

NORTH CAROLINA

IDENTITY THEFT RANKING BY STATE: Rank 22, 67.0 Complaints Per 100,000

Population, 6069 Complaints (2007)

Updated January 19, 2009

Current Laws:

The crime of identity theft occurs when a person knowingly obtains, possesses, or uses the identifying information of another person, living or dead, with the intent to fraudulently represent that he/she is the other person for the purposes of making financial or credit transactions in the other person's name; to obtain anything of value, benefit, or advantage; or for the purpose of avoiding legal consequences. It is a class G felony, punishable by 8 to 20 months in jail (sentences increase if the defendant has any prior felony convictions). However, if the victim suffers arrest, detention, or conviction as a proximate result of the offense, or the person is in possession of the identifying information of three or more separate people, it is a class F felony, punishable by 10 to 24 months in jail (sentences increase if the defendant has any prior felony convictions).

“Identifying information” includes a Social Security or employer taxpayer identification number; driver’s license, state identification card, or passport numbers; checking or savings account numbers; credit or debit card numbers; personal identification (PIN) codes; electronic identification numbers, e-mail names or addresses; digital signatures; any other numbers or information that can be used to access a person’s financial resources; biometric data; fingerprints; passwords; or a parent’s maiden name.

Statute: §14.113.20:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.20.html

A person is guilty of trafficking in stolen identities if he/she sells, transfers, or purchases the identifying information of another person with the intent to commit identity theft or to assist another person in committing identity theft. Violations are a Class E felony, punishable by 15 to 47 months in jail (sentences increase if the defendant has any prior felony convictions).

Statute: §14-113.20A:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.20A.html

Jurisdiction: The crime is considered to be committed in the county where the victim resides, where the perpetrator resides, where any part of the financial identity fraud took place, or in any other county instrumental to the completion of the offense, regardless of whether the defendant was actually present in that county.

Statute: §14.113.21:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.21.html

The Attorney General may investigate any complaint regarding identity theft, and must refer all cases of identity theft to the district attorney where the crime was deemed committed.

Statute: §14-113.23:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.23.html

Payment Cards: A person is guilty of financial transaction card theft, a class I felony, when he:

- Takes, obtains, or withholds a financial transaction card from the person, possession, custody or control of another without the cardholder's consent and with the intent to use it;
- With knowledge that the card has been so taken, obtained, or withheld, receives the card with the intent to use, sell, or transfer it to a person other than the issuer or cardholder;
- Receives a card that he knows to have been lost, mislaid, or delivered by mistake, and who retains possession with intent to use, sell, or transfer it;
- Sells or buys a card from a person other than the issuer;
- During any 12-month period, receives financial transaction cards issued in the names of two or more persons that he has reason to know were obtained improperly, as described above; or
- With the intent to defraud any person, uses a scanning device to access, read, obtain, memorize, or store information encoded on another person's financial transaction card or receives the encoded information from another person's financial transaction card.

A financial transaction card (FTC) means any instrument or device, including a credit card, credit plate, bank services card, banking card, check guarantee card, debit card, or by any other name, issued with or without fee by an issuer for the use of the cardholder:

- In obtaining money, goods, services, or anything else of value on credit;
- In certifying or guaranteeing to a person or business the availability to the cardholder of funds on deposit that are equal to or greater than the amount necessary to honor a draft or check payable to the order of such person or business;
- In providing the cardholder access to a demand deposit account or time deposit account.

Statute: §14-113.9:

www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.9.html

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 financial transaction cards have been obtained in fraudulently.

Statute: §14-113.10:

www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.10.html

It is a class I felony to sign a financial transaction card, if not the cardholder or a person authorized by him, with intent to defraud the issuer, a person or organization providing money, goods, services or anything else of value, or any other person, signs a financial transaction card.

Statute: §14-113.11:

www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.11.html

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

- Uses for the purpose of obtaining money, goods, services or anything else of value a financial transaction card obtained or retained, or which was received with knowledge that it was obtained or retained, fraudulently or which he knows is forged, altered, expired, revoked or was obtained as a result of a fraudulent application;
- Obtains money, goods, services, or anything else of value by representing without the consent of the cardholder that he is the holder of a specified card; presenting the financial transaction card without the authorization or permission of the cardholder; representing that he is the holder of a card and such card has not in fact been issued; or using a financial transaction card to knowingly and willfully exceed the actual balance of a demand deposit account or time deposit account; or an authorized credit line;
- Deposits into his account or any account, by means of an automated banking device, a false, fictitious, forged, altered or counterfeit check, draft, money order, or any other such document not his lawful or legal property; or
- Receives money, goods, services or anything else of value as a result of a false, fictitious, forged, altered, or counterfeit check, draft, money order or any other such document having been deposited into an account via an automated banking device, knowing at the time of receipt of the money, goods, services, or item of value that the document so deposited was false, fictitious, forged, altered or counterfeit or that the above deposited item was not his lawful or legal property.
- Upon application for a financial transaction card to an issuer, knowingly makes or causes to be made a false statement or report relative to his name, occupation, financial condition, assets, or liabilities; or willfully and substantially overvalues any assets, or willfully omits or substantially undervalues any indebtedness for the purpose of influencing the issuer to issue a financial transaction card.

Violations are a class 2 misdemeanor if the value of all money, goods, services, and other things of value does not exceed \$500 in any six-month period, and a class I felony if over \$500.

Statute: §14-113.13:

www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.13.html

Social Security Numbers: State law restricts the public availability of Social Security numbers (SSNs). It allows businesses to collect SSNs and other identifying information only for legitimate purposes or when required by law. The law also prevents businesses from using SSNs for customer identification, printing it on any card or material mailed to an individual unless required by federal law, and restricts them from selling or displaying SSNs to a third party without an individual's written consent. It also prohibits requiring an individual to transmit his SSN over the Internet unless the connection with the Internet is secure or the number is encrypted. The law also prohibits requiring an individual's SSN for access to an Internet

website, unless a password or unique personal identification number or other authentication device is also required for access.

Statute: §75-62:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-62.html

Disposal of Customer Records: To prevent identity theft, state law restricts how businesses can dispose of paper records with personal identifying information about individuals. The law prohibits businesses from knowingly discarding paper records or documents with sensitive identifying data without first redacting the data or shredding or otherwise destroying the documents.

Statute: §75-64:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-64.html

Criminal Identity Theft: In order to combat criminal identity theft, in which a person assumes the identity of another during an arrest or motor vehicle infraction, state law allows law enforcement to take photographs of a person who is cited for a motor vehicle moving violation and does not produce a valid drivers license upon request, if the officer has a reasonable suspicion concerning the true identity of the person. This photo may not be used for any purpose other than to confirm the identity of the alleged offender and must be destroyed upon final disposition of the charge.

Statute: 15A-502:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_15A/GS_15A-502.html

Victim Assistance:

Mandatory Police Reports: A person who has learned or reasonably suspects that he/she has been the victim of identity theft may contact the local law enforcement agency that has jurisdiction over his/her residence. Even if the crime was committed in another jurisdiction, the local law enforcement agency may take the complaint, issue an incident report, and provide the complainant with a copy of the report. The agency may refer the report to the law enforcement agency where the crime occurred for investigation and prosecution. A complaint filed or report issued under this section is not required to be counted as an open case for purposes of compiling open case statistics.

Statute: §14-113.21A:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.21A.html

Restitution: In addition to criminal penalties, the court may order a person convicted of identity theft crimes to pay restitution to the victim for financial loss caused by the violation. This may include, in addition to actual losses, lost wages, attorneys' fees, and other costs incurred by the victim in correcting his/her credit history or credit rating.

Statute: §14-113.22:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.22.html

Civil Suits: Identity theft victims may sue the offender for damages, even if the person has not been charged criminally, up to triple the actual damages or \$5,000, whichever is greater.

Statute: §1-539.2C:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_1/GS_1-539.2C.html

Court Records: In any case in which a person obtains the identifying information of another person, uses that information to commit another crime, and is convicted of that additional crime, the court records must be changed to reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

Statute: §14-113.22:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_14/GS_14-113.22.html

Expungement: Victims of criminal identity theft whose charges were dismissed or who were found not guilty or whose conviction was set aside may apply to have those charges or convictions removed from their record.

Statute: §15A-147:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_15A/GS_15A-147.html

Form for Expungement:

<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications/&file=Form%20for%20Expungement.pdf>

Security Freeze: All North Carolina consumers are allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened 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 by certified mail. Consumer reporting agencies may charge a fee of up to \$10 to place or temporarily lift a security freeze. However, security freezes are free for victims of identity theft who provide a copy of a police report and for veterans who have received notification from the U.S. Department of Veterans Affairs that their personal identifying information may have been part of a data breach.

The reporting agency must place the freeze within five business days after receiving the request, and within ten 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 a temporary unlocking of the freeze must be completed within three business days.

Statute: §75-63:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-63.html

Instructions on How to Place a Security Freeze:

<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications&file=securityfreeze.pdf>

Sample Letter:

<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications/&file=freeze%20letter081806.pdf>

Security Breach: State law requires government 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. A security breach is defined as the unauthorized access and acquisition of unencrypted or unredacted records and data containing personal information with corresponding names, such as a person's first initial and last name. Notification must occur if there is a reasonable likelihood that consumers' identifying information, including Social Security numbers, bank account numbers, credit card and debit card numbers, personal identification numbers, driver's license number, biometric data (fingerprints), or any other number that can be used to access financial resources has been compromised. In addition, the access and acquisition of an individual's e-mail name or address, Internet account number, Internet username, or password may be considered a breach if it would permit access to financial accounts and resources.

Once a business or agency discovers or is informed of a security breach, it must notify the individuals affected, regardless of number. The notice must be clear and conspicuous and given without unreasonable delay. Notice can be delayed if law enforcement decides that disclosure of the breach would impede a criminal investigation. The notice can be mailed, e-mailed, or given by phone. If contact information is not available, more than 500,000 people were affected by the breach, or if providing notification would cost more than \$250,000, substitute forms of notice may be given, including posting a notice on a website and notifying major statewide media. If the breach affects more than 1,000 people, the business must also notify the Consumer Protection Division of the North Carolina Attorney General's Office.

Statute: §75-65:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-65.html

Office of the Attorney General, "Received a Security Breach Letter?"

(<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications/&file=breachtip.pdf>)

This document explains: *"Most law enforcement agencies will not issue a police report unless your private information has actually been used to commit identity theft. If you suspect that you have become the victim of identity theft, contact local law enforcement immediately."*

"Security Breach Information"

(<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications/&file=breachinfo081606.pdf>)

Protection of Personal Information: State law prohibits any person or company from knowingly broadcasting or publishing to the public on radio, television, in writing, or on the Internet, the personal information of another person with actual knowledge that the person whose personal information has been disclosed has previously objected to any such disclosure.

Statute: §75-66:

http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/BySection/Chapter_75/GS_75-66.html

State Resources:

Office of the Attorney General, “Stop ID Theft In Its Tracks” (<http://noscamnc.gov/>)

“Victim Toolkit” (<http://noscamnc.gov/toolkit.html>)

“The key to minimizing the damage an ID thief can do to your wallet and your reputation is taking action fast. The information below will guide you in reporting the crime, contacting financial organizations and taking back your security and privacy.”

“Identity Theft Victim Toolkit”

(<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications/&file=ID%20Theft%20Victim%20Toolkit.pdf>)

This document includes a comprehensive checklist that victims should take, depending on which of their personal identifying information was stolen. It directs victims that their first step should be to: **“Promptly report the fraud to law enforcement. North Carolina law provides that identity theft is a felony. Report the fraud to your local police department, and, if known, the police department in the location where your identity was used for illegal purposes. Get a copy of the police report. This immediately alerts local law enforcement to the crime, and it establishes that you acted diligently. Get a police report, complaint number or other similar record, which you may need when contacting your creditors. Also, keep the phone number of your fraud investigator handy. Identity theft is a crime often involving more than one jurisdiction. Therefore, you may need to be persistent when attempting to file a police report. Stress the importance of a police report; many creditors require one to resolve your dispute. Credit bureaus will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but only if you can give them a copy of the police report.**

It also includes a sample letter to creditors, identity theft affidavit, and a fraudulent account statement.

“Steps To Take When Your ID Is Stolen”

(<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications/&file=steps081606.pdf>)

This document tells victims that the first step they should take if their ID is stolen is to: *“File a Police Report.”* It explains that victims should optimally *“file a police report where the crime occurred. The case is more likely to be investigated where the crime took place. Example: If your credit card number was used at a business in Charlotte, file a report with the Charlotte-Mecklenburg Police Department.”* The second choice is to: *“file a police report where you live or where the suspected thief lives.”* It explains that victims should file a police report because *“filing a police report triggers helpful protections under both federal and state law, such as an*

extended fraud alert and a free security freeze. A police report will be useful as you contact creditors to try to restore your credit. Get a copy of your police report.”

“Steps To Take When Your ID Has Been Used Criminally”

(<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications/&file=criminal081706.pdf>)

This document includes information for victims of criminal identity theft, which occurs when “a criminal, during an investigation or upon arrest, gives your name and information to law enforcement instead of his or her own. Victims of criminal identity theft may be arrested, detained or convicted for crimes committed by someone else in their name.” It includes steps to take regarding worthless check charges, traffic charges, including failure to appear in court and guilty plea, and other criminal charges. It recommends that for criminal charges, victims should “Contact the charging officer. Schedule a time to meet with the officer to prove that you were not the person charged. If you don’t live nearby, ask law enforcement in your area to take your picture and fingerprints and send them to the charging officer or Assistant District Attorney.”

“Freeze Access to Your Credit”

(<http://www.ncdoj.com/DocumentStreamerClient?directory=Publications&file=securityfreeze.pdf%20>)

Division of Motor Vehicles, “Identity Theft: What Can You Do”

(http://www.ncdot.org/DMV/other_services/licensetheft/identityTheft.html)

This document includes tips for people whose identity may have been stolen.

Legislation:

2007:

HB 454 allows a law enforcement officer to take a photograph of a person who is cited for a motor vehicle moving violation and does not produce a valid driver’s license upon request, if the officer has a reasonable suspicion concerning the true identity of the person. This photo may not be used for any purpose other than to confirm the identity of the alleged offender and must be destroyed upon final disposition of the charge. This law seeks to combat criminal identity theft, in which a person assumes the identity of another during an arrest or motor vehicle infraction.

The legislation also prohibits any person or company from knowingly broadcasting or publishing to the public on radio, television, in writing, or on the Internet, the personal information of another person with actual knowledge that the person whose personal information has been disclosed has previously objected to any such disclosure.

2006:

HB 1248 requires government agencies to notify consumers when their personal information is compromised during a security breach. Previously, only businesses were required to disclose the loss of such data.

2005:

The Identity Theft Protection Act (**SB 1048**) contains several important provisions to prevent identity theft and help victims of the crime. It allows businesses to collect Social Security numbers (SSNs) and other identifying information only for legitimate purposes or when required by law. It prevents businesses from using SSNs for customer identification, printing it on any card or material mailed to an individual unless required by federal law, and restricts them from selling or displaying SSNs to a third party without an individual's written consent. It also prohibits companies from requiring a consumer to transmit a SSN over the Internet, unless the connection is secure or the SSN is encrypted, and from requiring an individual to use his/her SSN to access the Web site, unless a password or unique personal identification number or other authentication device is also required to access the site.

In addition, companies would be required to take preventative measures to combat identity theft in handling customers' personal information. It requires companies to properly shred or destroy any records containing customers' personal information before they throw it away. An amendment to the bill exempts Internet account numbers, e-mail addresses and names, and drivers' license numbers on law enforcement records from being considered personal information under this statute.

The bill also requires most businesses to notify customers if a security breach compromises their personal information and puts them at risk of identity theft. Notification must occur if there is a reasonable likelihood that their identifying information, including SSNs, bank account numbers, driver's license number, biometric data (fingerprints), passwords, or a parent's maiden name, has been compromised. If the breach affects more than 1,000 people, the business must also notify the Consumer Protection Division of the North Carolina Attorney General's Office.

The bill also grants consumers the right to place a security freeze on their credit reports to prevent an identity thief from opening an account or obtaining credit under their name.

It also allows victims of identity theft to file complaints at their local police departments. A person who has learned or reasonably suspects that he/she is a victim of identity theft may contact the local law enforcement agency that has jurisdiction over the person's actual residence. The agency may take the complaint, issue an incident report, and provide the complainant with a copy of the report. The agency may refer the report to a law enforcement if the jurisdiction where the crime committed.

2002:

HB 1100 is designed to toughen the state's financial fraud laws while expanding the rights of victims to sue identity thieves. The bill makes it a felony to traffic the information of others for financial gain. Financial identity fraud is also expanded to include taking the information of living or dead people, such as fingerprints and passwords. In addition, identity theft victims could sue the thief for damages, even if the person has not been charged criminally, up to triple the actual damages or \$5,000, whichever is greater. A court may also order convicted thieves to pay restitution.

2001:

SB 262 provides that a person who is wrongfully charged with a criminal offense due to identity fraud could have the wrongful charge cleared from their record. This law applies to court records, DMV records, law enforcement agency records, and any other state or local government records.