

088104444

HOUSE BILL NO. 390

Offered January 9, 2008

Prefiled January 4, 2008

A BILL to amend and reenact § 2.2-603 of the Code of Virginia and to amend the Code of Virginia by adding in Title 2.2 a chapter numbered 38.1, consisting of sections numbered 2.2-3820 and 2.2-3821, relating to the Compromised Data Notification Act.

Patrons—Bulova and Plum

Referred to Committee on General Laws

Be it enacted by the General Assembly of Virginia:

1. That § 2.2-603 of the Code of Virginia is amended and reenacted and that the Code of Virginia is amended by adding in Title 2.2 a chapter numbered 38.1, consisting of sections numbered 2.2-3820 and 2.2-3821, as follows:

§ 2.2-603. Authority of agency directors.

A. Notwithstanding any provision of law to the contrary, the agency director of each agency in the executive branch of state government shall have the power and duty to (i) supervise and manage the department or agency and (ii) prepare, approve, and submit to the Governor all requests for appropriations and to be responsible for all expenditures pursuant to appropriations.

B. The director of each agency in the executive branch of state government, except those that by law are appointed by their respective boards, shall not proscribe any agency employee from discussing the functions and policies of the agency, without prior approval from his supervisor or superior, with any person unless the information to be discussed is protected from disclosure by the Virginia Freedom of Information Act (§ 2.2-3700 et seq.) or any other provision of state or federal law.

C. Subsection A shall not be construed to restrict any other specific or general powers and duties of executive branch boards granted by law.

D. This section shall not apply to those agency directors that are appointed by their respective boards or by the Board of Education. Directors appointed in this manner shall have the powers and duties assigned by law or by the board.

E. In addition to the requirements of subsection C of § 2.2-619, the director of each agency in any branch of state government shall, at the end of each fiscal year, report to (i) the Secretary of Finance and the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance a listing and general description of any federal contract, grant, or money in excess of \$1,000,000 for which the agency was eligible, whether or not the agency applied for, accepted, and received such contract, grant, or money, and, if not, the reasons therefore and the dollar amount and corresponding percentage of the agency's total annual budget that was supplied by funds from the federal government and (ii) the Chairmen of the House Committees on Appropriations and Finance, and the Senate Committee on Finance any amounts owed to the agency from any source that are more than six months delinquent, the length of such delinquencies, and the total of all such delinquent amounts in each six-month interval. Clause (i) shall not be required of public institutions of higher education.

F. The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, incidents described in § 2.2-3821, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence.

CHAPTER 38.1.

COMPROMISED DATA NOTIFICATION ACT.

§ 2.2-3820. Findings; definitions.

A. The General Assembly finds that the Commonwealth, as steward of sensitive personal information, has an obligation to notify in a timely manner any individual whose personal information has been compromised and where harm to that individual could reasonably be expected as a consequence.

B. As used in this chapter:

"Agency" means an administrative unit of state government, including any department, institution, commission, board, council, authority, or other body, however designated.

"Breach of the security of a system" means the unauthorized acquisition or release of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information

INTRODUCED

HB390

59 *maintained by an agency. Good faith acquisition or release of personal information by an employee or*
60 *agent of an agency for the purposes of the agency shall not constitute a breach of the security of a*
61 *system provided the personal information is not used for or is not subject to further unauthorized*
62 *disclosure.*

63 *"Notice" means written or telephonic notice; electronic notice, if such notice provided is consistent*
64 *with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or*
65 *substitute notice, if the agency required to provide notice demonstrates that the cost of providing notice*
66 *will exceed \$75,000, or that the affected class of Virginia residents to be notified exceeds 100,000*
67 *residents, or that the agency does not have sufficient contact information to provide notice. Substitute*
68 *notice shall include (i) e-mail notice, if the agency has e-mail addresses for the members of the affected*
69 *class of Virginia residents, (ii) conspicuous posting of the notice on the website of the agency if it*
70 *maintains one, and (iii) notification to major statewide media.*

71 *"Personal information" means the first name or first initial and last name of an individual in*
72 *combination with any one or more of the following data elements, when either the name or the data*
73 *elements are not encrypted: (i) social security number; (ii) driver's license number or identification card*
74 *number; (iii) medical or educational records; or (iv) account number, credit card, or debit card number,*
75 *in combination with any required security code, access code, or password that would permit access to*
76 *the financial account of an individual.*

77 *§ 2.2-3821. Obligation of state agencies.*

78 *Following discovery or notification of a breach of a security system an agency that owns or licenses*
79 *computerized data that includes personal information shall provide notice of the breach to all residents*
80 *of Virginia whose unencrypted personal information was or is reasonably believed to have been*
81 *acquired by an unauthorized person. The notice shall be given in the most expedient time possible and*
82 *without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures*
83 *necessary to determine the scope of the breach and restore the reasonable integrity of the system.*