No. 109. An act relating to consumer protection.

(H.254)

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

Sec. 1. 9 V.S.A. chapter 63, subchapter 1C is added to read:

Subchapter 1C. Discount Membership Programs

§ 2470aa. DEFINITIONS

In this subchapter:

(1) "Billing information" means any data that enables a seller of a discount membership program to access a consumer's credit or debit card, bank, or other account, but does not include the consumer's name, e-mail address, telephone number, or mailing address. For credit card and debit card accounts, billing information includes the full account number, card type, and expiration date, and, if necessary, the security code. For accounts at a financial institution, "billing information" includes the full account number and routing number, and, if necessary, the name of the financial institution holding the account.

(2) A "discount membership program" is a program that entitles consumers to receive discounts, rebates, rewards, or similar incentives on the purchase of goods or services or both, in whole or in part, from any third party.

§ 2470bb. APPLICABILITY

A discount membership program is a good or service within the meaning of subsection 2451a(b) of this chapter. This subchapter applies only to persons

who are regularly and primarily engaged in trade or commerce in this state in connection with offering or selling discount membership programs. This subchapter shall not apply to an electronic payment system, as defined in 9 V.S.A. § 2480o, or to a financial institution, as defined in 8 V.S.A. § 11101(32).

§ 2470cc. REQUIRED DISCLOSURES; CONSENT

(a) No person shall charge or attempt to charge a consumer for a discount membership program, or to renew a discount membership program beyond the term expressly agreed to by the consumer or the term permitted under section 2470ff of this title, whichever is shorter, unless:

(1) Before obtaining the consumer's billing information, the person has clearly and conspicuously disclosed to the consumer all material terms of the transaction, including:

(A) A description of the types of goods and services on which a discount is available;

(B) The name of the discount membership program and the name and address of the seller of the program;

(C) The amount, or a good faith estimate, of the typical discount on each category of goods and services;

(D) The cost of the program, including the amount of any periodic charges, how often such charges are imposed, and the method of payment;

(E) The right to cancel and to terminate the program, which shall be no more restrictive than as required by section 2470ee of this subchapter, and a toll-free telephone number and e-mail address that can be used to cancel the membership;

(F) The maximum length of membership, as described in section 2470ff of this subchapter;

(G) In the event that the program is offered on the Internet through a link or referral from another business's website, the fact that the seller is not affiliated with that business;

(H) The fact that periodic notices of the program billings will be e-mailed or mailed to the consumer, as the case may be, consistent with section 2470dd of this title; and

(2) The person has received express informed consent for the charge from the consumer whose credit or debit card, bank, or other account will be charged, by:

(A) Obtaining from the consumer:

(i) the consumer's billing information; and

(ii) the consumer's name and address and a means to contact the consumer; and

(B) Requiring the consumer to perform an additional affirmative action, such as clicking on an online confirmation button, checking an online

box that indicates the consumer's consent to be charged the amount disclosed, or expressly giving consent over the telephone.

(b) A person who sells discount membership programs shall retain evidence of a consumer's express informed consent for at least three years after the consent is given.

§ 2470dd. PERIODIC NOTICES

(a) A person who periodically charges a consumer for a discount membership program shall send the consumer a notice of the charge no less frequently than every three months from the date of initial enrollment that clearly and conspicuously discloses:

(1) A description of the program;

(2) The name of the discount membership program and the name and address of the seller of the program;

(3) The cost of the program, including the amount of any periodic charges, how often such charges are imposed, and the method of payment;

(4) The right to cancel and to terminate the program, which shall be no more restrictive than as required by section 2470ee of this subchapter, and a toll-free number and e-mail address that can be used to cancel the membership; and

(5) The maximum length of membership, as described in section 2470ff of this subchapter.

(b) The notice specified in subsection (a) of this section:

(1) Shall be sent:

(A) To the consumer's last known e-mail address, if the consumer enrolled in the discount membership program online or by e-mail, with the subject line, "IMPORTANT INFORMATION ABOUT YOUR DISCOUNT PROGRAM BILLING," or substantially similar words, provided that the sender takes reasonable steps to verify that the e-mail has been opened; or

(B) Otherwise by first-class mail to the consumer's last known mailing address, with the heading on the enclosure and outside envelope, "IMPORTANT INFORMATION ABOUT YOUR DISCOUNT PROGRAM BILLING," or substantially similar words; and

(2) Shall not include any solicitation or advertising.

§ 2470ee. CANCELLATION AND TERMINATION

(a) In addition to any other right to revoke an offer, a consumer may cancel the purchase of a discount membership program until midnight on the 30th day after the date the consumer has given express informed consent to be charged for the program. If the consumer cancels within the 30-day period, the seller of the discount membership program shall, within ten days of receiving the notice of cancellation, provide a full refund to the consumer.

(b) Notice of cancellation shall be deemed given when deposited in a mailbox properly addressed and postage prepaid or when e-mailed to the e-mail address of the seller of the discount membership program.

(c) In addition to the right to cancel described in this subchapter, a consumer may terminate a discount membership program at any time by providing notice to the seller by one of the methods described in this section. In that case, the consumer shall not be obligated to make any further payments under the program and shall not be entitled to any discounts under the program for any period of time after the last month for which payment has been made.

(d) If the seller of a discount membership program cancels the program for any reason other than nonpayment by the consumer, the seller shall make pro rata reimbursement to the consumer of all periodic charges paid by the consumer for periods of time after cancellation. Prior to such cancellation, the seller shall first provide reasonable notice and an explanation of the cancellation in writing to the consumer.

§ 2470ff. MAXIMUM LENGTH OF PLAN

No person shall sell, or offer for sale, a discount membership program lasting longer than 18 months.

§ 2470gg. BILLING INFORMATION

No person who offers or sells discount membership programs shall obtain billing information relating to a consumer except directly from the consumer.

§ 2470hh. VIOLATIONS

(a) A violation of this subchapter is deemed to be a violation of section 2453 of this title.

(b) The attorney general has the same authority to make rules, conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as is provided under subchapter 1 of this chapter.

Sec. 2. 9 V.S.A. chapter 63 is amended to read:

CHAPTER 63. CONSUMER ~~FRAUD~~ PROTECTION

* * *

§ 2453. PRACTICES PROHIBITED; ANTITRUST AND CONSUMER ~~FRAUD~~ PROTECTION

* * *

§ 2461e. REQUIREMENTS FOR GUARANTEED PRICE PLANS AND PREPAID CONTRACTS

* * *

(d) Private right of action under consumer ~~fraud~~ protection act. In addition to the remedies set forth in sections 2458 and 2461 of this title, a home heating oil, kerosene, or liquefied petroleum gas dealer may bring an action against its heating oil, kerosene, or liquefied petroleum gas suppliers for failing to honor its contract with the home heating oil, kerosene, or liquefied petroleum gas dealer. The home heating oil, kerosene, or liquefied petroleum gas dealer

bringing the action may recover all remedies available to consumers under subsection 2461(b) of this title.

* * *

§ 2480q. PENALTIES

(a) The following penalties shall apply to violations of this subchapter:

* * *

(3) A violation of section 2480p of this subchapter shall be deemed a violation of ~~chapter 63~~ section 2453 of this title~~, the Consumer Fraud Act~~. The attorney general has the same authority to conduct civil investigations, enter into assurances of discontinuance, and bring civil actions as provided under subchapter 1 ~~of chapter 63~~ of this ~~title~~ chapter.

* * *

Sec. 3. REDESIGNATION OF TERM "CONSUMER FRAUD" TO READ "CONSUMER PROTECTION"

(a) The legislative council, under its statutory revision authority pursuant to 2 V.S.A. § 424, is directed to delete the term "consumer fraud" and to insert in lieu thereof the term "consumer protection" wherever it appears in each of the following sections: 7 V.S.A. § 1010; 8 V.S.A. §§ 2706, 2709, and 2764; 9 V.S.A. § 2471; 18 V.S.A. §§ 1511, 1512, 4086, 4631, 4633, 4634, and 9473; 20 V.S.A. § 2757; and 33 V.S.A. §§ 1923 and 2010; and in any other sections as appropriate.

(b) Notwithstanding the provisions of 3 V.S.A. chapter 25, the attorney general shall have the authority to delete the term "consumer fraud" and to insert in lieu thereof the term "consumer protection" wherever it appears in the attorney general's rules, regulations, and procedures and shall exercise such authority upon passage of this act as he or she deems to be necessary, appropriate, and consistent with the purposes of this section.

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

CHAPTER 62: PROTECTION OF PERSONAL INFORMATION

§ 2430. DEFINITIONS

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

* * *

(5)(A) "~~Personal~~ Personally identifiable information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) Social Security number;

(ii) Motor vehicle operator's license number or nondriver identification card number;

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

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

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

* * *

(8)(A) "Security breach" means unauthorized acquisition ~~or access~~ of ~~computerized~~ electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of ~~personal~~ a consumer's personally identifiable information maintained by the data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition ~~or access~~ of ~~personal~~ personally identifiable information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the ~~personal~~ personally identifiable information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

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

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

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

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

(iv) that the information has been made public.

§ 2435. NOTICE OF SECURITY BREACHES

(a) This section shall be known as the Security Breach Notice Act.

(b) Notice of breach.

(1) Except as set forth in subsection (d) of this section, any data collector that owns or licenses computerized ~~personal~~ personally identifiable information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the security breach

shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in ~~subdivision~~ subdivisions (3) and (4) of this subsection, or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any data collector that maintains or possesses computerized data containing ~~personal~~ personally identifiable information of a consumer that the ~~business~~ data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing ~~personal~~ personally identifiable information that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in ~~subdivision~~ subdivisions (3) and (4) of this subsection.

(3) A data collector or other entity subject to this subchapter, other than a person or entity licensed or registered with the department of financial regulation under Title 8 or this title, shall provide notice of a breach to the attorney general's office as follows:

(A)(i) The data collector shall notify the attorney general of the date of the security breach and the date of discovery of the breach and shall provide

a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency as provided in subdivisions (3) and (4) of this subsection, of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to this section, whichever is sooner.

(ii) Notwithstanding subdivision (A)(i) of this subdivision (b)(3), a data collector who, prior to the date of the breach, on a form and in a manner prescribed by the office of the attorney general, had sworn in writing to the attorney general that it maintains written policies and procedures to maintain the security of personally identifiable information and respond to a breach in a manner consistent with Vermont law shall notify the attorney general of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers pursuant to subdivision (1) of this subsection.

(iii) If the date of the breach is unknown at the time notice is sent to the attorney general, the data collector shall send the attorney general the date of the breach as soon as it is known.

(iv) Unless otherwise ordered by a court of this state for good cause shown, a notice provided under this subdivision (3)(A) shall not be disclosed to any person other than the authorized agent or representative of the attorney general, a state's attorney, or another law enforcement officer engaged

in legitimate law enforcement activities without the consent of the data collector.

(B)(i) When the data collector provides notice of the breach pursuant to subdivision (1) of this subsection (b), the data collector shall notify the attorney general of the number of Vermont consumers affected, if known to the data collector, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection (b).

(ii) The data collector may send to the attorney general a second copy of the consumer notice, from which is redacted the type of personally identifiable information that was subject to the breach, and which the attorney general shall use for any public disclosure of the breach.

(4) The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or homeland security investigation or jeopardize public safety or national or homeland security interests. In the event law enforcement makes the request in a manner other than in writing, the data collector shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data collector when the law

enforcement agency no longer believes that notification may impede a law enforcement investigation, or a national or homeland security investigation or jeopardize public safety or national or homeland security interests. The data collector shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.

~~(4)~~(5) The notice to a consumer shall be clear and conspicuous. The notice shall include a description of each of the following, if known to the data collector:

(A) The incident in general terms.

(B) The type of ~~personal~~ personally identifiable information that was subject to the ~~unauthorized access or acquisition~~ security breach.

(C) The general acts of the ~~business~~ data collector to protect the ~~personal~~ personally identifiable information from further ~~unauthorized access or acquisition~~ security breach.

(D) A ~~toll-free~~ telephone number, toll-free if available, that the consumer may call for further information and assistance.

(E) Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

(F) The approximate date of the security breach.

~~(5)~~(6) For purposes of this subsection, notice to consumers may be provided by one of the following methods:

* * *

(h) Vermont law enforcement agencies, including the department of public safety, shall not be considered a data collector. Except as provided in subdivisions (b)(2) and (b)(3) of this section, Vermont law enforcement agencies, including the department of public safety, shall be exempt from this subchapter.

Sec. 5. 3 V.S.A. § 2222 is amended to read:

§ 2222. POWERS AND DUTIES; BUDGET AND REPORT

(a) In addition to the duties expressly set forth elsewhere by law the secretary shall:

* * *

(9) Submit to the general assembly concurrent with the governor's annual budget request required under 32 V.S.A. § 306, a strategic plan for information technology and information security which outlines the significant deviations from the previous year's ~~information technology~~ plan, and which details the plans for information technology activities of state government for the following fiscal year as well as the administration's financing recommendations for these activities. For purposes of this section, "information security" shall mean protecting information and information

systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability. All such plans shall be reviewed and approved by the commissioner of information and innovation prior to being included in the governor's annual budget request. The plan shall identify the proposed sources of funds for each project identified. The plan shall also contain a review of the state's information technology and information security and an identification of priority projects by agency. The plan shall include, for any proposed information technology activity with a cost in excess of $100,000.00:

(A) a life-cycle costs analysis including planning, purchase and development of applications, the purchase of hardware and the ~~on-going~~ ongoing operation and maintenance costs to be incurred over the expected life of the systems; and a cost-benefit analysis which shall include acquisition costs as well as operational and maintenance costs over the expected life of the system;

(B) the cost savings ~~and/or~~ or service delivery improvements or both which will accrue to the public or to state government;

(C) a statement identifying any impact of the proposed new computer system on the privacy or disclosure of individually identifiable information;

(D) a statement identifying costs and issues related to public access to nonconfidential information;

(E) a statewide budget for all information technology activities with a cost in excess of ~~$100,000~~ $100,000.00.

(10) The secretary shall annually submit to the general assembly a five-year information technology and information security plan which indicates the anticipated information technology activities of the legislative, executive, and judicial branches of state government. For purposes of this section, "information technology activities" shall mean:

(A) the creation, collection, processing, storage, management, transmission, or conversion of electronic data, documents, or records;

(B) the design, construction, purchase, installation, maintenance, or operation of systems, including both hardware and software, which perform these activities.

* * *

Sec. 6. 22 V.S.A. § 901 is amended to read:

§ 901. DEPARTMENT OF INFORMATION AND INNOVATION

The department of information and innovation, created in 3 V.S.A. § 2283b, shall have all the responsibilities assigned to it by law, including the following:

(1) to provide direction and oversight for all activities directly related to information technology and information security, including telecommunications services, information technology equipment, software,

accessibility, and networks in state government. For purposes of this section, "information security" is defined as in 3 V.S.A. § 2222(a)(9);

(2) to manage GOVnet;

(3) to review all information technology and information security requests for proposal in accordance with agency of administration policies;

(4) to review and approve information technology activities in all departments with a cost in excess of $100,000.00, and annually submit to the general assembly a strategic plan and a budget for information technology and information security as required of the secretary of administration by 3 V.S.A. § 2222(a)(9). For purposes of this section, "information technology activities" is defined in 3 V.S.A. § 2222(a)(10);

(5) to administer the independent review responsibilities of the secretary of administration described in 3 V.S.A. § 2222(g);

(6) to perform the responsibilities of the secretary of administration under 30 V.S.A. § 227b;

(7) to administer communication, information, and technology services, which are transferred from the department of buildings and general services;

(8) to inventory technology assets within state government;

(9) to coordinate information technology and information security training within state government;

* * *

(11) to provide technical support and services to the department of human resources and of finance and management for the statewide central accounting and encumbrance system, the statewide budget development system, the statewide human resources management system, and other agency of administration systems as may be assigned by the secretary; and

(12) not later than July 1, 2013, to adopt rules requiring the auditing and updating of state websites.

Sec. 7. EFFECTIVE DATE

This act shall take effect on passage.

Approved: May 8, 2012