19104706D

HOUSE BILL NO. 2793

Offered January 18, 2019

A BILL to amend the Code of Virginia by adding a section numbered 59.1-443.4 and by adding in Title 59.1 a chapter numbered 35.2, consisting of sections numbered 59.1-444.4 through 59.1-444.10, relating to cybersecurity; personal information privacy; care and disposal of customer records; responsibility and accountability for connected devices.

Patron—Ayala

Referred to Committee on Commerce and Labor

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding a section numbered 59.1-443.4 and by adding in Title 59.1 a chapter numbered 35.2, consisting of sections numbered 59.1-444.4 through 59.1-444.10, as follows:

§ 59.1-443.4. Care and disposal of customer records.

A. As used in this section:

"Business" means a sole proprietorship, partnership, corporation, association, or other person, however organized and whether or not organized to operate at a profit. "Business" includes an entity that disposes of records.

"Customer" means an individual resident of the Commonwealth who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

"Personal information" means any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including, but not limited to, the individual's name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" includes a customer's username or email address in combination with a password or security question and answer that would permit access to an online account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted. "Records" does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

B. A business shall take all reasonable steps to dispose of, or arrange for the disposal of, customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

C. A business that owns, licenses, or maintains personal information about a customer shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information in order to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

D. The provisions of this section do not apply to:

1. A business subject to the medical privacy and security rules issued by the federal Department of Health and Human Services as 45 C.F.R. Parts 160 and 164; or

2. A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with such state or federal law shall be deemed compliance with this section with regard to those subjects. This subdivision does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

E. In addition to any remedy provided by § 59.1-444, a customer who suffers loss or pecuniary damage resulting from a violation of the provisions of this section shall be entitled to bring an individual action to recover damages and reasonable attorney fees.

CHAPTER 35.2.

SECURITY FOR CONNECTED DEVICES.

§ 59.1-444.4. Definitions.

A. As used in this chapter, unless the context requires otherwise:

"Authentication" means a method of verifying the authority of a user, process, or device to access resources in an information system.

"Connected device" means any device or other physical object that is capable of connecting directly or indirectly to the Internet.

"Consumer" means a person that purchases a connected device.

"Manufacturer" means the person that manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in the Commonwealth. For the purposes of this definition, a contract with another person to manufacture on the person's behalf does not include a contract only to purchase a connected device or a contract only to purchase and brand a connected device.

"Security feature" means a feature of a device designed to provide security for that device.

"Unauthorized access, destruction, use, modification, or disclosure" means access, destruction, use, modification, or disclosure that is not authorized by the consumer.

§ 59.1-444.5. Duties of manufacturers.

A. A manufacturer of a connected device shall equip the device with reasonable security features that are:

1. Appropriate to the nature and function of the connected device;

2. Appropriate to the information the connected device may collect, contain, or transmit;

3. Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure; and

4. In compliance with current standards and best practices as found within industry standards for cybersecurity and resiliency, including the Internet of Things (IoT) Security Guidance prepared by the Open Web Application Security Project Foundation and the Best Practice Guidelines prepared by the IoT Security Foundation.

B. Subject to all of the requirements of subsection A, if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature for purposes of subsection A if:

1 The preprogrammed passphrase is unique and randomized for each connected device manufactured;

2 The preprogrammed password will be at least 10 characters in length and contain at least three of the following:

a. At least one uppercase character;

b. At least one lowercase character;

c. At least one digit; and

d. At least one special character; or

3. The device contains a security feature that requires a user to generate a new means of authentication that meets the requirements listed in subdivisions 2 a through d before access is granted to the connected device for the first time or when the connected device is reset.

§ 59.1-444.6. Responsibility and accountability.

A. Manufacturers shall demonstrate conformity with industry standards for cybersecurity and resiliency, including providing to the Chief Information Officer of the Commonwealth an annual report of compliance with industry-recognized best practices as specified by organizations such as the Open Web Application Security Project Foundation and the IoT Security Foundation.

B. A provider of computing devices shall be liable for vulnerabilities that contribute to system breaches that compromise data when the provider fails to conform to the extent possible to industry standards for cybersecurity and resiliency described in subsection A.

§ 59.1-444.7. Transparency.

Manufacturers shall provide an opt-in forum or registration capability to allow consumers to know when a vulnerability or breach is discovered, based on specific devices or classes of devices. Manufacturers shall make patch notification and end-of-life support events easily obtainable by registered users of the manufacturer's connected devices.

§ 59.1-444.8. Notification.

When a manufacturer is aware of existing vulnerabilities that put more than 500 users at risk, the manufacturer shall notify the office of the Chief Information Officer of the Commonwealth and provide remediation steps, including patches, updates, and setting changes, to consumers without unreasonable delay.

§ 59.1-444.9. Limitations.

A. This chapter shall not be construed to impose any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses to add to a connected device.

B. This chapter shall not be construed to impose any duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications, to review or enforce compliance with this chapter.

C. This chapter shall not be construed to impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the user's discretion.

D. This chapter shall not apply to any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority.

E. The duties and obligations imposed by this chapter are cumulative with any other duties or obligations imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law.

F. This chapter shall not be construed to limit the authority of a law-enforcement agency to obtain connected device information from a manufacturer as authorized by law or pursuant to an order of a court of competent jurisdiction.

§ 59.1-444.10. Remedies; enforcement.

This chapter shall not be construed to provide a basis for a private right of action for any person, including a consumer or user of a connected device. The Attorney General, the attorney for the Commonwealth, or the attorney for a locality shall have the exclusive authority to enforce the provisions of this chapter by causing an action to be brought in the appropriate circuit court for injunctive relief of any violation of this chapter.

2. That the provisions of this act shall become effective on January 1, 2020.