24100817D

HOUSE BILL NO. 666

Offered January 10, 2024

Prefiled January 9, 2024

A BILL to amend and reenact §§ 2.2-2009, 2.2-5514, and 18.2-186.6 of the Code of Virginia, relating to state agencies; electronic information breach.

Patron—Freitas

Referred to Committee on Communications, Technology and Innovation

Be it enacted by the General Assembly of Virginia:

1. That §§ 2.2-2009, 2.2-5514, and 18.2-186.6 of the Code of Virginia are amended and reenacted as follows:

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

A. To provide for the security of state government electronic information from unauthorized uses, intrusions or other security threats, the CIO shall direct the development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, standards, and guidelines shall apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies. The CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs. Such policies, standards, and guidelines shall, at a minimum:

1. Address the scope and frequency of security audits. In developing and updating such policies, standards, and guidelines, the CIO shall designate a government entity to oversee, plan, and coordinate the conduct of periodic security audits of all executive branch agencies and independent agencies. The CIO shall coordinate these audits with the Auditor of Public Accounts and the Joint Legislative Audit and Review Commission. The Chief Justice of the Supreme Court and the Joint Rules Committee of the General Assembly shall determine the most appropriate methods to review the protection of electronic information within their branches;

2. Control unauthorized uses, intrusions, or other security threats;

3. Provide for the protection of confidential data maintained by state agencies against unauthorized access and use in order to ensure the security and privacy of citizens of the Commonwealth in their interaction with state government. Such policies, standards, and guidelines shall include requirements that (i) any state employee or other authorized user of a state technology asset provide passwords or other means of authentication to use a technology asset and access a state-owned or state-operated computer network or database and (ii) a digital rights management system or other means of authenticating and controlling an individual's ability to access electronic records be utilized to limit access to and use of electronic records that contain confidential information to authorized individuals;

4. Address the creation and operation of a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate with the CIO, including (i) providing the CIO with information required to create and implement a Commonwealth risk management program, (ii) creating an agency risk management program, and (iii) complying with all other risk management activities; ~~and~~

5. Provide requirements for prompt notification of affected citizens of the Commonwealth in the event of a breach of the security of a state agency's electronic information from unauthorized uses, intrusions, or other security threats, which breach compromises such citizens' personal information as defined in § 2.2-3801; and

~~5.~~ *6.* Require that any contract for information technology entered into by the Commonwealth's executive, legislative, and judicial branches and independent agencies require compliance with applicable federal laws and regulations pertaining to information security and privacy.

B. 1. The CIO shall annually report to the Governor, the Secretary, and General Assembly on the results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies that have not implemented acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats. For any executive branch agency or independent agency whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the executive branch agency's or

independent agency's information technology projects pursuant to subsection B of § 2.2-2016.1, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor and Secretary any other appropriate actions.

2. Executive branch agencies and independent agencies subject to such audits as required by this section shall fully cooperate with the entity designated to perform such audits and bear any associated costs. Public bodies that are not required to but elect to use the entity designated to perform such audits shall also bear any associated costs.

C. In addition to coordinating security audits as provided in subdivision B 1, the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures. Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance and Appropriations. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities.

D. The provisions of this section shall not infringe upon responsibilities assigned to the Comptroller, the Auditor of Public Accounts, or the Joint Legislative Audit and Review Commission by other provisions of the Code of Virginia.

E. The CIO shall promptly receive reports from public bodies in the Commonwealth made in accordance with § 2.2-5514 and shall take such actions as are necessary, convenient, or desirable to ensure the security of the Commonwealth's electronic information and confidential data.

F. The CIO shall provide technical guidance to the Department of General Services in the development of policies, standards, and guidelines for the recycling and disposal of computers and other technology assets. Such policies, standards, and guidelines shall include the expunging, in a manner as determined by the CIO, of all confidential data and personal identifying information of citizens of the Commonwealth prior to such sale, disposal, or other transfer of computers or other technology assets.

G. The CIO shall provide all directors of agencies and departments with all such information, guidance, and assistance required to ensure that agencies and departments understand and adhere to the policies, standards, and guidelines developed pursuant to this section.

H. The CIO shall promptly notify all public bodies as defined in § 2.2-5514 of hardware, software, or services that have been prohibited pursuant to Chapter 55.3 (§ 2.2-5514 et seq.). The CIO shall restrict access to prohibited applications and websites in accordance with the provisions of § 2.2-5514.1.

I. 1. This subsection applies to the Commonwealth's executive, legislative, and judicial branches and independent agencies.

2. In collaboration with the heads of executive branch and independent agencies and representatives of the Chief Justice of the Supreme Court and the Joint Rules Committee of the General Assembly, the CIO shall develop and annually update a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats. The curriculum shall include activities, case studies, hypothetical situations, and other methods of instruction (i) that focus on forming good information security habits and procedures among state employees and (ii) that teach best practices for detecting, assessing, reporting, and addressing information security threats.

3. Every state agency shall provide annual information security training for each of its employees using the curriculum and materials developed by the CIO pursuant to subdivision 2. Employees shall complete such training within 30 days of initial employment and by January 31 each year thereafter.

State agencies may develop additional training materials that address specific needs of such agency, provided that such materials do not contradict the training curriculum and materials developed by the CIO.

The CIO shall coordinate with and assist state agencies in implementing the annual information security training requirement.

4. Each state agency shall (i) monitor and certify the training activity of its employees to ensure compliance with the annual information security training requirement, (ii) evaluate the efficacy of the information security training program, and (iii) forward to the CIO such certification and evaluation, together with any suggestions for improving the curriculum and materials, or any other aspects of the training program. The CIO shall consider such evaluations when it annually updates its curriculum and materials.

§ 2.2-5514. Prohibited products and services and required incident reporting.

A. For the purposes of this section, "public body" means any legislative body; any court of the Commonwealth; any authority, board, bureau, commission, district, or agency of the Commonwealth; any political subdivision of the Commonwealth, including counties, cities, and towns, city councils, boards of supervisors, school boards, planning commissions, and governing boards of institutions of higher education; and other organizations, corporations, or agencies in the Commonwealth supported

wholly or principally by public funds. "Public body" includes any committee, subcommittee, or other entity however designated of the public body or formed to advise the public body, including those with private sector or citizen members and corporations organized by the Virginia Retirement System.

B. No public body may use, whether directly or through work with or on behalf of another public body, any hardware, software, or services that have been prohibited by the U.S. Department of Homeland Security for use on federal systems.

C. Every public body shall report all (i) known incidents that threaten the security of the Commonwealth's data or communications or result in exposure of data protected by federal or state laws and (ii) other incidents compromising the security of the public body's information technology systems with the potential to cause major disruption to normal activities of the public body or other public bodies. Such reports shall be made to the Virginia Fusion Intelligence Center within 24 hours from when the incident was discovered. The Virginia Fusion Intelligence Center shall share such reports with the Chief Information Officer, as described in § 2.2-2005, or his designee at the Virginia Information Technologies Agency, promptly upon receipt.

D. Every state agency shall promptly notify, as described in § 18.2-186.6, affected citizens of the Commonwealth in the event of a breach of the security of such state agency's electronic information from an unauthorized use, intrusion, or other security threat, where such breach compromises such citizens' personal information as defined in § 2.2-3801.

§ 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, *or state agency* as part of a database of personal information regarding multiple individuals and that causes, or the individual ~~or~~, entity, *or state agency* 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, *or state agency* of an individual ~~or~~, entity, *or state agency* for the purposes of the individual ~~or~~, entity, *or state agency* 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 state agency* 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, *or state agency*;

2. Telephone notice;

3. Electronic notice; or

4. Substitute notice, if the individual ~~or the~~, entity, *or state agency* 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, *or state agency* 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, *or state agency* 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, *or state agency* if the individual ~~or the~~, entity, *or state agency* 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, *or state agency* 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;

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;

4. Passport number; or

5. Military identification number.

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, *or state agency* reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual ~~or~~, entity, *or state agency* 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, *or state agency* 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, *or state agency* notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual ~~or~~, entity, *or state agency* 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, *or state agency* 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, *or state agency* 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, *or state agency* that maintains computerized data that includes personal information that the individual ~~or~~, entity, *or state agency* 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, *or state agency* reasonably believes the personal information was accessed and acquired by an unauthorized person.

E. In the event an individual ~~or~~, entity, *or state agency* provides notice to more than 1,000 persons at one time pursuant to this section, the individual ~~or~~, entity, *or state agency* 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 *or state agency* 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. Nothing in this section shall apply to an individual or entity regulated by the State Corporation Commission's Bureau of Insurance.

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. With respect to employers, this subsection applies only to information regarding the employer's employees, and does not apply to information regarding the employer's customers or other non-employees.

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.