GENERAL ASSEMBLY OF NORTH CAROLINA

SESSION 2005

S **4**

SENATE BILL 1048

Judiciary I Committee Substitute Adopted 5/23/05
House Committee Substitute Favorable 7/26/05
Fourth Edition Engrossed 8/22/05

Short Title: Identity Theft Protection Act of 2005.	(Public)
Sponsors:	
Referred to:	

March 24, 2005

A BILL TO BE ENTITLED

AN ACT ENACTING THE IDENTITY THEFT PROTECTION ACT OF 2005.

The General Assembly of North Carolina enacts:

SECTION 1. Chapter 75 of the General Statutes is amended by adding a new Article to read:

"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 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.

(4) "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. § 168l(b).

(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.

"**§ 75-62. Social security number protection.**

(a) Except as provided in subsection (b) of this section, a business may not do any of the following:

(1) Intentionally communicate or otherwise make available to the general public an individual's social security number.

(2) Intentionally print or imbed an individual's social security number on any card required for the individual to access products or services provided by the person or entity.

(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.

(5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed.

(6) Sell, lease, loan, trade, rent, or otherwise intentionally disclose an individual's social security number to a third party without written consent to the disclosure from the individual, when the party making

the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's social security number.

(b) Subsection (a) of this section shall not apply in the following instances:

(1) When a social security number is included in an application or in documents related to an enrollment process, or to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the social security number for the purpose of obtaining a credit report pursuant to 15 U.S.C. § 1681(b)(2). A social security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

(2) To the collection, use, or release of a social security number for internal verification or administrative purposes.

(3) To the opening of an account or the provision of or payment for a product or service authorized by an individual.

(4) To the collection, use, or release of a social security number to investigate or prevent fraud, conduct background checks, conduct social or scientific research, collect a debt, obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq., undertake a permissible purpose enumerated under Gramm Leach Bliley, 12 C.F.R. § 216.13-15, or locate an individual who is missing, a lost relative, or due a benefit, such as a pension, insurance, or unclaimed property benefit.

(5) To a business acting pursuant to a court order, warrant, subpoena, or when otherwise required by law.

(6) To a business providing the social security number to a federal, state, or local government entity, including a law enforcement agency, court, or their agents or assigns.

(7) To a social security number that has been redacted.

(c) A business covered by this section shall make reasonable efforts to cooperate, through systems testing and other means, to ensure that the requirements of this Article are implemented.

(d) A violation of this section is a violation of G.S. 75-1.1.

"**§ 75-63. Security freeze.**

(a) A consumer may place a security freeze on the consumer's credit report by making a request in writing by certified mail to a consumer reporting agency. A security freeze shall prohibit, subject to exceptions in subsection (l) of this section, the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. When a security freeze is in place, a consumer reporting agency may not release the consumer's credit report or information to a third party without prior express authorization from the consumer. This subsection

does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report.

(b) A consumer reporting agency shall place a security freeze on a consumer's credit report no later than five business days after receiving a written request from the consumer.

(c) The consumer reporting agency shall send a written confirmation of the security freeze to the consumer within 10 business days of placing the freeze and at the same time shall provide the consumer with a unique personal identification number or password, other than the consumer's social security number, to be used by the consumer when providing authorization for the release of the consumer's credit report for a specific period of time.

(d) If the consumer wishes to allow the consumer's credit report to be accessed for a specific period of time while a freeze is in place, the consumer shall contact the consumer reporting agency, request that the freeze be temporarily lifted, and provide all of the following:

(1) Proper identification.

(2) The unique personal identification number or password provided by the consumer reporting agency pursuant to subsection (c) of this section.

(3) The proper information regarding the time period for which the report shall be available to users of the credit report.

(e) A consumer reporting agency may develop procedures involving the use of telephone, fax, the Internet, or other electronic media to receive and process a request from a consumer to temporarily lift a freeze on a credit report pursuant to subsection (d) of this section in an expedited manner.

(f) A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report pursuant to subsection (d) of this section shall comply with the request no later than three business days after receiving the request.

(g) A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer's credit report only in the following cases:

(1) Upon the consumer's request, pursuant to subsections (d) or (j) of this section.

(2) If the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer. If a consumer reporting agency intends to remove a freeze upon a consumer's credit report pursuant to this subdivision, the consumer reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer's credit report.

(h) If a third party requests access to a consumer credit report on which a security freeze is in effect and this request is in connection with an application for credit or any other use and the consumer does not allow the consumer's credit report to be accessed for that specific period of time, the third party may treat the application as incomplete.

(i) If a consumer requests a security freeze pursuant to this section, the consumer reporting agency shall disclose to the consumer the process of placing and temporarily

lifting a security freeze and the process for allowing access to information from the consumer's credit report for a specific period of time while the security freeze is in place.

(j) A security freeze shall remain in place until the consumer requests that the security freeze be removed. A consumer reporting agency shall remove a security freeze within three business days of receiving a request for removal from the consumer, who provides all of the following:

(1) Proper identification.

(2) The unique personal identification number or password provided by the consumer reporting agency pursuant to subsection (c) of this section.

(k) A consumer reporting agency shall require proper identification of the person making a request to place or remove a security freeze.

(l) The provisions of this section do not apply to the use of a consumer credit report by any of the following:

(1) A person, or the person's subsidiary, affiliate, agent, subcontractor, or assignee with whom the consumer has, or prior to assignment had, an account, contract, or debtor-creditor relationship for the purposes of reviewing the active account or collecting the financial obligation owing for the account, contract, or debt.

(2) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subsection (d) of this section for purposes of facilitating the extension of credit or other permissible use.

(3) Any person acting pursuant to a court order, warrant, or subpoena.

(4) A state or local agency, or its agents or assigns, which administers a program for establishing and enforcing child support obligations.

(5) A state or local agency, or its agents or assigns, acting to investigate fraud, including Medicaid fraud, or acting to investigate or collect delinquent taxes or assessments, including interest and penalties, unpaid court orders, or to fulfill any of its other statutory responsibilities.

(6) A federal, state, or local governmental entity, including law enforcement agency, court, or their agent or assigns.

(7) A person for the purposes of prescreening as defined by the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq.

(8) Any person for the sole purpose of providing for a credit file monitoring subscription service to which the consumer has subscribed.

(9) A consumer reporting agency for the purpose of providing a consumer with a copy of the consumer's credit report upon the consumer's request.

(10) Any depository financial institution for checking, savings, and investment accounts.

(11) Any property and casualty insurance company for use in setting or adjusting a rate, adjusting a claim, or underwriting for property and casualty insurance purposes.

(m) If a security freeze is in place, a consumer reporting agency shall not change any of the following official information in a credit report without sending a written confirmation of the change to the consumer within 30 days of the change being posted to the consumer's file: name, date of birth, social security number, and address. Written confirmation is not required for technical modifications of a consumer's official information, including name and street abbreviations, complete spellings, or transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address and the former address.

(n) The following persons are not required to place in a credit report a security freeze pursuant to this section provided, however, that any person that is not required to place a security freeze on a credit report under the provisions of subdivision (3) of this subsection shall be subject to any security freeze placed on a credit report by another consumer reporting agency from which it obtains information:

(1) A check services or fraud prevention services company, which reports on incidents of fraud or issues authorizations for the purpose of approving or processing negotiable instruments, electronic fund transfers, or similar methods of payment.

(2) A deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or other similar negative information regarding a consumer to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution.

(3) A consumer reporting agency that does all of the following:

a. Acts only to resell credit information by assembling and merging information contained in a database of one or more credit reporting agencies.

b. Does not maintain a permanent database of credit information from which new credit reports are produced.

(o) This section does not prevent a consumer reporting agency from charging a fee of no more than ten dollars ($10.00) to a consumer for each freeze, removal of the freeze, or temporary lifting of the freeze for a period of time, regarding access to a consumer credit report, except that a consumer reporting agency may not charge any fee to a victim of identity theft who has submitted a copy of a valid investigative or incident report or complaint with a law enforcement agency about the unlawful use of the victim's identifying information by another person.

(p) At any time that a consumer is required to receive a summary of rights required under section 609 of the federal Fair Credit Reporting Act, the following notice shall be included:

"**North Carolina Consumers Have the Right to Obtain a Security Freeze.**

You have a right to place a "security freeze" on your credit report pursuant to North Carolina law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gains access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, rental housing, employment, investment, license, cellular phone, utilities, digital signature, Internet credit card transactions, or other services, including an extension of credit at point of sale.

The freeze will be placed within five business days. When you place a security freeze on your credit report, within 10 business days, you will be provided a personal identification number or a password to use when you want to remove or lift temporarily the security freeze.

A freeze does not apply when you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control, or similar activities.

You should plan ahead and lift a freeze if you are actively seeking credit or services as a security freeze may slow your applications, as mentioned above.

You can remove a freeze or authorize temporary access for a specific period of time by contacting the consumer reporting agency and providing all of the following:

(1) Your personal identification number or password,

(2) Proper identification to verify your identity, and

(3) Proper information regarding the period of time you want your report available to users of the credit report.

A consumer reporting agency that receives a request from you to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request. A consumer reporting agency may charge you up to ten dollars ($10.00) for each time you freeze, remove the freeze, or temporarily lift the freeze for a period of time, except a consumer reporting agency may not charge any amount to a victim of identify theft who has submitted a copy of a valid investigative or incident report or complaint with a law enforcement agency about the unlawful use of the victim's identifying information by another person.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report."

(q) A violation of this section is a violation of G.S. 75-1.1.

"**§ 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."

SECTION 2. G.S. 14-113.21 reads as rewritten:

"**§ 14-113.21. Venue of offenses.**

In any criminal proceeding brought under G.S. 14-113.20, the crime is considered to be committed in ~~any county in which~~ the county where the victim resides, where the perpetrator resides, where any part of the financial identity fraud took place, or in any other county instrumental to the completion of the offense, regardless of whether the defendant was ever actually present in that county."

SECTION 3. Article 19C of Chapter 14 of the General Statutes is amended by adding a new section to read:

"**§ 14-113.21A. Investigation of offenses.**

(a) A person who has learned or reasonably suspects that the person has been the victim of identity theft may contact the local law enforcement agency that has jurisdiction over the person's actual residence. Notwithstanding the fact that jurisdiction may lie elsewhere for investigation and prosecution of a crime of identity theft, the local law enforcement agency may take the complaint, issue an incident report, and provide the complainant with a copy of the report and may refer the report to a law enforcement agency in that different jurisdiction.

(b) Nothing in this section interferes with the discretion of a local law enforcement agency to allocate resources for investigations of crimes. A complaint filed or report issued under this section is not required to be counted as an open case for purposes of compiling open case statistics."

SECTION 4. Chapter 132 of the General Statutes is amended by adding a new section to read:

"**§ 132-1.8. Social security numbers and other personal identifying information.**

(a) The General Assembly finds the following:

(1) The social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes and other legitimate consensual purposes.

(2) Although there are legitimate reasons for State and local government agencies to collect social security numbers and other personal identifying information from individuals, government should collect the information only for legitimate purposes or when required by law.

(3) When State and local government agencies possess social security numbers or other personal identifying information, the governments

should minimize the instances this information is disseminated either internally within government or externally with the general public.

(b) Except as provided in subsections (c) and (d) of this section, no agency of the State or its political subdivisions, or any agent or employee of a government agency, shall do any of the following:

(1) Collect a social security number from an individual unless authorized by law to do so or unless the collection of the social security number is otherwise imperative for the performance of that agency's duties and responsibilities as prescribed by law. Social security numbers collected by an agency must be relevant to the purpose for which collected and shall not be collected until and unless the need for social security numbers has been clearly documented.

(2) Fail, when collecting a social security number from an individual, to segregate that number on a separate page from the rest of the record, or as otherwise appropriate, in order that the social security number can be more easily redacted pursuant to a valid public records request.

(3) Fail, when collecting a social security number from an individual, to provide, at the time of or prior to the actual collection of the social security number by that agency, that individual, upon request, with a statement of the purpose or purposes for which the social security number is being collected and used.

(4) Use the social security number for any purpose other than the purpose stated.

(5) Intentionally communicate or otherwise make available to the general public a person's social security number or other identifying information. "Identifying information", as used in this subdivision, shall have the same meaning as in G.S. 14-113.20(b), except it 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 drivers license numbers appearing on law enforcement records.

(6) Intentionally print or imbed an individual's social security number on any card required for the individual to access government services.

(7) Require an individual to transmit the individual's social security number over the Internet, unless the connection is secure or the social security number is encrypted.

(8) Require an individual to use the individual's social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.

(9) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law required that the social security number be on the document to be mailed. A social security number that is permitted to be mailed under this subdivision

may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

(c) Subsection (b) of this section does not apply in the following circumstances:

(1) To social security numbers or other identifying information disclosed to another governmental entity or its agents, employees, or contractors if disclosure is necessary for the receiving entity to perform its duties and responsibilities. The receiving governmental entity and its agents, employees, and contractors shall maintain the confidential and exempt status of such numbers.

(2) To social security numbers or other identifying information disclosed pursuant to a court order, warrant, or subpoena.

(3) To social security numbers or other identifying information disclosed for public health purposes pursuant to and in compliance with Chapter 130A of the General Statutes.

(4) To social security numbers or other identifying information that have been redacted.

(5) To certified copies of vital records issued by the State Registrar and other authorized officials pursuant to G.S. 130A-93(c). The State Registrar may disclose any identifying information other than social security numbers on any uncertified vital record.

(6) To any recorded document in the official records of the register of deeds of the county.

(7) To any document filed in the official records of the courts.

(d) No person preparing or filing a document to be recorded or filed in the official records by the register of deeds or of the courts may include any person's social security, employer taxpayer identification, drivers license, state identification, passport, checking account, savings account, credit card, or debit card number, or personal identification (PIN) code or passwords in that document, unless otherwise expressly required by law or court order, adopted by the State Registrar on records of vital events, or redacted. Any loan closing instruction that requires the inclusion of a person's social security number on a document to be recorded shall be void. Any person who violates this subsection shall be guilty of an infraction, punishable by a fine not to exceed five hundred dollars ($500.00) for each violation.

(e) The validity of an instrument as between the parties to the instrument is not affected by the inclusion of personal information on a document recorded or filed with the official records of the register of deeds. The register of deeds may not reject an instrument presented for recording because the instrument contains an individual's personal information.

(f) Any person has the right to request that a register of deeds or clerk of court remove, from an image or copy of an official record placed on a register of deeds' or court's Internet Web site available to the general public or an Internet Web site available to the general public used by a register of deeds or court to display public records by the register of deeds or clerk of court, the person's social security, employer taxpayer

identification, drivers license, state identification, passport, checking account, savings account, credit card, or debit card number, or personal identification (PIN) code or passwords contained in that official record. The request must be made in writing, legibly signed by the requester, and delivered by mail, facsimile, or electronic transmission, or delivered in person to the register of deeds or clerk of court. The request must specify the personal information to be redacted, information that identifies the document that contains the personal information and unique information that identifies the location within the document that contains the social security, employer taxpayer identification, drivers license, state identification, passport, checking account, savings account, credit card, or debit card number, or personal identification (PIN) code or passwords to be redacted. The request for redaction shall be considered a public record with access restricted to the register of deeds, the clerk of court, their staff, or upon order of the court. The register of deeds or clerk of court shall have no duty to inquire beyond the written request to verify the identity of a person requesting redaction and shall have no duty to remove redaction for any reason upon subsequent request by an individual or by order of the court, if impossible to do so. No fee will be charged for the redaction pursuant to such request. Any person who requests a redaction without proper authority to do so shall be guilty of an infraction, punishable by a fine not to exceed five hundred dollars ($500.00) for each violation.

(g) A register of deeds or clerk of court shall immediately and conspicuously post signs throughout his or her offices for public viewing and shall immediately and conspicuously post a notice on any Internet Web site available to the general public used by a register of deeds or clerk of court a notice stating, in substantially similar form, the following:

(1) Any person preparing or filing a document for recordation or filing in the official records may not include a social security, employer taxpayer identification, drivers license, state identification, passport, checking account, savings account, credit card, or debit card number, or personal identification (PIN) code or passwords in the document, unless expressly required by law or court order, adopted by the State Registrar on records of vital events, or redacted so that no more than the last four digits of the identification number is included.

(2) Any person has a right to request a register of deeds or clerk of court to remove, from an image or copy of an official record placed on a register of deeds' or clerk of court's Internet Web site available to the general public or on an Internet Web site available to the general public used by a register of deeds or clerk of court to display public records, any social security, employer taxpayer identification, drivers license, state identification, passport, checking account, savings account, credit card, or debit card number, or personal identification (PIN) code or passwords contained in an official record. The request must be made in writing and delivered by mail, facsimile, or electronic transmission, or delivered in person, to the register of deeds or clerk of court. The request must specify the personal information to be

redacted, information that identifies the document that contains the personal information and unique information that identifies the location within the document that contains the social security, employer taxpayer identification, drivers license, state identification, passport, checking account, savings account, credit card, or debit card number, or personal identification (PIN) code or passwords to be redacted. No fee will be charged for the redaction pursuant to such a request. Any person who requests a redaction without proper authority to do so shall be guilty of an infraction, punishable by a fine not to exceed five hundred dollars ($500.00) for each violation.

(h) Any affected person may petition the court for an order directing compliance with this section. No liability shall accrue to a register of deeds or clerk of court or to his or her agent for any action related to provisions of this section or for any claims or damages that might result from a social security number or other identifying information on the public record or on a register of deeds' or clerk of court's Internet website available to the general public or an Internet Web site available to the general public used by a register of deeds or clerk of court."

SECTION 5. Chapter 120 of the General Statutes is amended by adding a new Article to read:

"Article 30.

"Miscellaneous.

"**§ 120-61. Report by State agencies to the General Assembly on ways to reduce incidence of identity theft.**

Agencies of the State shall evaluate and report annually by January 1 to the General Assembly about the agency's efforts to reduce the dissemination of personal identifying information, as defined in G.S. 14-113.20(b). The evaluation shall include the review of public forms, the use of random personal identification numbers, restriction of access to personal identifying information, and reduction of use of personal identifying information when it is not necessary. Special attention shall be given to the use, collection, and dissemination of social security numbers. If the collection of a social security number is found to be unwarranted, the State agency shall immediately discontinue the collection of social security numbers for that purpose."

SECTION 6. G.S. 14-113.20 reads as rewritten:

"**§ 14-113.20. ~~Financial identity fraud.~~Identity theft.**

(a) A person who knowingly obtains, possesses, or uses identifying information of another person, living or dead, with the intent to fraudulently represent that the person is the other person for the purposes of making financial or credit transactions in the other person's name, to obtain anything of value, benefit, or advantage, or for the purpose of avoiding legal consequences is guilty of a felony punishable as provided in G.S. 14-113.22(a).

(b) The term "identifying information" as used in this Article includes the following:

(1) Social security or employer taxpayer identification numbers.

(2) Drivers ~~license~~ license, State identification card, or passport numbers.

(3) Checking account numbers.
(4) Savings account numbers.
(5) Credit card numbers.
(6) Debit card numbers.
(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
(8) Electronic identification ~~numbers.~~numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
(9) Digital signatures.
(10) Any other numbers or information that can be used to access a person's financial resources.
(11) Biometric data.
(12) Fingerprints.
(13) Passwords.
(14) Parent's legal surname prior to marriage.

(c) It shall not be a violation under this Article for a person to do any of the following:

(1) Lawfully obtain credit information in the course of a bona fide consumer or commercial transaction.
(2) Lawfully exercise, in good faith, a security interest or a right of offset by a creditor or financial institution.
(3) Lawfully comply, in good faith, with any warrant, court order, levy, garnishment, attachment, or other judicial or administrative order, decree, or directive, when any party is required to do so."

SECTION 7. The Revisor of Statutes shall make the following technical and conforming corrections:

(1) Rename Article 19C of Chapter 14 of the General Statutes from "Financial Identity Fraud" to "Identity Theft".
(2) Replace the phrase "financial identity fraud" with the phrase "identity theft" wherever the terms appear throughout Article 19C of Chapter 14 of the General Statutes.

SECTION 8. G.S. 15A-147(a) reads as rewritten:

"**§ 15A-147. Expunction of records when charges are dismissed or there are findings of not guilty as a result of identity ~~fraud.~~theft.**

(a) If any person is named in a charge for an infraction or a crime, either a misdemeanor or a felony, as a result of another person using the identifying information of the named person ~~to commit an infraction or crime~~ and the charge against the named person is dismissed, a finding of not guilty is entered, or the conviction is set aside, the named person may apply by petition or written motion to the court where the charge was last pending on a form approved by the Administrative Office of the Courts supplied by the clerk of court for an order to expunge from all official records any entries relating to the person's apprehension, charge, or trial. The court, after notice to the district attorney, shall hold a hearing on the motion or petition and, upon finding that the person's identity was used without permission and the charges were dismissed or the person was found not guilty, the court shall order the expunction."

SECTION 9. G.S. 1-539.2C reads as rewritten:

"**§ 1-539.2C. Damages for identity ~~fraud.~~theft.**

(a) Any person whose property or person is injured by reason of an act made unlawful by Article 19C of Chapter 14 of the General Statutes may sue for civil damages. Damages may be in an amount of up to five thousand dollars ($5,000) but no less than five hundred dollars ($500.00) for each incident, or three times the amount of actual damages, whichever amount is greater. A person seeking damages as set forth in this section may also institute a civil action to enjoin and restrain future acts that would constitute a violation of this section. The court, in an action brought under this section, may award reasonable attorneys' fees to the prevailing party."

SECTION 10. The provisions of this act are severable. If any phrase, clause, sentence, provision, or section is declared to be invalid or preempted by federal law or regulation, the validity of the remainder of this act shall not be affected thereby.

SECTION 11. G.S. 75-62(a)(2), (3), (4), and (5), as enacted in Section 1 of this act, become effective October 1, 2006. G.S. 132-1.8(b)(6), (7), (8), and (9), as enacted in Section 4 of this act, become effective July 1, 2007. Section 6 of this act becomes effective December 1, 2005, and applies to offenses committed, and to causes of action arising, on or after that date. The remainder of this act becomes effective December 1, 2005.