

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2005

S

D

SENATE DRS35133-LR-49 (02/22)

Short Title: Report Hacker/Fraudulent Access to ID Data. (Public)

Sponsors: Senator Forrester.

Referred to:

1 A BILL TO BE ENTITLED
2 AN ACT REQUIRING THAT DATA AGGREGATORS AND OTHER BUSINESSES
3 IMMEDIATELY NOTIFY INDIVIDUALS OF UNAUTHORIZED OR
4 FRAUDULENT ACCESS TO PERSONAL INFORMATION FOLLOWING
5 INFORMATION SECURITY BREACHES.

6 The General Assembly of North Carolina enacts:

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

9 "Article 41.

10 "Personal Information Security Breach Notification Act.

11 "§ 66-335. Definitions.

12 The following definitions apply in this Article:

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

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

- 1 (3) Customer. – An individual who provides personal information to a
2 business for the purpose of purchasing or leasing a product or
3 obtaining a service from the business.
- 4 (4) Data aggregator. – A type of business that compiles personal
5 information on individuals for sale to other businesses and entities,
6 whether or not the individuals have given permission to obtain the
7 personal information.
- 8 (5) Individual. – A natural person.
- 9 (6) Owns or licenses. – The phrase includes personal information that a
10 business retains as part of the business' internal customer account or
11 for the purpose of using that information in transactions with the
12 person to whom the information relates.
- 13 (7) Personal information. – Any information that identifies, relates to,
14 describes, or is capable of being associated with a particular
15 individual, including his or her name, signature, social security
16 number, physical characteristics or description, address, telephone
17 number, passport number, drivers license or state identification card
18 number, insurance policy number, education, employment,
19 employment history, bank account number, credit card number, debit
20 card number, or any other financial information. Personal information
21 does not include publicly available information that is lawfully made
22 available to the general public from federal, state, or local government
23 records.
- 24 (8) Records. – Any material, regardless of the physical form, on which
25 information is recorded or preserved by any means, including in
26 written or spoken words, graphically depicted, printed, or
27 electromagnetically transmitted. The term does not include publicly
28 available directories containing information an individual has
29 voluntarily consented to have publicly disseminated or listed, such as
30 name, address, or telephone number.

31 **"§ 66-336. Legislative intent; purposes.**

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

38 **"§ 66-337. Protection of personal information required.**

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

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

7 **"§ 66-338. Notice of personal information security breach required; forms of**
8 **notice; substantial compliance.**

9 (a) Any data aggregator or other business that conducts business in North
10 Carolina, and that compiles or owns or licenses computerized data that includes
11 personal information, shall disclose any breach of the security of the system following
12 discovery or notification of the breach in the security of the data to any resident of
13 North Carolina whose unencrypted personal information was or is reasonably believed
14 to have been either acquired by an unauthorized person or by fraudulent means. Except
15 as provided by subsection (b) of this section, the disclosure required shall be made in
16 the most expedient time possible and without unreasonable delay. Any business or data
17 aggregator that maintains computerized data that includes personal information that the
18 business does not own shall notify the owner or licensee of the information of any
19 breach of the security of the data immediately following discovery, if the personal
20 information was or is reasonably believed to have been acquired by an unauthorized
21 person or by fraudulent means.

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

- 23 (1) A law enforcement agency determines that the notification will impede
24 a criminal investigation or the delay. In this case, the notification
25 required by this section shall be made after the law enforcement
26 agency determines that it will not compromise the investigation.
27 (2) The delay is consistent with any measures necessary to determine the
28 scope of the breach and restore the reasonable integrity of the data
29 system.

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

- 32 (1) Written notice to each affected individual by U.S. Mail.
33 (2) Electronic notice to each affected individual, if the notice provided is
34 consistent with the provisions of Article 40 of this Chapter, the
35 Uniform Electronic Transactions Act.
36 (3) Substitute notice, if (i) the business demonstrates that the cost of
37 providing notice would exceed one hundred twenty-five thousand
38 dollars (\$125,000), (ii) the affected class of subject persons to be
39 notified exceeds 250,000, or (iii) the business does not have sufficient
40 contact information. Substitute notice shall be given when all of the
41 following occur:
42 a. Electronic mail notice is given when the business has valid
43 e-mail addresses for the subject persons.

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

3 c. Notification is provided through major Statewide media.

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

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

15 "§ 66-339. Penalties.

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

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

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

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

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

27 "§ 66-340. Exceptions.

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

29 (1) A covered entity governed by the medical privacy and security rules
30 issued by the federal Department of Health and Human Services, Parts
31 160 and 164 of Title 45 of the Code of Federal Regulations,
32 established pursuant to the Health Insurance Portability and
33 Availability Act of 1996 (HIPAA).

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

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

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