17104720D

SENATE BILL NO. 1033

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the Senate Committee on Finance
on January 25, 2017)

(Patron Prior to Substitute—Senator Howell)

A BILL to amend and reenact § 18.2-186.6 of the Code of Virginia, relating to a notification requirement for breach of payroll data.

Be it enacted by the General Assembly of Virginia:

1. That § 18.2-186.6 of the Code of Virginia is amended and reenacted as follows:

§ 18.2-186.6. Breach of personal information notification.

A. As used in this section:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

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

"Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

"Financial institution" has the meaning given that term in 15 U.S.C. § 6809 (3).

"Individual" means a natural person.

"Notice" means:

1. Written notice to the last known postal address in the records of the individual or entity;

2. Telephone notice;

3. Electronic notice; or

4. Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Substitute notice consists of all of the following:

a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

c. Notice to major statewide media.

Notice required by this section shall not be considered a debt communication as defined by the Fair Debt Collection Practices Act in 15 U.S.C. § 1692a.

Notice required by this section shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the individual or entity to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; and

(5) 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 does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

1. Five digits of a social security number; or

2. The last four digits of a driver's license number, state identification card number, or account number.

B. If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or 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 may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

C. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

D. An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.

E. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or 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. § 1681a (p), of the timing, distribution, and content of the notice.

F. An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information that are consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of the security of the system.

G. An entity that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) and maintains procedures for notification of a breach of the security of the system in accordance with the provision of that Act and any rules, regulations, or guidelines promulgated thereto shall be deemed to be in compliance with this section.

H. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this section.

I. Except as provided by subsections J and K, pursuant to the enforcement duties and powers of the Office of the Attorney General, the Attorney General may bring an action to address violations of this section. The Office of the Attorney General may impose a civil penalty not to exceed $150,000 per breach of the security of the system or a series of breaches of a similar nature that are discovered in a single investigation. Nothing in this section shall limit an individual from recovering direct economic damages from a violation of this section.

J. A violation of this section by a state-chartered or licensed financial institution shall be enforceable exclusively by the financial institution's primary state regulator.

K. A violation of this section by an individual or entity regulated by the State Corporation Commission's Bureau of Insurance shall be enforced exclusively by the State Corporation Commission.

L. 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 organized Criminal Gang File of the Virginia Criminal Information Network (VCIN), established pursuant to Chapter 2 (§ 52-12 et seq.) of Title 52.

M. Notwithstanding any other provision of this section, any employer or payroll service provider that owns or licenses computerized data relating to income tax withheld pursuant to Article 16 (§ 58.1-460 et seq.) of Chapter 3 of Title 58.1 shall notify the Office of the Attorney General without unreasonable delay after the discovery or notification of unauthorized access and acquisition of unencrypted and unredacted computerized data containing a taxpayer identification number in combination with the income tax withheld for that taxpayer that compromises the confidentiality of such data and that creates a reasonable belief that an unencrypted and unredacted version of such information was accessed and acquired by an unauthorized person, and causes, or the employer or payroll provider reasonably believes has caused or will cause, identity theft or other fraud.

Such employer or payroll service provider shall provide the Office of the Attorney General with the name and federal employer identification number of the employer as defined in § 58.1-460 that may be affected by the compromise in confidentiality. Upon receipt of such notice, the Office of the Attorney General shall notify the Department of Taxation of the compromise in confidentiality. The notification required under this subsection that does not otherwise require notification under this section shall not be subject to any other notification, requirement, exemption, or penalty contained in this section.