessary to determine the scope of the security breach and restore the  
3 reasonable integrity, security, and confidentiality of the data system.

4 (2) ~~Any~~ A data collector that ~~maintains or possesses computerized data~~  
5 ~~containing~~ personally identifiable information of a consumer that the data  
6 collector does not own or license ~~or any data collector that acts or conducts~~  
7 ~~business in Vermont that maintains or possesses records or data containing~~  
8 ~~personally identifiable information that the data collector does not own or~~  
9 ~~license~~ shall notify the owner or licensee of the information of ~~any~~ a security  
10 breach immediately following discovery or notification of the breach  
11 consistent with section 2434 of this chapter, ~~consistent with the legitimate~~  
12 ~~needs of~~ unless a law enforcement as provided in subdivisions (3) and agency  
13 requests a delay under subdivision (4) of this subsection.

14 (3) A data collector ~~or other entity subject to this subchapter~~ shall  
15 provide notice of a security breach to the Attorney General or to the  
16 Department of Financial Regulation, as applicable, as follows:

17 (A)(i) A data collector ~~or other entity~~ regulated by the Department of  
18 Financial Regulation under Title 8 or this title shall provide notice of a breach  
19 to the Department. ~~All other data collectors or other entities subject to this~~  
20 ~~subchapter~~

1           (ii) A data collector that is not regulated by the Department of  
2 Financial Regulation shall provide notice of a breach to the Attorney General.

3           (B)(i) ~~The A~~ data collector shall ~~notify~~ communicate to the Attorney  
4 General or the Department, as applicable, ~~of~~ the date of the security breach,  
5 ~~and~~ the date of discovery or notification of the breach, and ~~shall provide a~~  
6 preliminary description of the breach within 14 business days, ~~consistent with~~  
7 ~~the legitimate needs of the law enforcement agency as provided in this~~  
8 ~~subdivision (3) and subdivision (4) of this subsection,~~ of the data collector's  
9 discovery or notification of the breach consistent with section 2434 of this  
10 chapter, or when the data collector provides notice to consumers pursuant to  
11 this section, whichever is sooner, unless a law enforcement agency requests a  
12 delay under subdivision (4) of this subsection (b).

13           (ii) Notwithstanding subdivision ~~(B)(i) of this subsection (b)(3)~~  
14 ~~(3)(B)(i) of this subsection (b)~~, a data collector who, prior to the date of the  
15 breach, on a form and in a manner prescribed by the Attorney General, had  
16 sworn in writing to the Attorney General that it maintains written policies and  
17 procedures to maintain the security of personally identifiable information and  
18 to respond to a breach in a manner consistent with Vermont law shall notify  
19 the Attorney General of the date of the security breach and the date of  
20 discovery of the breach and shall provide a description of the breach prior to

1 providing notice of the breach to consumers pursuant to subdivision (1) of this  
2 subsection.

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

7 (iv) Unless otherwise ordered by a court of this State for good  
8 cause shown, no person may disclose a notice provided under ~~this~~ subdivision  
9 (3)(B) ~~shall not be disclosed of this subsection (b)~~ to any person other than the  
10 Department, the authorized agent or representative of the Attorney General, a  
11 ~~state's attorney~~ State's Attorney, or another law enforcement officer engaged  
12 in legitimate law enforcement activities, without the consent of the data  
13 collector.

14 (C)(i) When ~~the~~ a data collector provides notice of ~~the~~ a security  
15 breach pursuant to subdivision (1) of this subsection (b), the data collector  
16 shall notify the Attorney General or the Department, as applicable, of the  
17 number of Vermont consumers affected, if known to the data collector, and  
18 shall provide a copy of the notice provided to consumers under subdivision (1)  
19 of this subsection ~~(b)~~.

20 (ii) The data collector may send to the Attorney General or the  
21 Department, as applicable, a second copy of the consumer notice, from which

1 is redacted the type of personally identifiable information that was subject to  
2 the breach, and which the Attorney General or the Department shall use for  
3 any public disclosure of the breach.

4 ~~(4)(A) The notice to a consumer required by this subsection shall be~~  
5 ~~delayed upon request of a law enforcement agency. A law enforcement agency~~  
6 ~~may request the delay if it believes~~ A data collector shall delay the release of a  
7 notice to consumers when the agency determines that notification may impede  
8 a law enforcement investigation, or a national or Homeland Security  
9 investigation, or jeopardize public safety or national or Homeland Security  
10 interests.

11 ~~(B) In the event~~ If a law enforcement ~~makes the request in a manner~~  
12 agency requests a delay other than in writing, the data collector shall document  
13 ~~such~~ the request contemporaneously in writing, including the name of the law  
14 enforcement officer making the request and the ~~officer's~~ law enforcement  
15 agency engaged in the investigation.

16 (C) A law enforcement agency shall promptly notify the data  
17 collector in writing when the law enforcement agency ~~no longer believes~~  
18 determines that notification ~~may~~ will no longer impede a law enforcement  
19 investigation, or a national or Homeland Security investigation, or jeopardize  
20 public safety or national or Homeland Security interests.

1           (D) The data collector shall provide notice as required by this section  
2 without unreasonable delay upon receipt of a written communication, ~~which~~  
3 ~~includes facsimile or electronic communication,~~ from the law enforcement  
4 agency withdrawing its request for delay.

5           (5) ~~The~~ A notice of a security breach sent to a consumer shall be clear  
6 and conspicuous. The notice shall include a description of each of the  
7 following, if known to the data collector:

8                   (A) ~~The~~ the incident in general terms;:

9                   (B) ~~The~~ the type of personally identifiable information that was  
10 subject to the security breach;:

11                   (C) ~~The~~ the general acts of the data collector to protect the personally  
12 identifiable information from further security breach;:

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

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

17                   (F) ~~The~~ the approximate date of the security breach.

18           (6) For purposes of this subsection, notice to consumers may be  
19 provided by one of the following methods:

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

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

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

4 (I) the data collector does not have contact information ~~set forth~~  
5 ~~in subdivisions (i) and (iii) of this subdivision (6)(A), required to provide notice~~  
6 under subdivision (6)(A)(i) or (iii) of this subsection (b); the data collector's  
7 primary method of communication with the consumer is by electronic means; ;  
8 the electronic notice does not request or contain a hypertext link to a request  
9 that the consumer provide personal information; ; and the electronic notice  
10 conspicuously warns consumers not to provide personal information in  
11 response to electronic communications regarding security breaches; or

12 (II) the notice provided is consistent with the provisions  
13 regarding electronic records and signatures for notices as ~~set forth~~ provided in  
14 15 U.S.C. § 7001; or

15 (iii) ~~Telephonic~~ telephonic notice, provided that telephonic contact  
16 is made directly with each affected consumer, and the telephonic contact is not  
17 through a prerecorded message.

18 (B) Substitute notice, if the data collector demonstrates that the cost  
19 of providing written or telephonic notice, ~~pursuant to subdivision (A)(i) or (iii)~~  
20 ~~of this subdivision (6)~~, to affected consumers would exceed \$5,000.00; or that  
21 the ~~affected~~ class of affected consumers to be provided written or telephonic

1 notice, pursuant to subdivision (A)(i) or (iii) of this subdivision (6), exceeds  
2 5,000; or the data collector does not have sufficient contact information.

3 Substitute notice shall consist of all of the following:

4 (i) conspicuous posting of the notice on the data collector's  
5 website page if the data collector maintains one; and

6 (ii) notification to major statewide and regional media.

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

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

1 ~~possible and a detailed explanation for said determination to the Vermont~~  
2 ~~Attorney General or to the Department of Financial Regulation in the event~~  
3 ~~that the data collector is a person or entity licensed or registered with the~~  
4 ~~Department under Title 8 or this title. The data collector may designate its~~  
5 ~~notice and detailed explanation to the Vermont Attorney General or the~~  
6 ~~Department of Financial Regulation as “trade secret” if the notice and detailed~~  
7 ~~explanation meet the definition of trade secret contained in 1 V.S.A.~~  
8 ~~§ 317(e)(9), as applicable.~~

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

14 (e) ~~Any~~ A waiver of the provisions of this subchapter is contrary to public  
15 policy and is void and unenforceable.

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

20 (1) The Federal Interagency Guidance Response Programs for  
21 Unauthorized Access to Consumer Information and Customer Notice, issued

1 on March 7, 2005, by the Board of Governors of the Federal Reserve System,  
2 the Federal Deposit Insurance Corporation, the Office of the Comptroller of  
3 the Currency, and the Office of Thrift Supervision.

4 (2) Final Guidance on Response Programs for Unauthorized Access to  
5 Member Information and Member Notice, issued on April 14, 2005, by the  
6 National Credit Union Administration.

7 (3) A financial institution regulated by the Department of Financial  
8 Regulation that is subject to subdivision (1) or (2) of this subsection shall  
9 notify the Department as soon as possible after it becomes aware of ~~an incident~~  
10 ~~involving unauthorized access to or use of personally identifiable information a~~  
11 security breach.

12 (g) Enforcement.

13 (1) With respect to all data collectors and other entities subject to this  
14 subchapter, other than a person or entity licensed or registered with the  
15 Department of Financial Regulation under Title 8 or this title, the Attorney  
16 General and ~~state's attorney~~ State's Attorney shall have ~~sole and full~~ the same  
17 authority ~~to investigate potential violations of this subchapter and to enforce,~~  
18 ~~prosecute, obtain, and impose remedies for a violation of this~~ the provisions of  
19 this subchapter or any rules ~~or regulations made~~ adopted pursuant to this  
20 chapter as the Attorney General and ~~state's attorney~~ State's Attorney have  
21 under chapter 63 of this title. ~~The Attorney General may refer the matter to the~~

1 ~~state's attorney in an appropriate case.~~ The Superior Courts shall have  
2 jurisdiction over any enforcement matter brought by the Attorney General or a  
3 ~~state's attorney~~ State's Attorney under this subsection.

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

12 (h) [Repealed.]

13 \* \* \*

14 Sec. 2. EFFECTIVE DATE

15 This act shall take effect on passage.