



South Carolina Association Of Counties

L. Gregory Pearce, Jr., President
Richland County

Michael B. Cone
Executive Director

TECHNICAL BULLETIN

July 18, 2008

To: County Council Chairmen
Chief Administrative Officers
County Attorneys
County Auditors
County Treasurers
Finance Directors
Personnel Directors
Clerks of Court
Register of Deeds

From: Kent Lesesne
SCAC Staff Attorney

Re: Identity Theft and Fraud Protection Act 2008- Act No. 190, (R. 202, S. 453)

This *Technical Bulletin* outlines changes adopted by the General Assembly in 2008 Act No. 190, relating to identity theft and fraud protection laws. A copy of the Act is enclosed for your convenience. Please consult your county attorney if you have specific questions about the interpretation or application of these changes. The SCAC staff is also available at 1-800-922-6081 to address general questions.

The South Carolina Legislature enacted Act 190 of 2008 (R. 202, S. 453), which provides a comprehensive change in the laws to address the growing problem of identity theft and identity fraud. It also provides some guidelines for counties on how to handle personal identifying information. The effective date of the Act is December 31, 2008.

Personal identifying information is defined pursuant to Section 16-13-510(C) and includes, but is not limited to: (1) social security numbers; (2) driver's license numbers; (3) checking account numbers; (4) savings account numbers; (5) credit card numbers; (6) debit card numbers; (7) personal identification numbers; (8) electronic identification numbers; (9) digital signatures; (10) other numbers or information which may be used to access a person's financial resources; or (11) identifying information that defines a person other than the person presenting the document. Documents described by item (11) include, but are not limited to, passports, driver's licenses, birth certificates, immigration documents, and state issued identification cards.

Under §37-20-160(A) of the Act, a person who is the victim of identity theft may, upon written request to a consumer reporting agency, place a security freeze on their consumer credit file. The security freeze can only be lifted at the request of the consumer. However, this security freeze does not apply to a local government entity, including a law enforcement agency or court, if acting pursuant to a court order, warrant, subpoena, or administrative subpoena. It also does not apply to a local official attempting to collect a debt owed by the consumer to a public entity.

While the law prohibits public posting or display of person's social security number and precludes the use of person's social security number in certain consumer transactions, under §37-20-180(B)(4) and (8), it does not preclude the use and release of a person's social security number to do a background check or collect a debt, including a debt collected pursuant to the Setoff Debt Collection Act, §12-56-10. It also does not preclude a person from providing their social security number to a local government entity, nor does it preclude the use of a social security number or other personal identifying information as part of the maintenance and reporting of employment records.

Although there are legitimate reasons for local government entities to collect social security numbers or other personal identifying information from individuals, government entities should collect the information only for legitimate purposes or when required by law. Local governments should also minimize the instances this information is disseminated either internally or externally with other governmental agencies or the general public. Public bodies that collect social security numbers must segregate that number on a separate page from the rest of the record, or as otherwise appropriate, so that the social security numbers may be easily redacted pursuant to a public records request in compliance with §30-2-310(A)(1)(b).

Pursuant to §30-2-310(B) and (C), public bodies disposing of technology hardware such as computer equipment must have all personal and confidential information removed and sanitized in accordance with standards and policies adopted by the State Budget and Control Board, Division of the State Chief Information Officer. When a public body disposes of a record that contains personal identifying information of an individual, it must modify the personal identifying information, by shredding, erasing, or other means, to make it unreadable or undecipherable. Section 30-2-310(D) allows a public body to contract with a third party in the business of shredding records.

Section 16-11-725 makes it a Class F felony crime to rummage through or steal another person's household garbage or litter for the purpose of obtaining information to commit financial identity fraud or identity theft. This provision does not prevent state or local law enforcement officers from apprehending suspected offenders who may be hiding in the cover of garbage or litter, but does not give law enforcement any additional rights or powers upon private property.

Under §30-2-330(A), a person preparing or filing a document to be recorded in the official records by the register of deeds or the clerk of court may not include an individual's social security number, driver's license, state identification, passport, checking or savings account, credit or debit card number, personal identification code, or passwords in the document, unless required by law or court order. Pursuant to §30-2-330(B), a consumer or their attorney may request, at no charge, that such personal identifying information be redacted from an image or copy of an official record of a public document, such as a mortgage, on the register of deeds or clerk of court's public website. The request must be in writing and must specify the identification page number of the documents that contains the personal identifying information. The register of deeds or the clerk of court has no duty to verify the identity of the person requesting the redaction, and they are immune from claims or damages that arise from personal identifying information on the public records. There is some question as to whether the information redaction process provided in §30-2-330(B) applies only to electronic copies or to physical copies in light of §30-1-30, which prohibits the alteration of public records.

Section 16-13-512(A)(1) and (3) states that any business or state or local government entity that accepts credit cards or debit cards must not print on a receipt more than five digits of the credit card or debit card number and the expiration date. This does not apply to credit card or debit card numbers taken solely by handwriting or by an imprint or copy of the credit or debit card. Machines in use before January 1, 2005 have to come into

compliance with this provision by December 31, 2011, while credit card machines put into use after January 1, 2005 have until December 31, 2009 to come into compliance with §16-13-512(D)(1) and (2).

Under the provisions of §1-11-490, beginning on July 1, 2009, all state agencies and political subdivisions must notify all affected individuals as soon as reasonably possible of a security breach in their database containing the individuals' personal identifying information. Section 37-20-110(15) defines a security breach as 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 reasonable likely to occur, or use of the information creates a material risk of harm to the consumer. Good faith acquisition and use of personal identifying information by an employee or agent of the person for a legitimate purpose is not considered a security breach.

Notice of a security breach may be given in writing, by facsimile, or by telephone. If the agency or political subdivision can demonstrate that the cost of providing notice would exceed two hundred fifty thousand dollars, the affected class of subject persons to be notified exceeds five hundred thousand, or there is insufficient contact information, the agency or political subdivision may provide notice by e-mail, post it conspicuously on their website, or by major statewide media. If notice is to be provided to more than one thousand persons at one time, the agency or political subdivision must also provide notification to Consumer Affairs and all national consumer reporting agencies. Failure to notify may result in an administrative fine up to one thousand dollars for each resident whose information was accessible by the breach, the amount of the fine to be determined by the Department of Consumer Affairs.

When dealing with 2008 Act No. 190, it would be prudent to also review the Federal Trade Commission "Red Flag Rule" identity theft prevention requirements, which is codified at 16 CFR 681. It requires all financial institutions and creditors to implement an identity theft program for customer accounts. The rule requires reasonable procedures to identify red flags such as an address discrepancy on a customer account or unusual or suspicious activity on an account such as a high number of credit inquiries. The procedures must be able to detect the red flags that have been established and respond to them appropriately. Finally, the red flag program must be updated periodically to reflect the risk of identity theft. All affected entities must comply with the red flag rule by November 8, 2008.