GENERAL ASSEMBLY OF NORTH CAROLINA

SESSION 2005

S **1**

SENATE BILL 783

Short Title:	Report Hacker/Fraudulent Access to ID Data.	(Public)
Sponsors:	Senators Forrester; Allran, Bingham, Brock, Garwood, Goodall, Hunt, Presnell, and Tillman.	
Referred to:	Commerce.	

March 23, 2005

A BILL TO BE ENTITLED

AN ACT REQUIRING THAT DATA AGGREGATORS AND OTHER BUSINESSES IMMEDIATELY NOTIFY INDIVIDUALS OF UNAUTHORIZED OR FRAUDULENT ACCESS TO PERSONAL INFORMATION FOLLOWING INFORMATION SECURITY BREACHES.

The General Assembly of North Carolina enacts:

SECTION 1. Chapter 66 of the General Statutes is amended by adding a new Article to read:

"Article 41.

"Personal Information Security Breach Notification Act.

"**§ 66-335. Definitions.**

The following definitions apply in this Article:

(1) Business. – A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this State, any other state, the United States, or of any other country, or the parent or the subsidiary of a financial institution.

(2) Breach of the security system. – Unauthorized or fraudulent acquisition of computerized data that (i) compromises the security, confidentiality, or integrity of personal information maintained by a business or (ii) could result in identity theft. Good faith acquisition of personal information by an employee or agent of a business for the purposes of the business is not a breach of the security of the system, provided that the personal information is not used or subject to unauthorized disclosure.

(3) Customer. – An individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

(4) Data aggregator. – A type of business that compiles personal information on individuals for sale to other businesses and entities, whether or not the individuals have given permission to obtain the personal information.

(5) Individual. – A natural person.

(6) Owns or licenses. – The phrase includes personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.

(7) Personal information. – Any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, drivers license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(8) Records. – Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

"**§ 66-336. Legislative intent; purposes.**

It is the intent of the General Assembly to protect the personal information of North Carolina residents. The purposes of this Article are (i) to encourage data aggregators, and businesses that own or license personal information about North Carolina customers, to provide reasonable security for personal information and (ii) to provide our citizens with notice of breaches of personal information security so the citizens can better protect themselves from fraud and identity theft.

"**§ 66-337. Protection of personal information required.**

(a) A data aggregator or other business that conducts business in North Carolina and compiles, owns, or licenses personal information about a North Carolina resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information in order to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(b) A business that conducts business in North Carolina and discloses personal information about a North Carolina resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information in order to protect the personal information from unauthorized or fraudulent access, destruction, use, modification, or disclosure.

"**§ 66-338. Notice of personal information security breach required; forms of notice; substantial compliance.**

(a) Any data aggregator or other business that conducts business in North Carolina, and that compiles or 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 North Carolina whose unencrypted personal information was or is reasonably believed to have been either acquired by an unauthorized person or by fraudulent means. Except as provided by subsection (b) of this section, the disclosure required shall be made in the most expedient time possible and without unreasonable delay. Any business or data aggregator that maintains computerized data that includes personal information that the business 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 or by fraudulent means.

(b) The notification required by this section may be delayed only if:

(1) A law enforcement agency determines that the notification will impede a criminal investigation or the delay. In this case, the notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(2) The delay is consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(c) For purposes of this section, notice may be provided by one of the following methods:

(1) Written notice to each affected individual by U.S. Mail.

(2) Electronic notice to each affected individual, if the notice provided is consistent with the provisions of Article 40 of this Chapter, the Uniform Electronic Transactions Act.

(3) Substitute notice, if (i) the business demonstrates that the cost of providing notice would exceed one hundred twenty-five thousand dollars ($125,000), (ii) the affected class of subject persons to be notified exceeds 250,000, or (iii) the business does not have sufficient contact information. Substitute notice shall be given when all of the following occur:

a. Electronic mail notice is given when the business has valid e-mail addresses for the subject persons.

b. Conspicuous posting of the notice is placed on the Web site page of the business, if the business maintains one.

c. Notification is provided through major Statewide media.

(d) Notwithstanding the provisions of subsection (c) of this section, a business that is not a data aggregator and that maintains its own customer notification procedures as part of an information security policy for the treatment of personal information that is otherwise consistent with the scope and timing requirements of this section shall be deemed to be in substantial compliance with the notification requirements of this section if the business notifies customers in accordance with its policies in the event of a breach of security of the system.

(e) In addition to, and contemporaneous with, the notice to individuals required by this section, a business shall notify the Consumer Protection Division of the Office of the Attorney General of North Carolina whenever there is a breach of the security system.

"**§ 66-339. Penalties.**

(a) An individual may bring a civil action against a business that fails to provide the notice required by this Article and may recover actual damages resulting from the failure to notify.

(b) Any business that violates this Article shall be liable for civil penalties as follows:

(1) In the amount of one hundred thousand dollars ($100,000) for the first offense.

(2) In the amount of one hundred fifty thousand dollars ($150,000) for the second offense.

(3) In the amount of three hundred thousand dollars ($300,000) for the third and subsequent offenses.

"**§ 66-340. Exceptions.**

(a) The provisions of this Article do not apply to any of the following:

(1) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(2) A business that is regulated by any State or federal law providing greater protection to personal information than that provided by this Article in regard to the subjects addressed by this Article. Compliance with that State or federal law shall be deemed compliance with this section with regard to those subjects.

(b) This section does not relieve a business from a duty to comply with any other requirements of other State and federal law regarding the protection and privacy of personal information."

SECTION 2. This act becomes effective January 1, 2006.