

SOUTH CAROLINA

IDENTITY THEFT RANKING BY STATE: Rank 30, 60.6 Complaints Per 100,000
Population, 2670 Complaints (2007)
Updated January 5, 2009

Current Laws: A person commits the crime 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 willfully:

- Obtains or records identifying information that would assist in accessing the financial records of the other person; or
- Accesses or attempts to access the financial resources of the other person through the use of identifying information.

A person commits the crime of identity fraud when he uses identifying information 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.

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:

- Social Security number;
- Driver's license number or state identification card number issued instead of a driver's license;
- 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
- 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.

Violations are a felony, punishable by up to ten years in prison and/or a fine. The court may order restitution to the victim.

Statute: §16-13-510: (must scroll down to appropriate section)

<http://www.scstatehouse.net/code/t16c013.htm>

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Jurisdiction: The crime is considered to have been committed in a county in which a part of the financial identity fraud took place, regardless of whether the defendant was ever actually in that county.

Statute: §16-13-520: (must scroll down to appropriate section)

<http://www.scstatehouse.net/code/t16c013.htm>

Payment Cards: A person is guilty of financial transaction card theft when he:

- Takes, obtains, or withholds a financial transaction card or number from the person, possession, custody, or control of another without the cardholder's consent and with the intent to use it; or who, with knowledge that it has been so taken, obtained, or withheld, receives the financial transaction card or number with intent to use it, sell it, or transfer it to a person other than the issuer or the cardholder;
- Receives a financial transaction card or number that he knows to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder, and who retains possession with intent to use it, sell it, or transfer it to a person other than the issuer or the cardholder;
- Is not the issuer, and sells a financial transaction card or number or buys a financial transaction card or number from a person other than the issuer;
- Is not the issuer, and during any twelve-month period, receives financial transaction cards or numbers issued in the names of two or more persons which he has reason to know were taken or retained under fraudulent circumstances.

Violations are a felony, punishable by up to five years in prison and/or a fine of \$3000 to \$5000.

Statute: §16-14-20: (must scroll down to appropriate section)

<http://www.scstatehouse.net/code/t16c014.htm>

When a person has in his possession or under his control financial transaction cards issued in the names of two or more other persons other than members of his immediate family, such possession is prima facie evidence that the cards have been obtained fraudulently.

Statute: §16-14-30: (must scroll down to appropriate section)

<http://www.scstatehouse.net/code/t16c014.htm>

A person is guilty of financial transaction card forgery when he:

- Falsely makes or embosses a purported financial transaction card, with intent to defraud a purported issuer, a person or organization providing money, goods, services or anything else of value, or any other person;
- Falsely encodes (records magnetically, electronically, or by other means information on a financial transaction card that will permit acceptance of that card by any automated banking device), duplicates or alters existing encoded information on a financial transaction card with intent to defraud a purported issuer, a person or organization providing money, goods, services or anything else of value, or any other person.
- Signs a financial transaction card, not being the cardholder or a person authorized by him with intent to defraud the issuer, or a person or organization providing money, goods, services or anything else of value.

Violations are a felony, punishable by up to five years in prison and/or a fine of \$3000 to \$5000.
Statute: §16-14-40: (must scroll down to appropriate section)
<http://www.scstatehouse.net/code/t16c014.htm>

Possession of two or more cards falsely made, embossed, or signed is prima facie evidence that the cards were obtained fraudulently.
Statute: §16-14-50: (must scroll down to appropriate section)
<http://www.scstatehouse.net/code/t16c014.htm>

A person is guilty of financial transaction card fraud when, with the intent to defraud the issuer, a person or organization providing money, goods, services, or anything else of value, or any other person, he:

- Uses a financial transaction card obtained or retained fraudulently;
- Uses a financial transaction card which he knows is forged, altered, expired, revoked, or obtained fraudulently;
- Presents the card without the authorization or permission of the cardholder;
- Represents that he is the holder of the card when it has in fact not been issued; or
- Upon application for a financial transaction card to an issuer, he knowingly makes or causes to be made a false statement or report relative to his name, occupation, financial condition, assets, or liabilities.

Violations are a misdemeanor, punishable by up to one year in jail and/or a fine of \$1000. If the value of the goods or services obtained exceeds \$500 in a six-month period, it is a felony, punishable by up to five years in prison and/or a fine of \$3000 to \$5000.
Statute: §16-14-60: (must scroll down to appropriate section)
<http://www.scstatehouse.net/code/t16c014.htm>

Dumpster Diving: It is unlawful for a person to rummage through or steal another person's household garbage or litter for the purpose of committing financial identity fraud or identity fraud or identity theft. Violators will be guilty of a misdemeanor and subject to a fine of up to \$250 for a first violation and \$1000 for each subsequent violation. If the person knowingly and willfully violates the law, it will be a Class F felony, punishable by up to five years in prison and/or a fine up to \$1000. A conviction of this crime, combined with the possession of identifying information, is prima facie evidence of financial identity fraud, identity fraud, or identity theft.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Change of Address: Consumer credit reporting agencies must notify creditors who use a consumer report if the agency becomes aware that an application to a card issuer to open a new credit card account bears an address for the consumer that is different from the address in its file on the consumer.

In addition, state law requires a credit card issuer that receives an application with a different address in response to a mailed unsolicited offer to verify the change of address with the person to whom the solicitation or offer was mailed. If the credit card issuer receives a written or oral request for a change of the cardholder's billing address, and within a period of up to 30 days

after the requested change receives a request for an additional credit card, the issuer may not mail the requested additional card to the new address or activate the additional card unless the issuer has verified the change of address.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Social Security Numbers: A person may not publicly post or display or otherwise intentionally communicate or make available to the public a consumers' Social Security number (SSN) or a portion of it containing 6 digits or more. In addition, under the law, it is illegal for any person to:

- Intentionally print or imbed a consumer's SSN 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;
- 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 SSN is encrypted;
- Require a consumer to use his SSN 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;
- Print a consumer's SSN 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 SSN to be on the document to be mailed;
- Sell, lease, loan, trade, rent, or otherwise intentionally disclose a consumer's SSN 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 SSN does so for a legitimate business or government purpose or unless authorized or specifically permitted by law to do so.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

State law also seeks to minimize the instances in which state and local government entities disseminate Social Security numbers (SSN) both internally within government or externally with the general public. It prohibits a public body from collecting a SSN 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 SSN is otherwise imperative for the performance of that body's duties and responsibilities. SSNs 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 SSNs has been clearly documented. The bill also:

- Requires that public bodies segregate SSNs on a separate page from the rest of the record so that the SSN may be easily redacted pursuant to a public records request.
- Requires that public bodies provide a statement of purpose or purposes for which the SSN is being collected and used.
- Prohibit public bodies from using the SSN for a purpose other than that stated.
- Prohibits public bodies from intentionally communicating or otherwise making available to the general public an individual's SSN or other personal identifying information.
- Prohibits the intentional printing or imbedding of an individual's SSN on any card required for the individual to access government services.
- Prohibits a public body from requiring an individual to transmit the individual's SSN over the Internet, unless the connection is secure or the SSN is encrypted.

- Prohibits a public body from requiring an individual to use his/her SSN 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.
- Prohibits a public body from printing an individual's SSN on materials that are mailed to the individual, unless state or federal law requires it.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Victim Assistance:

Mandatory Police Reports: 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 is required to 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.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Criminal Identity Theft: Under state law, if a person obtains personal identifying information of another person and uses that information to commit a crime in addition to the crime of identity theft, court records must reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

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 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.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

The State Law Enforcement Division (SLED) must establish and maintain appropriate records of individuals who have been the victims of identity theft. The records will be maintained in a computerized database, and access to the records will be limited to criminal justice agencies, except that a victim of identity theft, or his authorized representative, will have access to the records in order to establish that he is a victim of identity theft. To be included in the database, a victim of identity theft must submit to SLED a copy of the police report, a full set of fingerprints, or other relevant information. SLED will 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.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Security Freeze: State law allows all consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information. To request a freeze, a consumer must request one in writing or by e-mail to the credit reporting agencies. Credit reporting agencies are not permitted to charge consumers to place or temporarily lift a credit freeze.

The reporting agency must place the freeze within five business days after receiving the request, and within ten business days must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time. Requests for removing the freeze must be completed within three business days. Requests for a temporary removal of the freeze, either for a designated time period or for a specific company, must be completed within 15 minutes if the request is made electronically or by telephone. In addition, consumer reporting agencies 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.

If a security freeze is in place, a consumer reporting agency must notify the consumer in writing of any changes in the file of the consumer's name, date of birth, Social Security number, or address within 30 days after the change is made.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Instructions for Placing a Security Freeze in South Carolina:

<http://www.consumersunion.org/pdf/security/securitySC.pdf>

Credit Report Disputes: If a consumer disputes the accuracy of an item in his records with a consumer reporting agency with a written request, the agency must 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 must provide forms for that notice and must assist a consumer in preparing the notice when requested. Within 30 days after receiving a notice of inaccuracy, the agency must deny or admit the inaccuracy to the consumer in writing. If the item is inaccurate, the consumer reporting agency must correct the item in its records, and on request by the consumer, inform any person who within the last 6 months received a report containing the inaccurate information.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Disposal of Records: To prevent identity theft, state law restricts how businesses and government agencies can dispose of records with personal identifying information about individuals. Beginning July 1, 2009, all organizations, businesses, and government agencies that collect personal information must have measures for the safe disposal of material in a manner that makes it unreadable or undecipherable. The law targets both paper records and electronic records, including those stored on computer equipment or computer media.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

Security Breach: Beginning July 1, 2009, state law will require state agencies and businesses operating in the state to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. The law applies to any state agencies, organizations or businesses that maintain consumers' personal information, and notification must be provided following discovery or notification of the breach in the security of the data. A security breach is defined as any 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.

Personal identifying information includes Social Security numbers, driver's license numbers, checking or savings account numbers, credit and debit card numbers, personal identification numbers, electronic identification numbers, digital signatures, or other numbers or information that can be used to access a person's financial resources, or identifying documentation that defines a person other than the person presenting the document. This includes, but is not limited to, passports, driver's licenses, birth certificates, immigration documents, and state-issued identification cards.

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. This notice can be provided to the affected person by mail, e-mail, or telephone. If the cost of providing regular notice would exceed \$250,000, the amount of people to be notified exceeds \$500,000, or the business does not have sufficient contact information, substitute notice can be used. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the entity's web site, and notification to major statewide media. Notice of the security breach must also be given to the Department of XXX if 1000 or more South Carolina consumers are affected.

Legislation: http://www.scstatehouse.net/sess117_2007-2008/bills/453.htm

State Resources:

Department of Consumer Affairs, "ID Theft: What To Do If It Happens To You"

(http://www.sconsumer.gov/publications/flyers/id_theft.pdf)

This document directs victims to: "*Contact local law enforcement and get a written report of the theft.*"

Office of Regulatory Affairs, "Identity Theft and Phishing"

(<http://www.regulatorystaff.sc.gov/ORSContent.asp?pageID=640>)

Legislation:

2008:

South Carolina lawmakers passed a comprehensive anti-identity theft law (**SB 453**). The bill:

- Allows South Carolina residents to place and lift a security freeze on their credit reports, without paying a fee. Indiana is currently the only state that requires credit agencies to provide freezes at no charge. Credit reporting agencies must temporarily lift a credit freeze within 15 minutes of receiving a consumer's request.
- Requires law enforcement agencies to take a report from a person who believes or suspects that he is a victim of identity theft.
- Requires credit reporting agencies to investigate, at consumers' requests, suspected inaccuracies in a credit report, then provide sufficient evidence the information is true and accurate. It also provides for penalties for agencies that fail to erase erroneous information from credit reports within 30 days of being properly notified.
- Requires businesses to properly dispose of sensitive paper and electronic consumer information so that it does not fall into the wrong hands.
- Requires companies and state agencies to notify customers when there's been a security breach that exposes their personal information.
- Prohibits some uses of Social Security numbers, including public posting or display, printing the number on any card required by consumers to access services or products, requiring unsecured transmission of it over the Internet, or printing it on any materials that are mailed to an individual unless such publication is required by state or federal law.
- Requires banks and other agencies to notify consumers when an application for a new line of credit has an address different from the one on file for that consumer.
- Makes it illegal to "rummage through or steal another person's household garbage or litter ... for the purpose of committing financial identity fraud or identity theft."
- Prohibits retailers from printing on a receipt more than five digits of a credit or debit card account number and the expiration date of the card. This 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.
- Requires the State Law Enforcement Division to establish an identity fraud database.

2006:

HB 3085 creates the offense of identity fraud for the purpose of obtaining and employment. It also adds “identifying documentation that defines a person other than the person presenting the document. This includes, but is not limited to, passports, driver's licenses, birth certificates, immigration documents, and state-issued identification cards” to the list of identifying information subject to the identity fraud law.

2000:

HB 3508 makes the crime of financial identity fraud a felony, punishable by up to ten years in prison and/or a fine. It targets people who use personal information such as a Social Security number, credit card or driver's license to access another person's financial information.