

HOUSE BILL NO. 2721

Offered January 12, 2005

Prefiled January 12, 2005

A BILL to amend and reenact § 59.1-444 of the Code of Virginia, and to amend the Code of Virginia by adding sections numbered 2.2-3808.4 and 59.1-443.2, relating to notice of breach of databases.

Patron-- Scott, J.M.

Referred to Committee on Science and Technology

Be it enacted by the General Assembly of Virginia:

§ 59.1-443.2. Notice of breach of information system.

A. As used in this section:

“Breach of the security of the system” means unauthorized access and acquisition of computerized data that compromises the security or confidentiality, or integrity of personal information maintained by the person as part of a database of personal information regarding multiple individuals and that causes or the person reasonable believes has caused or will cause identity theft or physical harm to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person 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 person and is not ~~or~~ subject to further unauthorized disclosure.

“Person” shall have the same meaning as defined in § 1-13.19; ~~however, person shall not include an agency as that term is defined in § 2.2-3801.~~

“Encryption.” The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

“Redact.” The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, or financial account number is accessible as part of the data.

“Personal information” means an individual’s first name or first initial and last name in combination with and linked to any one or more of the following data elements, when ~~either~~ or the data elements are not encrypted, redacted r secured by any other method or technology that renders the personal information unreadable or unusable: (i) social security number; (ii) driver’s license number; or, (iii) Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account. For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

B.

1. Any person that conducts business in the Commonwealth, and 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 in the security of the data to any

resident of the Commonwealth whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person and that causes or the person reasonable believes has caused or will cause identity theft or physical harm to any resident of the Commonwealth. The disclosure 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, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

2. A person must disclose the breach 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.

C. Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as practicable immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.

D. The notification required by this section may be delayed if a law-enforcement agency determines, and advises the person, that the notification will impede a criminal or civil investigation. The notification required by this section shall be made after the law-enforcement agency determines that it will not compromise the investigation or national or homeland security. However, if after an investigation by the person or law enforcement agency, there is no reasonable belief that the personal information so acquired will be used in any unlawful manner, no notification shall be required by this section.

E. Notice may be provided by one of the following methods:

1. Written notice.

2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 701 of the Electronic Signatures in Global and National Commerce Act (Public Law 106-229, 15 U.S.C. § 7001), the Uniform Electronic Transactions Act (§ 59.1-479 et seq.).

3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$50,000 ~~\$250,000~~, or that the affected class of subject persons to be notified exceeds 100,000 ~~500,000~~, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:

a. E-mail notice when the person has an e-mail address for the subject persons,

b. Conspicuous posting of the notice on the Internet website of the person, if the person maintains one, and

c. Notification to major statewide media.

F. Notwithstanding subsection E, a person that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is ~~otherwise~~ consistent with the timing requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.

G. When a person provides notification under this Act to more than 1,000 individuals at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in Section 603 of the Fair Credit Reporting Act (PUBLIC LAW 91-508, 15 U.S.C. § 1681A), of the timing, distribution, and number of notices. ~~If a person, upon providing a disclosure pursuant to this section, indicates that the individual may obtain a copy of his credit report from a consumer reporting agency, the person shall consult the consumer reporting agency as to the timing, content and distribution of the disclosure.~~

H. This act deals with subject matter that is of concern to the entire Commonwealth, and it is the intent of the General Assembly that this Act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within this Commonwealth regarding the matters expressly set forth in this Act.

§ 59.1-444. Damages; Injunction.

A. A violation of this Act that results in injury or loss to residents of this Commonwealth may be enforced by the Office of the Attorney General as an unfair trade practice pursuant to section.

The Office of Attorney General shall have exclusive authority to bring action and may obtain either actual damages for a violation of this Act or a civil penalty not to exceed \$150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation. ~~A person aggrieved by a violation of this chapter shall be entitled to institute an action to recover damages in the amount of \$100 per violation or actual damages, whichever is greater.~~

~~B. In addition, if If the aggrieved party prevails, he may be awarded reasonable attorney's fees and court costs.~~

~~C. The provisions of this chapter may be enforced by injunction or any other available equitable or legal remedy.~~

~~D. Actions under this section shall be brought in the general district court for the city or county in which the transaction or other violation that gave rise to the action occurred.~~

B.E. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

§ 59.1-445. Applicability.

This act shall apply to the discovery or notification of a breach of the security of the system that occurs on or after the effective date of this section.

§ 59.1-446. Effective Date

This act shall take effect in 120 days