

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:

1. That § 59.1-444 of the Code of Virginia is amended and reenacted, and that the Code of Virginia is amended by adding sections numbered 2.2-3808.4 and 59.1-443.2 as follows:

§ 2.2-3808.4. *Notice of breach.*

A. *As used in this section:*

“Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an agency. Good faith acquisition of personal information by an employee or agent of an agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

“Personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (i) social security number; (ii) Virginia driver’s license number; or, (iii) 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 chapter, “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. *Any agency that owns or licenses computerize 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 Virginia whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. 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 subdivision D of this subsection, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the information system.*

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

D. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation. 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 7001 of Title 15 of the United States Code.

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

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

b. Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one, and

c. Notification to major statewide media.

F. Notwithstanding subsection E, an agency that maintains its own notification procedures as part of an information 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 it notifies subject persons in accordance with its policies in the event of a breach of security.

G. If an agency, 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 agency shall consult the consumer reporting agency as to the timing, content and distribution of the disclosure.

§ 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 acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person. 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 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.

“Personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (i) social security number; (ii) driver’s license number; or, (iii) 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. 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 personal information was, or is reasonably believed to have been, acquired by an unauthorized person. 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.

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 immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

D. The notification required by this section may be delayed if a law-enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law-enforcement agency determines that it will not compromise the investigation. 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 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 \$250,000, or that the affected class of subject persons to be notified exceeds 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 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 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. 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.

§ 59.1-444. Damages; Injunction.

A. 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.

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