

**SECTION 1.** This act may be cited as the "Financial Identity Fraud and Identity Theft Protection Act".

**SECTION 2.** Title 37 of the 1976 Code is amended by adding:

"CHAPTER 20

Consumer Identity Theft Protection

**Section 37-20-110.** For purposes of this chapter:

(1) 'Consumer' means an individual residing in the State of South Carolina who undertakes a transaction for personal, family, or household purposes.

(2) 'Consumer credit-reporting agency' or 'consumer reporting agency' means a person that, for monetary fees or 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 about consumers for the purpose of furnishing consumer reports to third parties.

(3) 'Consumer report' or 'credit report' means any written, oral, electronic, or other communication of information by a consumer credit-reporting agency regarding a consumer's creditworthiness, credit standing, credit capacity, character, debts, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected in whole or in part for the purpose of establishing a consumer's eligibility for any of the following:

(a) credit or insurance to be used primarily for personal, family, or household purposes;

(b) employment purposes, meaning the use of a consumer report for the purpose of evaluating a consumer for employment, promotion, reassignment, or retention as an employee; or

(c) any other purpose authorized pursuant to 15 USC Section 1681b.

'Consumer report' or 'credit report' does not include a report containing information as to a transaction between the consumer and the person making the report; an authorization or approval by the issuer of a credit card or similar device, directly or indirectly, of a specific extension of credit; a communication of information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among those persons and the consumer has the opportunity, to direct that the information not be communicated among them, or a report in which a person conveys an adverse decision in response to a request from a third party to make a specific extension of credit, directly or indirectly, to the consumer, if the third party advises the consumer of the name and address of the person to whom the request was made and the person makes the required disclosures to the consumer pursuant to the provisions of the federal 'Fair Credit Reporting Act'.

(4) 'Credit card' has the same meaning as in Section 103 of the Truth in Lending Act, 15 USC Section 160 and includes a lender credit card, as defined in Section 37-1-301(16) and a seller credit card, as defined in Section 37-1-301(26).

(5) 'Creditworthiness' means an entry in a consumer's credit file that affects the ability of a consumer to obtain and retain credit, employment, business or professional licenses, investment opportunities, or insurance. Entries affecting creditworthiness include, but are not limited to, payment information, defaults, judgments, liens, bankruptcies, collections, records of arrest and indictments, and multiple credit inquiries.

(6) 'Debit card' means a 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 that financial institution, for the purpose of transferring money between accounts or obtaining money, property, labor, or services.

(7) 'Disposal' means the:

(a) discarding or abandonment of records containing personal identifying information; or

(b) sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of personal identifying information, other nonpaper media upon which records of personal identifying information are stored, or other equipment for nonpaper storage of information.

(8) 'File' means all information on a consumer that is recorded and retained by a consumer credit-reporting agency,

regardless of how the information is stored.

(9) 'Financial identity fraud' and 'identity fraud' are as defined in Section 16-13-510 and include the term 'identity theft'.

(10) 'Person' means a natural person, an individual, or an organization as defined in Section 37-1-301(20).

(11)(a) For purposes of this chapter, 'personal identifying information' means personal identifying information as defined in Section 16-13-510(D).

(b) 'Personal identifying information' does not mean information about vehicular accidents, driving violations, and driver's status.

(12) 'Proper identification' means information generally considered sufficient to identify a person. If a person is reasonably unable to identify himself or herself with the information described in item (11), 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.

(13) 'Publicly post' or 'publicly display' means to exhibit in a place of public view.

(14) 'Records' means material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics.

(15) 'Security breach' means an incident of unauthorized access to and acquisition of records or data that was not rendered unusable through encryption, redaction, or other methods containing personal identifying information that compromises the security, confidentiality, or integrity of personal identifying information maintained by a person when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the consumer. Good faith acquisition of personal identifying information by an employee or agent of the person for a legitimate purpose is not a security breach, if the personal identifying information is not used for a purpose other than a lawful purpose of the person and is not subject to further unauthorized disclosure.

(16) 'Security freeze' means a notice placed in a consumer credit report, at the request of the consumer and subject to certain exceptions, that prohibits the consumer credit-reporting agency from releasing a credit report containing all or any part of the consumer's credit report or any information derived from it without the express authorization of the consumer.

**Section 37-20-120.** (A) A consumer credit-reporting agency must give notice to each creditor who uses a consumer report if the agency becomes aware that an application to a card issuer to open a new seller or lender credit card account bears an address for the consumer that is different from the address in its file of the consumer.

(B) A seller or lender credit card issuer that mails an offer or solicitation to receive a credit card and, in response, receives a completed application for a seller or lender credit card listing an address that is substantially different from the address on the offer or solicitation shall verify the change of address by contacting the person to whom the solicitation or offer was mailed, or by using other reasonable means of verifying the account holder's identity.

(C) When a seller or lender credit card issuer receives a written or oral request for a change of the cardholder's billing address and within a period not to exceed thirty days after the requested address change receives a written or oral request for an additional credit card, the credit card issuer may not mail the requested additional credit card to the new address or activate the requested additional credit card unless the issuer has verified the change of address.

(D) This section does not apply to a person that sends or receives address discrepancy notices in compliance with 15 USC 1681c(h) or regulations promulgated pursuant to it.

**Section 37-20-130.** A person who learns or reasonably suspects that he is the victim of identity theft may initiate a law enforcement investigation by reporting to a local law enforcement agency that has jurisdiction over his actual legal residence. The law enforcement agency shall take the report, provide the complainant with a copy of the report, and begin an investigation or refer the matter to the law enforcement agency where the crime was committed for an investigation.

**Section 37-20-140.** (A) If a person is convicted of unlawfully obtaining the personal identifying information of another person without the other person's authorization and using that information to commit a crime, the court records must reflect that the person whose identity was falsely used to commit the crime did not commit the crime. (B) A person who reasonably believes that he is the victim of identity theft may petition the circuit court or have the County Office of Victims' Assistance petition the circuit court on his behalf, for an expedited judicial determination of his factual innocence, if the identity thief was arrested for and convicted of a crime under the victim's identity, or if the victim's identity has been mistakenly associated with a record of criminal conviction. A judicial determination of factual innocence made pursuant to this section may be heard and determined upon declarations, affidavits, police reports, or other material, relevant, and reliable information submitted by the parties. If the court determines that the petition is meritorious and that there is no reasonable cause to believe that the petitioner committed the offense for which the identity thief was arrested and convicted, the court shall find the petitioner factually innocent of that offense and issue an order certifying the determination and ordering the expunction of the erroneous conviction. (C) A court may at any time vacate the determination of factual innocence if information submitted in support of the petition is found to contain material misrepresentation or fraud.

**Section 37-20-150.** (A) The State Law Enforcement Division shall establish and maintain appropriate records of individuals who have been the victims of identity theft. The records will be maintained in a computerized database at such time that funds are appropriated to the State Law Enforcement Division. Access to the records is limited to criminal justice agencies, except that a victim of identity theft, or his authorized representative, shall have access to the records in order to establish that he is a victim of identity theft. (B) A victim of identity theft must submit to the State Law Enforcement Division a copy of the police report, a full set of fingerprints, or other relevant information required by the State Law Enforcement Division for the inclusion in the records of identity theft victims. The State Law Enforcement Division shall verify the identity of the victim against a driver's license or other identification records maintained by the Department of Motor Vehicles or by other agencies.

**Section 37-20-160.** (A) On written request sent by certified mail or electronic mail that includes proper identification provided by a consumer, the consumer's attorney-in-fact, or the consumer's legal guardian, if the consumer has not been a victim of identity theft or if the consumer has reason to believe that he is the victim of financial identity fraud, as evidenced by a copy of a valid police report, investigative report, or complaint made pursuant to Section 16-13-510, a consumer reporting agency shall place a security freeze on the consumer's consumer file not later than the fifth business day after the date the agency receives the request. (B) On written request for a security freeze from a consumer pursuant to subsection (A), a consumer reporting agency shall disclose to the consumer the process of placing, removing, and temporarily lifting a security freeze and the process for allowing access to information from the consumer's consumer file for a specific requester or period while the security freeze is in effect. (C) A consumer reporting agency, not later than the tenth business day after the date the agency receives the request for a security freeze shall:  
(1) send a written confirmation of the security freeze to the consumer; and  
(2) provide the consumer with a unique personal identification number or password to be used by the consumer to authorize a removal or temporary lifting of the security freeze. (D) A consumer may request in writing a replacement personal identification number or password. The request must comply with the requirements for requesting a security freeze pursuant to subsection (A). The consumer reporting agency, not later than the third business day after the date the agency receives the request for a replacement personal identification number or password, shall provide the consumer with a new unique personal identification number or password to be used by the consumer instead of the number or password that was provided earlier. (E) If a security freeze is in place, a consumer reporting agency shall notify the consumer in writing of a change

in the consumer file to the consumer's name, date of birth, social security number, or address not later than thirty calendar days after the date the change is made. The agency shall send notification of a change of address to the new address and former address. This section does not require notice of an immaterial change, including a street abbreviation change or correction of a transposition of letters or misspelling of a word.

(F) A consumer reporting agency shall notify a person who requests a consumer report if a security freeze is in effect for the consumer file involved in that report and the consumer report may not be released without express authorization by the consumer.

(G)(1) On a request by a consumer electronically, in writing, or by telephone and with proper identification provided by a consumer, including the consumer's personal identification number or password provided pursuant to subsection (C)(2), a consumer reporting agency shall remove a security freeze not later than the third business day after the date the agency receives the request at a point designated by the agency to receive the request.

(2)(a) On a request by a consumer electronically or by telephone and with proper identification provided by a consumer, including the consumer's personal identification number or password provided pursuant to subsection (C)(2), a consumer reporting agency, within fifteen minutes of receiving the request, shall lift the security freeze temporarily for a:

(i) certain properly designated period; or

(ii) certain properly identified requester.

(b) It is not a violation of this item if the consumer reporting agency is prevented from timely lifting the freeze by an act of God, a fire, a storm, an earthquake, an accident, or other event beyond the agency's control.

(H) A consumer reporting agency may develop procedures involving the use of a telephone, a facsimile machine, the Internet, or another electronic medium to receive and process a request from a consumer pursuant to this section.

(I) A consumer reporting agency shall remove a security freeze placed on a consumer file if the security freeze was placed due to a material misrepresentation of fact by the consumer. The consumer reporting agency shall notify the consumer in writing before removing the security freeze pursuant to this subsection.

(J) A consumer reporting agency may not charge a fee for a freeze, removal of a freeze, temporary lifting of a freeze, or reinstatement of a freeze.

(K) A security freeze does not apply to the use of a consumer report provided to:

(1) a state or local governmental entity, including a law enforcement agency or court or private collection agency, if the entity, agency, or court is acting pursuant to a court order, warrant, subpoena, or administrative subpoena;

(2) a child support agency acting to investigate or collect child support payments or acting pursuant to Title IV-D of the Social Security Act (42 USC Section 651 et seq.);

(3) the Department of Social Services acting to investigate fraud;

(4) the Department of Revenue acting to administer state tax laws;

(5) a local official authorized to investigate or collect delinquent amounts owed to a public entity;

(6) a person for the purposes of prescreening as provided by the Fair Credit Reporting Act (15 USC Section 1681 et seq.), as amended;

(7) a person with whom the consumer has an account or contract or to whom the consumer has issued a negotiable instrument, or the person's subsidiary, affiliate, agent, assignee, prospective assignee, subcontractor, or private collection agency, for purposes related to that account, contract, or instrument;

(8) a subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted pursuant to subsection (G)(2);

(9) a person who administers a credit file monitoring subscription service to which the consumer has subscribed;

(10) a person for the purpose of providing a consumer with a copy of the consumer's report on the consumer's request;

(11) a depository financial institution for checking, savings, and investment accounts;

(12) an insurance company for the purpose of conducting its ordinary business; or

(13) a consumer reporting agency that:

(a) acts only to resell credit information by assembling and merging information contained in a database of another

consumer reporting agency or multiple consumer reporting agencies; and

(b) does not maintain a permanent database of credit information from which new consumer reports are produced.

(L) The requirement of this section to place a security freeze on a consumer file does not apply to:

(1) a check service or fraud prevention service company that issues consumer reports:

(a) to prevent or investigate fraud; or

(b) for purposes of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payment;

(2) a deposit account information service company that issues consumer reports related to account closures caused by fraud, substantial overdrafts, automated teller machine abuses, or similar negative information regarding a consumer to an inquiring financial institution for use by the financial institution only in reviewing a consumer request for a deposit account with that institution; or

(3) a consumer reporting agency's database or file that consists of information concerning, and used for, one or more of the following, but not for credit granting purposes:

(a) criminal record information;

(b) fraud prevention or detection;

(c) personal loss history information; and

(d) employment, tenant, or individual background screening.

(M) A consumer reporting agency shall honor a security freeze placed on a consumer file by another consumer reporting agency.

(N) If a third party requests access to a consumer report on which a security freeze is in effect, this request is in connection with an application for credit or another use, and the consumer does not allow his credit report to be accessed, the third party may treat the application as incomplete. The presence of a security freeze on the file of a consumer must not be considered an adverse factor in the consumer's creditworthiness, credit standing, or credit capacity.

(O) The provisions of this section are cumulative, and an action taken pursuant to this section is not an election to take that action to the exclusion of other action authorized by law.

**Section 37-20-170.** (A) If a consumer disputes the accuracy of an item in the consumer's records with a consumer reporting agency, the consumer may give notice in writing to the consumer reporting agency specifying in what manner the report is inaccurate and the consumer reporting agency shall reinvestigate the inaccuracy at no charge to the consumer, provide the consumer with sufficient evidence that the information is true and accurate information as it relates to that consumer, and record the current status of the disputed information. The consumer reporting agency shall provide forms for that notice and shall assist a consumer in preparing the notice when requested.

(B) Within thirty days after receiving a notice of inaccuracy, a consumer reporting agency shall deny or admit the inaccuracy to the consumer in writing. If the consumer reporting agency denies the inaccuracy, the consumer reporting agency shall include the following information with the written results of the reinvestigation:

(1) the basis for the denial;

(2) a copy of the consumer's file that is based on the consumer's file as revised as a result of the reinvestigation, including the business name and address of any furnisher of information who was contacted in connection with that information and, if reasonably available, the telephone number of the furnisher;

(3) a notice that, if requested by the consumer, the consumer reporting agency shall provide the consumer with a description of the procedure used by the consumer reporting agency to determine the accuracy and completeness of the information; and

(4) sufficient evidence that the information is true and accurate information as it relates to that consumer.

(C) If the consumer reporting agency admits that the item is inaccurate, it shall correct the item in its records and, on request by the consumer, it shall inform any person who within the last six months has previously received a report containing that inaccurate information.

(D) In addition to all other penalties that may be imposed, a consumer credit-reporting agency or other person that

knowingly and wilfully violates a provision of this chapter is liable for three times the amount of actual damages or three thousand dollars for each incident, whichever is greater, as well as reasonable attorney's fees and costs.

(E) In addition to all other penalties that may be imposed, a consumer credit-reporting agency or other person that negligently violates this chapter is liable for the greater of actual damages or one thousand dollars for each incident, as well as reasonable attorney's fees and costs.

(F) In addition to the damages assessed pursuant to subsections (D) and (E), if the injury is to the consumer's creditworthiness, credit standing, credit capacity, character, general reputation, employment options, or eligibility for insurance, and results from the failure to take inaccurate information off of a credit report and the failure is not corrected by the consumer credit-reporting agency within ten days after the entry of a judgment for damages, the assessed damages must be increased to one thousand dollars each day until the inaccurate information is removed from the consumer's record.

(G) A consumer seeking damages pursuant to this section also may institute a civil action to enjoin and restrain future acts constituting a violation of this chapter.

(H) The remedial provisions of this chapter are cumulative of and in addition to any other action at law and any action taken by the Department of Consumer Affairs pursuant to Chapter 6 of this title.

(I) This section is not intended, and must not be construed, to confer liability on a person who acts reasonably and who does not act wilfully or negligently.

**Section 37-20-180.** (A) Except as provided in subsection (B) of this section, a person may not:

(1) publicly post or publicly display or otherwise intentionally communicate or make available to the general public a consumer's social security number or a portion of it containing six digits or more;

(2) intentionally print or imbed a consumer's social security number or any portion of it containing six digits or more on any card required for the consumer to access products or services provided by the person;

(3) require a consumer to transmit his social security number or a portion of it containing six digits or more over the Internet, unless the connection is secure or the social security number is encrypted;

(4) require a consumer to use his social security number or a portion of it containing six digits or more 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 a consumer's social security number or a portion of it containing six digits or more on 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 a consumer's social security number or a portion of it containing six digits or more to a third party without written consent to the disclosure from the consumer, unless the third party seeking disclosure of the social security number does so for a legitimate business or government purpose or unless authorized or specifically permitted by law to do so or unless the disclosure is otherwise imperative for the performance of the person's duties and responsibilities as prescribed by law. A legitimate business purpose of the third party includes, but is not limited to, locating an individual to provide a benefit to that individual, such as a pension, insurance, or unclaimed property benefit, or to find an individual who is missing or a lost relative, or to serve civil process. A legitimate purpose of the third party does not include the bulk purchase or rental of social security numbers or use in marketing.

(B) This section does not apply:

(1) if 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 the federal Fair Credit Reporting Act. A social security number that is permitted to be mailed pursuant to this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope or may not be visible on or through the envelope;

(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 a consumer;

(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, including a debt collected pursuant to the Setoff Debt Collection Act, Section 12-56-10, and the Governmental Enterprise Accounts Receivable Collections program, Section 12-4-580, or obtain a credit report from or furnish data to a consumer reporting agency, pursuant to the federal Fair Credit Reporting Act or to undertake a purpose permissible pursuant to the Gramm-Leach-Bliley Act or Driver's Privacy Protection Act;

(5) to a person acting pursuant to a court order, warrant, subpoena, or other legal process;

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

(7) to a financial institution as defined in the Gramm-Leach-Bliley Act;

(8) to the submission and use of a social security number or other personal identifying information as part of the maintenance and reporting of employment records, employment verification, or in the course of the administration or provision of employee benefits programs, claims, and procedures related to employment including, but not limited to, termination from employment, retirement from employment, injuries suffered during the course of employment, and other such claims, benefits, and procedures;

(9) to a recorded document in the official records of a county; or

(10) to a document filed in the official records of the court.

**Section 37-20-190.** (A) When a business disposes of a business record that contains personal identifying information of a customer of a business, the business shall modify, by shredding, erasing, or other means, the personal identifying information to make it unreadable or undecipherable.

(B) A business is considered to comply with subsection (A) if it contracts with a person engaged in the business of disposing of records for the modification of personal identifying information on behalf of the business in accordance with subsection (A).

(C) This section does not apply to:

(1) a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act;

(2) a health insurer 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; or

(3) a consumer credit-reporting agency that is subject to and in compliance with the federal Fair Credit Reporting Act.

**Section 37-20-200.** (A) In addition to all other penalties that may be imposed, a consumer credit-reporting agency or other person that wilfully violates a provision of this chapter is liable for three times the amount of actual damages or not more than one thousand dollars for each incident, whichever is greater, as well as reasonable attorney's fees and costs.

(B) In addition to all other penalties that may be imposed, a consumer credit-reporting agency or other person that negligently violates this chapter is liable for actual damages and reasonable attorney's fees and costs.

(C) In addition to the damages assessed pursuant to subsections (A) and (B), if the injury is to the consumer's creditworthiness, credit standing, credit capacity, character, general reputation, employment options, or eligibility for insurance, and results from the failure to place and enforce the security freeze provided for in Section 37-20-160 and the failure is not corrected by the consumer credit-reporting agency within ten days after the entry of a judgment for damages, the assessed damages must be increased to not more than one thousand dollars each day until the security freeze is imposed.

(D) A consumer seeking damages pursuant to this section also may institute a civil action to enjoin and restrain future acts constituting a violation of this chapter.

(E) The remedial provisions of this chapter are cumulative of and in addition to any other action at law and any

action taken by the Department of Consumer Affairs pursuant to Chapter 6 of this title.

(F) This section is not intended, and must not be construed, to confer liability on a person who acts reasonably and who does not act wilfully or grossly negligent.

(G) Damages provided by this section do not apply to Section 37-20-170."

Redesignation as Article 1; Personal Identifying Information Privacy Protection

**SECTION 3.A.** The Family Privacy Protection Act, Sections 30-2-10 through 30-2-50, is redesignated as Article 1, Chapter 2, Title 30.

B. Chapter 2, Title 30 of the 1976 Code is amended by adding:

"Article 3

Personal Identifying Information Privacy Protection

**Section 30-2-300.** The General Assembly finds:

(1) The social security number can be used as a tool to perpetuate fraud against an individual and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to the 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 entities to collect social security numbers and other personal identifying information from individuals, government entities should collect the information only for legitimate purposes or when required by law. An entity that provides employee benefits has a legitimate need to collect and use social security numbers and personal identifying information as part of its administration and provision of employee benefits programs.

(3) When state and local government entities 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.

**Section 30-2-310.** (A)(1) Except as provided in Sections 30-2-320 and 30-2-330 of this article, a public body, as defined in Section 30-1-10(B), may not:

(a) collect a social security number or any portion of it containing six digits or more 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 body's duties and responsibilities as prescribed by law. Social security numbers collected by a public body must be relevant to the purpose for which collected and must not be collected until and unless the need for social security numbers has been clearly documented;

(b) fail, when collecting a social security number or portion of it containing six digits or more from an individual, to segregate that number on a separate page from the rest of the record, or as otherwise appropriate, so that the social security number may be easily redacted pursuant to a public records request;

(c) fail, when collecting a social security number or any portion of it containing six digits or more from an individual, to provide, at the time of or before the actual collection of the social security number by that public body, upon request of the individual, a statement of the purpose or purposes for which the social security number is being collected and used;

(d) use the social security number or a portion of it containing six digits or more for any purpose other than the purpose stated;

(e) intentionally communicate or otherwise make available to the general public an individual's social security number or a portion of it containing six digits or more or other personal identifying information. 'Personal identifying information', as used in this section, has the same meaning as 'personal identifying information' in Section 16-13-510, except that it does not include electronic identification names, including electronic mail

addresses, or parent's legal surname before marriage;

(f) intentionally print or imbed an individual's social security number or a portion of it containing six digits or more on any card required for the individual to access government services;

(g) require an individual to transmit the individual's social security number or a portion of it containing six digits or more over the Internet, unless the connection is secure or the social security number is encrypted;

(h) require an individual to use the individual's social security number or a portion of it containing six digits or more 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; or

(i) print an individual's social security number or a portion of it containing six digits or more on materials that are mailed to the individual, unless state or federal law requires the social security number be on the mailed document.

(2) An entity that collects and uses social security numbers or other personal identifying information as part of the maintenance and reporting of employment records or the administration or provision of employee benefits programs is exempt from the prohibitions in this subsection.

(B) Before a public body, as defined in Section 30-1-10(B), may transfer or dispose of information technology hardware or storage media owned or leased by it, all personal and confidential information must be removed and the hardware and storage media must be sanitized in accordance with standards and policies adopted by the State Budget and Control Board, Division of the State Chief Information Officer. The director or appropriate information technology manager of the public body owning or leasing the information technology hardware or storage media shall verify that all personal and confidential information is removed and the information technology hardware and storage media are sanitized in accordance with those standards and policies before the transfer or disposal occurs.

(C) When a public body disposes of a record that contains personal identifying information of an individual, the body shall modify, by shredding, erasing, or other means, the personal identifying information to make it unreadable or undecipherable.

(D) A public body is considered to comply with subsection (C) if it contracts with a person engaged in the business of disposing of records for the modification of personal identifying information on behalf of the body in accordance with subsection (C).

**Section 30-2-320.** Social security numbers and identifying information may be disclosed:

(1) to another governmental entity or its agents, employees, or contractors, if disclosure is necessary for the receiving entity to perform its duties and responsibilities, including a debt collected pursuant to the Setoff Debt Collection Act, Section 12-56-10, and the Governmental Enterprise Accounts Receivable Collections program, Section 12-4-580. The receiving governmental entity and its agents, employees, and contractors shall maintain the confidential and exempt status of those numbers;

(2) pursuant to a court order, warrant, or subpoena;

(3) for public health purposes;

(4) on certified copies of vital records issued by the director of the Department of Health and Environmental Control as the state registrar, pursuant to Section 44-63-30 and authorized officials pursuant to Section 44-63-40. The state registrar may disclose personal identifying information other than social security number on an uncertified vital record;

(5) on a recorded document in the official records of the county;

(6) on a document filed in the official records of the courts; and

(7) to an employer for employment verification or in the course of administration or provision of employee benefit programs, claims, and procedures related to employment including, but not limited to, termination from employment, retirement from employment, injuries suffered during the course of employment, and other such claims, benefits, and procedures.

**Section 30-2-330.** (A) A person preparing or filing a document to be recorded or filed in the official records by the register of deeds or the clerk of court of a county may not include an individual's social security, driver's 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 or rule adopted by the state registrar on records of vital events. A loan closing instruction that requires the inclusion of an individual's social security number on a document to be recorded is void. A person who violates this subsection is guilty of a misdemeanor, punishable by a fine not to exceed five hundred dollars for each violation. (B) Notwithstanding Section 30-1-30, or another provision of law, an individual or his attorney-in-fact or legal guardian may request that a register of deeds or clerk of court remove, from an image or copy of an official record placed on a publicly available Internet web site or a publicly available Internet web site used by a register of deeds or court to display public records by the register of deeds or clerk of court, the individual's social security, driver's 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 identification page number that contains the social security, driver's 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 register of deeds or clerk of court has no duty to inquire beyond the written request to verify the identity of an individual requesting redaction. A fee must not be charged for the redaction pursuant to the request.

(C) A register of deeds or clerk of court immediately and conspicuously shall post signs throughout his offices for public viewing and a notice on any Internet web site or remote electronic site made available by the register of deeds or clerk of court and used for the ordering or display of official records or images or copies of official records a notice, stating, in substantially similar form, the following:

'A person preparing or filing a document for recordation or filing in the official records may not include a social security, driver's 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. An individual 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 publicly available Internet web site or on a publicly available Internet web site used by a register of deeds or clerk of court to display public records, any social security, driver's 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 in person, to the register of deeds or clerk of court. The request must specify the identification page number that contains the social security, driver's license, state identification, passport, checking account, savings account, credit card, debit card number, or personal identification (PIN) code, or passwords to be redacted. There is no fee for the redaction pursuant to request.'

**Section 30-2-340.** Any affected individual may petition the court for an order directing compliance with this section. Liability may not accrue to a register of deeds or clerk of court or to his agents for claims or damages that arise from a social security number or other identifying information on the public record."

Breach of security of state agency data; time effective

**SECTION 4.A.** Article 1, Chapter 1, Title 11 of the 1976 Code is amended by adding:

"**Section 1-11-490.** (A) An agency of this State owning or licensing computerized data or other data that includes personal identifying information shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose unencrypted and unredacted personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(B) An agency maintaining computerized data or other data that includes personal identifying information that the agency does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

(C) The notification required by this section may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it no longer compromises the investigation.

(D) For purposes of this section:

(1) 'Agency' means any agency, department, board, commission, committee, or institution of higher learning of the State or a political subdivision of it.

(2) 'Breach of the security of the system' means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromise the security, confidentiality, or integrity of personal identifying information maintained by the agency, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the consumer. Good faith acquisition of personal identifying information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.

(3) 'Personal identifying information' has the same meaning as 'personal identifying information' in Section 16-13-510(D).

(E) The notice required by this section may be provided by:

(1) written notice;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 USC and Chapter 6, Title 26 of the 1976 Code;

(3) telephonic notice; or

(4) substitute notice, if the agency demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five hundred thousand or the agency has insufficient contact information. Substitute notice consists of:

(a) e-mail notice when the agency has an e-mail address for the subject persons;

(b) conspicuous posting of the notice on the agency's web site page, if the agency maintains one; or

(c) notification to major statewide media.

(F) Notwithstanding subsection (E), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(G) A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:

(1) institute a civil action to recover damages;

(2) seek an injunction to enforce compliance; and

(3) recover attorney's fees and court costs, if successful.

(H) An agency that knowingly and wilfully violates this section is subject to an administrative fine up to one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

(I) If the agency provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice."

B. This section is effective on July 1, 2009.

Household garbage private

**SECTION 5.** Article 7, Chapter 11, Title 16 of the 1976 Code is amended by adding:

"**Section 16-11-725.** (A) It is unlawful for a person to rummage through or steal another person's household garbage or litter, as defined in Section 44-67-30(4), for the purpose of committing financial identity fraud or identity fraud or identity theft as defined in Sections 16-13-510 and 37-20-110.

(B)(1) A person that violates the provisions of this section is guilty of a misdemeanor and, upon conviction, must be fined not more than two hundred fifty dollars for the first violation and one thousand dollars for each subsequent violation.

(2) A person who knowingly and wilfully violates the provisions of this section is guilty of a Class F felony and, upon conviction, must be imprisoned not more than five years and fined not more than one thousand dollars, or both.

(C) A conviction pursuant to the provisions of this section and the possession of identifying information as defined in Section 16-13-510 is prima facie evidence of financial identity fraud, identity fraud, or identity theft pursuant to Sections 37-20-110.

(D) This section does not prohibit a duly constituted officer of the law from performing his official duties in ferreting out offenders or suspected offenders against violating the laws of this State or a county or municipality for the purpose of apprehending the suspected violator. The provisions of this section must not be construed to give an officer any additional rights or powers upon private property but must be construed as preserving only his previous powers."

Credit and debit card receipts

**SECTION 6.** Article 2, Chapter 13, Title 16 of the 1976 Code is amended by adding:

"**Section 16-13-512.** (A) Except as provided in this section, a person, firm, partnership, association, corporation, limited liability company, or any other entity which accepts credit cards or debit cards for the transaction of business must not print on a receipt provided to the cardholder at the point of sale:

(1) more than five digits of the credit card or debit card account number; and

(2) the expiration date of the credit card or debit card.

(B) This section does not apply to transactions in which the sole means of recording the cardholder's credit card or debit card account number is by handwriting or by an imprint or copy of the credit card or debit card.

(C)(1) A person that violates the provisions of this section is guilty of a misdemeanor and, upon conviction, must be fined not more than two hundred fifty dollars for the first violation and one thousand dollars for each subsequent violation.

(2) A person that knowingly and wilfully violates the provisions of this section is guilty of a Class F felony and, upon conviction, must be imprisoned not more than five years and fined not more than one thousand dollars, or both.

(D) This section, in compliance with Public Law 108-159, Section 113 of Title 1, is effective:

(1) three years after its enactment as to a cash register or other machine or device that electronically prints receipts for credit card or debit card transactions and that is in use before January 1, 2005; or

(2) one year after its enactment for those machines and devices first put into use on or after January 1, 2005."

Breach of security of business data; time effective

**SECTION 7.A.** Chapter 1, Title 39 of the 1976 Code is amended by adding:

"**Section 39-1-90.** (A) A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is

reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(B) A person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

(C) The notification required by this section may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it no longer compromises the investigation.

(D) For purposes of this section:

(1) 'Breach of the security of the system' means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. Good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.

(2) 'Person' has the same meaning as in Section 37-20-110(10).

(3) 'Personal identifying information' has the same meaning as 'personal identifying information' in Section 16-13-510(D).

(E) The notice required by this section may be provided by:

(1) written notice;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures in Section 7001 of Title 15 USC and Chapter 6, Title 11 of the 1976 Code;

(3) telephonic notice; or

(4) substitute notice, if the person demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five hundred thousand or the person has insufficient contact information. Substitute notice consists of:

(a) e-mail notice when the person has an e-mail address for the subject persons;

(b) conspicuous posting of the notice on the web site page of the person, if the person maintains one; or

(c) notification to major statewide media.

(F) Notwithstanding subsection (E), a person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(G) A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:

(1) institute a civil action to recover damages in case of a wilful and knowing violation;

(2) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section;

(3) seek an injunction to enforce compliance; and

(4) recover attorney's fees and court costs, if successful.

(H) A person who knowingly and wilfully violates this section is subject to an administrative fine in the amount of one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to

be decided by the Department of Consumer Affairs.

(I) This section does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act.

(J) 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 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, as amended, is considered to be in compliance with this section.

(K) If a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice."

B. This section is effective on July 1, 2009.

#### Identity fraud

**SECTION 8.** Section 16-13-510 of the 1976 Code, as last amended by Act 350 of 2006, is further amended to read: "**Section 16-13-510.** (A) It is unlawful for a person to commit the offense of financial identity fraud or identity fraud.

(B) A person is guilty of financial identity fraud when he, without the authorization or permission of another person and with the intent of unlawfully appropriating the financial resources of that person to his own use or the use of a third party knowingly and wilfully:

(1) obtains or records identifying information which would assist in accessing the financial records of the other person; or

(2) accesses or attempts to access the financial resources of the other person through the use of identifying information as defined in subsection (D).

(C) A person is guilty of identity fraud when he uses identifying information, as defined in subsection (D), of another person for the purpose of obtaining employment or avoiding identification by a law enforcement officer, criminal justice agency, or another governmental agency including, but not limited to, law enforcement, detention, and correctional agencies or facilities.

(D) 'Personal identifying information' means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted:

(1) social security number;

(2) driver's license number or state identification card number issued instead of a driver's license;

(3) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or

(4) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

(E) A person who violates the provisions of this section is guilty of a felony and, upon conviction, must be fined in the discretion of the court or imprisoned not more than ten years, or both. The court may order restitution to the victim pursuant to the provisions of Section 17-25-322."

#### Repeal

**SECTION 9.** Section 16-13-515 of the 1976 Code, as added by Act 350 of 2006, is repealed.

#### Savings clause

**SECTION 10.** The repeal or amendment by this act of any law, whether temporary or permanent or civil or criminal, does not affect pending actions, rights, duties, or liabilities founded thereon, or alter, discharge, release or extinguish any penalty, forfeiture, or liability incurred under the repealed or amended law, unless the repealed or amended provision shall so expressly provide. After the effective date of this act, all laws repealed or amended by this act must be taken and treated as remaining in full force and effect for the purpose of sustaining any pending or vested right, civil action, special proceeding, criminal prosecution, or appeal existing as of the effective date of this act, and for the enforcement of rights, duties, penalties, forfeitures, and liabilities as they stood under the repealed or amended laws.

Severability clause

**SECTION 11.** If any section, subsection, paragraph, subparagraph, sentence, clause, phrase, or word of this act is for any reason held to be unconstitutional or invalid, such holding shall not affect the constitutionality or validity of the remaining portions of this act, the General Assembly hereby declaring that it would have passed this act and each and every section, subsection, paragraph, subparagraph, sentence, clause, phrase, and word thereof, irrespective of the fact that any one or more other sections, subsections, paragraphs, subparagraphs, sentences, clauses, phrases, or words hereof may be declared to be unconstitutional, invalid, or otherwise ineffective.

Time effective

**SECTION 12.** Except as otherwise provided herein, this act is effective December 31, 2008.