

North Carolina General Statutes

Chapter 75 – Monopolies, Trusts, and Consumer Protection

Article 2A – Identity Theft Protection Act

§ 75-60. Title.

This Article shall be known and may be cited as the "Identity Theft Protection Act".

§ 75-61. 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. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency.

(2) "Consumer". – An individual.

(3) "Consumer report" or "credit report". – Any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for any of the following:

- a. Credit to be used primarily for personal, family, or household purposes.
- b. Employment purposes.
- c. Any other purpose authorized under 15 U.S.C. § 1681(b).

(4) "Consumer reporting agency". – Any person who, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

(5) "Credit card". – Has the same meaning as in section 103 of the Truth in Lending Act (15 U.S.C. § 160, et seq.).

(6) "Debit card". – Any card or device issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account holding assets of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money, property, labor, or services.

(7) "Disposal" includes the following:

- a. The discarding or abandonment of records containing personal information.

- b. The sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of personal information, or other nonpaper media upon which records of personal information are stored, or other equipment for nonpaper storage of information.
- (8) "Encryption". – The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.
- (9) "Person". – Any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.
- (10) "Personal information". – A person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.
- (11) "Proper identification". – Information generally deemed sufficient to identify a person. If a person is unable to reasonably identify himself or herself with the information described above, a consumer reporting agency may require additional information concerning the consumer's employment and personal or family history in order to verify the consumer's identity.
- (12) "Records". – Any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.
- (13) "Redaction". – The rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data.
- (14) "Security breach". – An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.
- (15) "Security freeze". – Notice placed in a credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer reporting agency from

releasing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer.

§ 75-64. Destruction of personal information records.

(a) Any business that conducts business in North Carolina and any business that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.

(b) The reasonable measures must include:

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed.

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed.

(3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity.

(c) A business may, after due diligence, enter into a written contract with, and monitor compliance by, another party engaged in the business of record destruction to destroy personal information in a manner consistent with this section. Due diligence should ordinarily include one or more of the following:

(1) Reviewing an independent audit of the disposal business's operations or its compliance with this statute or its equivalent.

(2) Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review.

(3) Reviewing and evaluating the disposal business's information security policies or procedures or taking other appropriate measures to determine the competency and integrity of the disposal business.

(d) A disposal business that conducts business in North Carolina or disposes of personal information of residents of North Carolina must take all reasonable measures to dispose of records containing personal information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of

personal information during or after the collection and transportation and disposing of such information.

(e) This section does not apply to any of the following:

(1) Any bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm Leach Bliley Act, 15 U.S.C. § 6801, et seq., as amended.

(2) Any health insurer or health care facility that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996.

(3) Any consumer reporting agency that is subject to and in compliance with the Federal Credit Reporting Act, 15 U.S.C. § 1681, et seq., as amended.

(f) A violation of this section is a violation of G.S. 75-1.1, but any damages assessed against a business because of the acts or omissions of its nonmanagerial employees shall not be trebled as provided in G.S. 75-16 unless the business was negligent in the training, supervision, or monitoring of those employees. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.

§ 75-65. Protection from security breaches.

(a) Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach. The disclosure notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (c) of this section, and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. For the purposes of this section, personal information shall not include electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.

(b) Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section.

(c) The notice required by this section shall be delayed if a law enforcement agency informs the business that notification may impede a criminal investigation or jeopardize national or homeland security, provided that such request is made in writing or the business documents such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. The notice required by this section shall be provided without unreasonable delay after the law enforcement agency communicates to the business its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

(d) The notice shall be clear and conspicuous. The notice shall include a description of the following:

- (1) The incident in general terms.
- (2) The type of personal information that was subject to the unauthorized access and acquisition.
- (3) The general acts of the business to protect the personal information from further unauthorized access.
- (4) A telephone number that the person may call for further information and assistance, if one exists.
- (5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

(e) For purposes of this section, notice to affected persons may be provided by one of the following methods:

- (1) Written notice.
- (2) Electronic notice, for those persons for whom it has a valid e-mail address and who have agreed to receive communications electronically if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001.
- (3) Telephonic notice provided that contact is made directly with the affected persons.
- (4) Substitute notice, if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2), or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- a. E-mail notice when the business has an electronic mail address for the subject persons.
- b. Conspicuous posting of the notice on the Web site page of the business, if one is maintained.
- c. Notification to major statewide media.

(f) In the event a business provides notice to more than 1,000 persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

(g) Any waiver of the provisions of this Article is contrary to public policy and is void and unenforceable.

(h) A financial institution that is subject to and in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance, shall be deemed to be in compliance with this section.

(i) A violation of this section is a violation of G.S. 75-1.1. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.

(j) Causes of action arising under this Article may not be assigned.