081553316

SENATE BILL NO. 307

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the Senate Committee for Courts of Justice on February 6, 2008)

(Patron Prior to Substitute—Senator Reynolds)

A BILL to amend the Code of Virginia by adding a section numbered 18.2-186.6, relating to identity theft prevention; notice of breach of information system.

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding a section numbered 18.2-186.6 as follows:

§ 18.2-186.6. Notice of breach of information system.

A. As used in this section:

"Breach of the security of the system" means the unauthorized acquisition and access of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Access to encrypted data shall be considered a breach if the encrypted data is acquired and accessed in an unencrypted form, or if the breach of the security of the system involves a person with access to the encryption key and the individual or commercial entity reasonably knows or should have known that such breach has caused or will cause identity theft or other fraud to any citizen of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.

"Commercial entity" includes (i) corporations, business trusts, estates, trusts, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, or any other legal entity, whether for profit or not-for-profit and (ii) governments, governmental subdivisions, and agencies.

"Encrypted" means transformation through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.

"Notice" means:

1. Written notice;

2. Telephonic notice;

3. Electronic notice, if the individual's or company's customary method of communication with a member of the affected class is by electronic means or if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or

4. Substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, or that the affected class of Virginia residents to be notified exceeds 100,000 residents, or that the individual or the commercial entity does not have sufficient contact information to provide notice. Substitute notice consists of all of the following: (i) email notice if the individual or the commercial entity has email addresses for the members of the affected class of Virginia residents, (ii) conspicuous posting of the notice on the website of the individual or the commercial entity if the individual or the commercial entity maintains one, and (iii) notification to major statewide media.

The notice required under this section shall not be considered a debt communication as defined by the Fair Debt Collections Practices Act (15 U.S.C. § 1692 et seq.).

The notice required under this section shall include a description of the following:

a. The incident in general terms;

b. The type of personal information that was subject to the unauthorized access and acquisition;

c. The general acts of the individual or commercial entity to protect the personal information from further unauthorized access;

d. A telephone number that the person may call for further information and assistance, if one exists; and

e. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth when the data elements are neither encrypted nor redacted:

1. Social security number;

2. Driver's license number or state identification card number issued in lieu of a driver's license number; or

3. Financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Redacted" means the transformation or truncation of data such that it is no longer usable or accessible.

B. An individual or a commercial entity that conducts business in Virginia and that owns or licenses computerized data that includes personal information about a resident of Virginia shall, when it becomes aware of a breach of the security of the system, (i) conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused and (ii) notify the Office of the Attorney General that a breach has occurred. Notification to Virginia residents under this section is not required if, after a reasonable investigation, the person or commercial entity determines that there is no reasonable likelihood of identity theft or fraud to affected Virginia residents. If there is a reasonable likelihood of identity theft or fraud to affected Virginia residents, notice shall be made in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection D, and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. If an individual or commercial entity knows of any pending investigation by a law-enforcement agency, the individual or commercial entity shall inform the investigating law-enforcement agency that it plans to issue a notice pursuant to this section no less than 48 hours prior to issuing such notice.

C. An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about a Virginia resident occurred or is reasonably likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the breach.

D. Notice required by this section may be delayed if a law-enforcement agency determines that the notice will impede a criminal investigation. Notice required by this section may be delayed to allow the individual or commercial entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section shall be made in good faith, without unreasonable delay, and as soon as possible after the law-enforcement agency determines that notification will no longer impede the investigation.

E. Under this section, an individual or commercial entity that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section is deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected Virginia residents in accordance with its policies in the event of a breach of the security of the system.

F. Under this section, an individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section if the individual or the commercial entity notifies affected Virginia residents in accordance with the maintained procedures when a breach occurs.

G. In the event an individual or commercial entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or commercial entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1682(a)(p), of the timing, distribution, and content of the notice.

H. Pursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action in law to address violations and ensure proper compliance with this section. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law. Nothing in this section shall limit an individual from recovering direct economic damages resulting from a violation of this section.

I. The provisions of this section shall not apply to criminal intelligence systems subject to the restrictions of 28 C.F.R. Part 23 that are maintained by law-enforcement agencies of the Commonwealth and the Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ 52-12 et seq.) of Title 52.