

20100251D

HOUSE BILL NO. 954

Offered January 8, 2020

Prefiled January 7, 2020

A BILL to amend and reenact §§ 59.1-200 and 59.1-444 of the Code of Virginia and 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 Communications, Technology and Innovation

Be it enacted by the General Assembly of Virginia:

1. That §§ 59.1-200 and 59.1-444 of the Code of Virginia are amended and reenacted and 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:

§ 59.1-200. Prohibited practices.

A. The following fraudulent acts or practices committed by a supplier in connection with a consumer transaction are hereby declared unlawful:

1. Misrepresenting goods or services as those of another;
2. Misrepresenting the source, sponsorship, approval, or certification of goods or services;
3. Misrepresenting the affiliation, connection, or association of the supplier, or of the goods or services, with another;
4. Misrepresenting geographic origin in connection with goods or services;
5. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;
6. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model;
7. Advertising or offering for sale goods that are used, secondhand, repossessed, defective, blemished, deteriorated, or reconditioned, or that are "seconds," irregulars, imperfects, or "not first class," without clearly and unequivocally indicating in the advertisement or offer for sale that the goods are used, secondhand, repossessed, defective, blemished, deteriorated, reconditioned, or are "seconds," irregulars, imperfects or "not first class";
8. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell at the price or upon the terms advertised.

In any action brought under this subdivision, the refusal by any person, or any employee, agent, or servant thereof, to sell any goods or services advertised or offered for sale at the price or upon the terms advertised or offered, shall be prima facie evidence of a violation of this subdivision. This paragraph shall not apply when it is clearly and conspicuously stated in the advertisement or offer by which such goods or services are advertised or offered for sale, that the supplier or offeror has a limited quantity or amount of such goods or services for sale, and the supplier or offeror at the time of such advertisement or offer did in fact have or reasonably expected to have at least such quantity or amount for sale;

9. Making false or misleading statements of fact concerning the reasons for, existence of, or amounts of price reductions;

10. Misrepresenting that repairs, alterations, modifications, or services have been performed or parts installed;

11. Misrepresenting by the use of any written or documentary material that appears to be an invoice or bill for merchandise or services previously ordered;

12. Notwithstanding any other provision of law, using in any manner the words "wholesale," "wholesaler," "factory," or "manufacturer" in the supplier's name, or to describe the nature of the supplier's business, unless the supplier is actually engaged primarily in selling at wholesale or in manufacturing the goods or services advertised or offered for sale;

13. Using in any contract or lease any liquidated damage clause, penalty clause, or waiver of defense, or attempting to collect any liquidated damages or penalties under any clause, waiver, damages, or penalties that are void or unenforceable under any otherwise applicable laws of the Commonwealth, or under federal statutes or regulations;

13a. Failing to provide to a consumer, or failing to use or include in any written document or material provided to or executed by a consumer, in connection with a consumer transaction any

INTRODUCED

HB954

59 statement, disclosure, notice, or other information however characterized when the supplier is required
60 by 16 C.F.R. Part 433 to so provide, use, or include the statement, disclosure, notice, or other
61 information in connection with the consumer transaction;

62 14. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection
63 with a consumer transaction;

64 15. Violating any provision of § 3.2-6512, 3.2-6513, or 3.2-6516, relating to the sale of certain
65 animals by pet dealers which is described in such sections, is a violation of this chapter;

66 16. Failing to disclose all conditions, charges, or fees relating to:

67 a. The return of goods for refund, exchange, or credit. Such disclosure shall be by means of a sign
68 attached to the goods, or placed in a conspicuous public area of the premises of the supplier, so as to be
69 readily noticeable and readable by the person obtaining the goods from the supplier. If the supplier does
70 not permit a refund, exchange, or credit for return, he shall so state on a similar sign. The provisions of
71 this subdivision shall not apply to any retail merchant who has a policy of providing, for a period of not
72 less than 20 days after date of purchase, a cash refund or credit to the purchaser's credit card account
73 for the return of defective, unused, or undamaged merchandise upon presentation of proof of purchase.
74 In the case of merchandise paid for by check, the purchase shall be treated as a cash purchase and any
75 refund may be delayed for a period of 10 banking days to allow for the check to clear. This subdivision
76 does not apply to sale merchandise that is obviously distressed, out of date, post season, or otherwise
77 reduced for clearance; nor does this subdivision apply to special order purchases where the purchaser
78 has requested the supplier to order merchandise of a specific or unusual size, color, or brand not
79 ordinarily carried in the store or the store's catalog; nor shall this subdivision apply in connection with a
80 transaction for the sale or lease of motor vehicles, farm tractors, or motorcycles as defined in
81 § 46.2-100;

82 b. A layaway agreement. Such disclosure shall be furnished to the consumer (i) in writing at the time
83 of the layaway agreement, or (ii) by means of a sign placed in a conspicuous public area of the
84 premises of the supplier, so as to be readily noticeable and readable by the consumer, or (iii) on the bill
85 of sale. Disclosure shall include the conditions, charges, or fees in the event that a consumer breaches
86 the agreement;

87 16a. Failing to provide written notice to a consumer of an existing open-end credit balance in excess
88 of \$5 (i) on an account maintained by the supplier and (ii) resulting from such consumer's overpayment
89 on such account. Suppliers shall give consumers written notice of such credit balances within 60 days of
90 receiving overpayments. If the credit balance information is incorporated into statements of account
91 furnished consumers by suppliers within such 60-day period, no separate or additional notice is required;

92 17. If a supplier enters into a written agreement with a consumer to resolve a dispute that arises in
93 connection with a consumer transaction, failing to adhere to the terms and conditions of such an
94 agreement;

95 18. Violating any provision of the Virginia Health Club Act, Chapter 24 (§ 59.1-294 et seq.);

96 19. Violating any provision of the Virginia Home Solicitation Sales Act, Chapter 2.1 (§ 59.1-21.1 et
97 seq.);

98 20. Violating any provision of the Automobile Repair Facilities Act, Chapter 17.1 (§ 59.1-207.1 et
99 seq.);

100 21. Violating any provision of the Virginia Lease-Purchase Agreement Act, Chapter 17.4
101 (§ 59.1-207.17 et seq.);

102 22. Violating any provision of the Prizes and Gifts Act, Chapter 31 (§ 59.1-415 et seq.);

103 23. Violating any provision of the Virginia Public Telephone Information Act, Chapter 32
104 (§ 59.1-424 et seq.);

105 24. Violating any provision of § 54.1-1505;

106 25. Violating any provision of the Motor Vehicle Manufacturers' Warranty Adjustment Act, Chapter
107 17.6 (§ 59.1-207.34 et seq.);

108 26. Violating any provision of § 3.2-5627, relating to the pricing of merchandise;

109 27. Violating any provision of the Pay-Per-Call Services Act, Chapter 33 (§ 59.1-429 et seq.);

110 28. Violating any provision of the Extended Service Contract Act, Chapter 34 (§ 59.1-435 et seq.);

111 29. Violating any provision of the Virginia Membership Camping Act, Chapter 25 (§ 59.1-311 et
112 seq.);

113 30. Violating any provision of the Comparison Price Advertising Act, Chapter 17.7 (§ 59.1-207.40 et
114 seq.);

115 31. Violating any provision of the Virginia Travel Club Act, Chapter 36 (§ 59.1-445 et seq.);

116 32. Violating any provision of §§ 46.2-1231 and 46.2-1233.1;

117 33. Violating any provision of Chapter 40 (§ 54.1-4000 et seq.) of Title 54.1;

118 34. Violating any provision of Chapter 10.1 (§ 58.1-1031 et seq.) of Title 58.1;

119 35. Using the consumer's social security number as the consumer's account number with the supplier,
120 if the consumer has requested in writing that the supplier use an alternate number not associated with

the consumer's social security number;

36. Violating any provision of Chapter 18 (§ 6.2-1800 et seq.) of Title 6.2;

37. Violating any provision of § 8.01-40.2;

38. Violating any provision of Article 7 (§ 32.1-212 et seq.) of Chapter 6 of Title 32.1;

39. Violating any provision of Chapter 34.1 (§ 59.1-441.1 et seq.);

40. Violating any provision of Chapter 20 (§ 6.2-2000 et seq.) of Title 6.2;

41. Violating any provision of the Virginia Post-Disaster Anti-Price Gouging Act, Chapter 46 (§ 59.1-525 et seq.);

42. Violating any provision of Chapter 47 (§ 59.1-530 et seq.);

43. Violating any provision of § 59.1-443.2 or 59.1-443.4;

44. Violating any provision of Chapter 48 (§ 59.1-533 et seq.);

45. Violating any provision of Chapter 25 (§ 6.2-2500 et seq.) of Title 6.2;

46. Violating the provisions of clause (i) of subsection B of § 54.1-1115;

47. Violating any provision of § 18.2-239;

48. Violating any provision of Chapter 26 (§ 59.1-336 et seq.);

49. Selling, offering for sale, or manufacturing for sale a children's product the supplier knows or has reason to know was recalled by the U.S. Consumer Product Safety Commission. There is a rebuttable presumption that a supplier has reason to know a children's product was recalled if notice of the recall has been posted continuously at least 30 days before the sale, offer for sale, or manufacturing for sale on the website of the U.S. Consumer Product Safety Commission. This prohibition does not apply to children's products that are used, secondhand or "seconds";

50. Violating any provision of Chapter 44.1 (§ 59.1-518.1 et seq.);

51. Violating any provision of Chapter 22 (§ 6.2-2200 et seq.) of Title 6.2;

52. Violating any provision of § 8.2-317.1;

53. Violating subsection A of § 9.1-149.1;

54. Selling, offering for sale, or using in the construction, remodeling, or repair of any residential dwelling in the Commonwealth, any drywall that the supplier knows or has reason to know is defective drywall. This subdivision shall not apply to the sale or offering for sale of any building or structure in which defective drywall has been permanently installed or affixed;

55. Engaging in fraudulent or improper or dishonest conduct as defined in § 54.1-1118 while engaged in a transaction that was initiated (i) during a declared state of emergency as defined in § 44-146.16 or (ii) to repair damage resulting from the event that prompted the declaration of a state of emergency, regardless of whether the supplier is licensed as a contractor in the Commonwealth pursuant to Chapter 11 (§ 54.1-1100 et seq.) of Title 54.1;

56. Violating any provision of Chapter 33.1 (§ 59.1-434.1 et seq.);

57. Violating any provision of § 18.2-178, 18.2-178.1, or 18.2-200.1;

58. Violating any provision of Chapter 17.8 (§ 59.1-207.45 et seq.);

59. Violating any provision of subsection E of § 32.1-126; and

60. Violating any provision of § 54.1-111 relating to the unlicensed practice of a profession licensed under Chapter 11 (§ 54.1-1100 et seq.) or Chapter 21 (§ 54.1-2100 et seq.) of Title 54.1.

B. Nothing in this section shall be construed to invalidate or make unenforceable any contract or lease solely by reason of the failure of such contract or lease to comply with any other law of the Commonwealth or any federal statute or regulation, to the extent such other law, statute, or regulation provides that a violation of such law, statute, or regulation shall not invalidate or make unenforceable such contract or lease.

§ 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

182 general public from federal, state, or local government records.

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

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

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

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

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

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

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

208 **§ 59.1-444. Damages.**

209 A person aggrieved by a violation of any provision of this chapter, except § 59.1-443.2 or
210 59.1-443.4, shall be entitled to institute an action to recover damages in the amount of \$100 per
211 violation. In addition, if the aggrieved party prevails, he may be awarded reasonable attorney's fees and
212 court costs. Actions under this section shall be brought in the general district court for the city or county
213 in which the transaction or other violation that gave rise to the action occurred. A violation of the
214 provisions of § 59.1-443.2 or 59.1-443.4 is a prohibited practice under the Virginia Consumer Protection
215 Act (§ 59.1-196 et seq.).

216 **CHAPTER 35.2.**

217 **SECURITY FOR CONNECTED DEVICES.**

218 **§ 59.1-444.4. Definitions.**

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

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

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

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

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

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

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

233 **§ 59.1-444.5. Duties of manufacturers.**

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

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

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

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

240 4. In compliance with current standards and best practices as found within industry standards for
241 cybersecurity and resiliency, including the Internet of Things (IoT) Security Guidance prepared by the
242 Open Web Application Security Project Foundation and the Best Practice Guidelines prepared by the
243 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 will 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 Attorney General 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, civil penalties of not more than \$2,500 per violation, and reasonable attorney fees. Any civil penalty collected under this section shall be paid to the general fund.

2. That the provisions of this act shall become effective on January 1, 2021.