

085686448

HOUSE BILL NO. 1469

Offered January 16, 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.*

Patrons—Byron, Merricks and Shannon

Referred to Committee on Science and Technology

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. Breach of personal information notification.

A. As used in this section:

"Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity 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 individual or entity or subject to further unauthorized disclosure.

"Encrypted" means the transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or the securing of the information by another method that renders the data elements unreadable or unusable.

"Entity" includes corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities or any other legal entity, whether for profit or not for profit.

"Financial institution" has the meaning given that term in 15 U.S.C § 6809(3).

"Individual" means a natural person.

"Notice" means:

(1) Written notice to the postal address in the records of the individual or entity;

(2) Telephone notice;

(3) Electronic notice; or

(4) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this subsection. Substitute notice consists of any two of the following:

a. E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

b. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the commercial entity maintains a website; and

c. Notice to major statewide media.

Notice required by this section shall not be considered a communication as defined by the Fair Debt Collection Practices Act in 15 U.S.C. § 1692a.

"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

1. Social Security Number;

2. Driver's license number or state identification card number issued in lieu of a driver's license; or

3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

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

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

1. Five digits of a social security number; or

INTRODUCED

HB1469

59 2. The last four digits of a driver's license number, state identification card number, or account
60 number.

61 B. An individual or entity that owns or licenses computerized data that includes personal information
62 shall disclose any breach of the security of the system following discovery or notification of the breach
63 of the security of the system to any resident of the Commonwealth whose unencrypted and unredacted
64 personal information was or is reasonably believed to have been accessed and acquired by an
65 unauthorized person and that causes, or the individual or entity reasonably believes has caused or will
66 cause, identity theft or another fraud to any resident of the Commonwealth. Except as provided in
67 subsection E or in order to take any measures necessary to determine the scope of the breach and to
68 restore the reasonable integrity of the system, the disclosure shall be made without unreasonable delay.

69 C. An individual or entity must disclose the breach of the security system if encrypted information is
70 accessed and acquired in an unencrypted form, or if the security breach involves a person with access
71 to the encryption key and the individual or entity reasonably believes that such a breach has caused or
72 will cause identity theft or other fraud to any resident of the Commonwealth.

73 D. An individual or entity that maintains computerized data that included personal information that
74 the individual or entity does not own or license shall notify the owner or licensee of the information of
75 any breach of the security of the system as soon as practicable following discovery, if the personal
76 information was accessed and acquired by an unauthorized person or the entity reasonably believes the
77 personal information was accessed and acquired by an unauthorized person.

78 E. Notice required by this section may be delayed if a law-enforcement agency determines and
79 advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland
80 or national security. Notice required by this section must be made without unreasonable delay after the
81 law-enforcement agency determines that the notification will no longer impede the investigation or
82 jeopardize national or homeland security.

83 F. An entity that maintains its own notification procedures as part of an information privacy or
84 security policy for the treatment of personal information that are consistent with the timing requirements
85 of this section shall be deemed to be in compliance with the notification requirements of this section if it
86 notifies residents of the Commonwealth in accordance with its procedures in the event of a breach of
87 the security of the system.

88 G. A financial institution that is subject to Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801
89 et seq.) and maintains procedures for notification of a breach of the security of the system in
90 accordance with the provision of this section and any rules, regulations, or guidelines promulgated
91 thereto shall be deemed to be in compliance with this section.

92 H. An entity that complies with the notification requirements or procedures pursuant to the rules,
93 regulations, procedures, or guidelines established by the entity's primary or functional federal regulator
94 shall be in compliance with this section.

95 I. A violation of this section that results in injury or loss to residents of the Commonwealth may be
96 enforced by the Office of the Attorney General. Except as provided by subsection J, the Office of the
97 Attorney General shall have exclusive authority to bring action and may obtain either actual damages
98 for a violation of this section or a civil penalty not to exceed \$150,000 per breach of the security of the
99 system or a series of breaches of a similar nature that are discovered in a single investigation.

100 J. A violation of this section by a state-chartered or licensed financial institution shall be enforceable
101 exclusively by the financial institution's primary state regulator.