

086219724

HOUSE BILL NO. 971

Offered January 9, 2008

Prefiled January 8, 2008

A *BILL to amend the Code of Virginia by adding a section numbered 18.2-186.6, relating to identity theft prevention; notice of breach of information system.*

Patron—Shannon

Referred to Committee for Courts of Justice

Be it enacted by the General Assembly of Virginia:**1. That the Code of Virginia is amended by adding a section numbered 18.2-186.6 as follows:**

§ 18.2-186.6. Notice of breach of information system.

A. *As used in this section:*

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

"Notice" means:

1. *Written notice;*

2. *Telephonic notice;*

3. *Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or*

4. *Substitute notice, if the person or business 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 residents, or the person or business does not have sufficient contact information. Substitute notice consists of all of the following: (i) email notice when the person or business has an email address for the subject persons, (ii) conspicuous posting of the notice on the website of the person or business, if the person or business maintains one, and (iii) notification to major statewide media.*

"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:

1. *Social Security number;*

2. *Driver's license number or other state identification card number; or*

3. *Account number, or 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.*

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

B. *Any person or business that conducts business in Virginia and that owns or licenses computerized data that includes personal information shall, when it becomes aware of an incident of unauthorized access to personal customer information, conduct a reasonable investigation to promptly determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about a customer has occurred or is reasonably possible, the person or business shall notify the affected customer as soon as possible. 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 E and consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, or to restore the reasonable integrity of the data system.*

C. *A person or business that maintains computerized data that includes personal information that the person or business does not own shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was acquired by an unauthorized person. Such cooperation shall include sharing information relevant to the breach with the owner or licensee.*

D. *A person or business shall not be required to disclose a breach of the security of the system if the person, business, or enforcement agency, after a reasonable and prompt investigation, determines that misuse of information about a customer has not occurred or is not reasonably possible and implements reasonable procedures to safeguard the interests of affected customers.*

INTRODUCED

HB971

59 *E. Notice required by this section may be delayed if a law-enforcement agency determines that the*
60 *notice will impede a criminal investigation. Notice required by this section shall be made after the*
61 *law-enforcement agency determines that it will not compromise the investigation.*

62 *F. Under this section, a person or business that maintains its own notice procedures as part of an*
63 *information security policy for the treatment of personal information, and whose procedures are*
64 *otherwise consistent with the timing requirements of this section is deemed to be in compliance with the*
65 *notice requirements of this section if the person or business notifies subject persons in accordance with*
66 *its policies in the event of a breach of security of the system.*

67 *G. Under this section, an individual or a commercial entity that is regulated by state or federal law*
68 *and that maintains procedures for a breach of the security of the system pursuant to the laws, rules,*
69 *regulations, or guidelines established by its primary or functional state or federal regulator is deemed to*
70 *be in compliance with this chapter if the individual or the commercial entity notifies affected Virginia*
71 *residents in accordance with the maintained procedures when a breach occurs.*

72 *H. Any customer injured by a violation of this section may institute a civil action to recover actual*
73 *damages or to enjoin any business that violates or has violated this section.*

74 *I. A financial institution that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801*
75 *et seq.) and maintains procedures for notification of a breach of the security of the system in*
76 *accordance with the provisions of this section and any rules, regulations, or guidelines promulgated*
77 *thereto, shall be deemed to be in compliance with this section.*