ID Safety
Protecting the *real* you, and *only* you.

In partnership with: INTERNATIONAL ASSOCIATION of CHIEFS OF POLICE Bank of America

GEORGIA
IDENTITY THEFT RANKING BY STATE: Rank 7, 91.6 Complaints Per 100,000 Population, 8744 Complaints (2007)
Updated: November 30, 2008

Current Laws: A person commits the offense of identity fraud when he or she willfully and fraudulently:

- Without authorization or consent, uses or possesses with intent to fraudulently use, identifying information concerning an individual;
- Uses identifying information of an individual under 18 years old over whom he or she exercises custodial authority;
- Uses or possesses with intent to fraudulently use, identifying information concerning a deceased individual;
- Creates, uses, or possesses with intent to fraudulently use, any counterfeit or fictitious identifying information concerning a fictitious individual with intent to use such counterfeit or fictitious identification information for the purpose of committing or facilitating the commission of a crime or fraud on another person; or
- Without authorization or consent, creates, uses, or possesses with intent to fraudulently use, any counterfeit or fictitious identifying information concerning a real individual with intent to use such counterfeit or fictitious identification information for the purpose of committing or facilitating the commission of a crime or fraud on another person.

A person commits the offense of identity fraud by receipt of fraudulent identification information when he or she willingly accepts for identification purposes identifying information that he or she knows to be fraudulent, stolen, counterfeit, or fictitious. For prosecution of this offense, it is not necessary to show a conviction of the principal thief, counterfeiter, or fraudulent user.

These provisions do not apply to a person under the age of 21 who uses a fraudulent, counterfeit, or other false identification card for the purpose of obtaining entry into a business establishment or for purchasing items that he or she is not of legal age to purchase.
Statute: §16-9-120: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

"Identifying information" includes, but is not limited to: current or former names; Social Security numbers; driver's license numbers; checking and savings account numbers; credit, debit, and other financial transaction card numbers; personal identification numbers; electronic identification numbers; digital or electronic signatures; medical identification numbers; birth dates; mother's maiden name; tax identification numbers; state identification card numbers; or any other numbers or information which can be used to access a person's or entity's resources.

Violations are punishable by one to ten years in prison and/or a fine up to $100,000. Second or subsequent offenses are punishable by three to fifteen years in prison and/or a fine up to $250,000. Each violation constitutes a separate offense.

Statute: §16-9-120: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

It is also unlawful to attempt to commit the offense of identity fraud, punishable by imprisonment or community service and/or a fine, up to the maximum punishment prescribed for the offense that was the object of the attempt.
Statute: §16-9-122: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Jurisdictions: The crime of identity fraud is considered to have been committed in any county where the person whose means of identification or financial information was appropriated resides or is found; or in any county in which any other part of the offense took place, regardless of whether the defendant was ever actually in such county.
Statute: §16-9-125: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Investigations: The Governor's Office of Consumer Affairs has the authority to investigate any complaints of consumer victims regarding identity theft. In conducting such investigations, the office has certain investigative powers. Any theft of personal financial information should be reported to the office. If, after such investigation, the office determines that a person has been a consumer victim of identity fraud, it will, at the request of the consumer victim, provide him/her with certification of the findings of the investigation. The office also maintains a repository for all complaints in state regarding identity fraud. Consumer victims of identity fraud may file complaints directly with the office.
Statute: §16-9-123: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Payment Cards: A person commits the offense of financial transaction card theft when he:

- Takes, obtains, or withholds a financial transaction card from the person, possession, custody, or control of another without the cardholder's consent; or who, with knowledge that it has been so taken, obtained, or withheld, receives the financial transaction card with intent to use it or to sell it or to transfer it to a person other than the issuer or the cardholder;
- Receives a financial transaction card that he knows to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder and he retains possession with intent to use it or sell it or to transfer it to a person other than the issuer or the cardholder;
- Not being the issuer, sells a financial transaction card or buys a financial transaction card from a person other than the issuer; or
- Not being the issuer, during any 12 month period receives two or more financial transaction cards in the names of persons which he has reason to know were taken or retained fraudulently.
- When a person has in his possession or under his control two or more financial transaction cards issued in the names of persons other than members of his immediate family or without the consent of the cardholder, such possession is prima-facie evidence that the financial transaction cards have been obtained fraudulently.

Statute: §16-9-31: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

A person commits the crime of financial card 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; a financial transaction card which he or she knows is forged, altered, expired, revoked, or was obtained as a result of a fraudulent application; or the financial transaction card account number of a financial transaction card which he or she knows has not in fact been issued or 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 or she is the holder of a specified card; presenting the financial transaction card without the authorization or permission of the cardholder; falsely representing that he or she is the holder of a card and such card has not in fact been issued; or giving, orally or in writing, a financial transaction card account number to the provider of the money, goods, services, or other thing of value for billing purposes without the authorization or permission of the cardholder for such use.
- 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, employer, 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 punishable by one to two years in prison and/or a fine up to $1,000, if the value of all money, goods, services, and other things of value does not exceed $100 in any six-month period. If the value exceeds $100 in a six-month period, it is a felony, punishable by one to three years in prison and/or a fine up to $5000.
Statute: §16-9-33: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Scanning Devices: State law prohibits the use of a scanning device or reencoder that is used to obtain or record encoded information from the magnetic strip of a payment card to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A reencoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are punishable by one to three years in prison and/or a fine up to $10,000. A second or subsequent offense is punishable by three to ten years in prison and/or a fine up to $50,000. Violators can also be ordered to make restitution to any consumer or business victim.
Statute: §10-15-4: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Phishing: State law prohibits phishing, a form of identity theft that uses an e-mail that appears to represent a legitimate Web site and requests personal information that can be used to access a person's financial accounts or obtain goods and services. The bill prohibits a person, with the intent to defraud, by means of a Web page, electronic mail message, or otherwise through the use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing himself, herself, or itself to be a business without the authority or approval of such business. It is also unlawful for any person, with actual knowledge, conscious avoidance of actual knowledge, or willfully, to possess with intent to use

in a fraudulent manner, sell, or distribute any identifying information obtained through phishing. Violators will be guilty of a felony and punished by imprisonment of one to twenty years, and/or a fine of $1000 to $500,000.
Statute: § 16-9-109.1: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Spyware: State law prohibits the use of spyware, computer software that can be sent through the Internet into a home or business computer to modify settings or record information without the user's knowledge. It prohibits a person or entity that is not the authorized user of a computer to knowingly, willfully, or with conscious indifference or disregard cause computer software to be copied on to a computer and use it to do any of the following: to take possession of another's computer, to divert Internet browsers to unauthorized websites, modify settings, collect personally identifiable information through keystroke logging, interfere with downloads, install or uninstall software without authorization, falsify an identity to obtain personal information, or mislead computer users in other ways.

Violations are a felony, punishable by one to ten years in prison and/or a fine of up to $3 million. In addition, the Attorney General may bring a civil action against any violator to enforce the penalties for the violation and may recover any or all of the following: a civil penalty of up to $100 per violation or up to $100,000 for a pattern or practice of such violations; costs and reasonable attorney's fees; and an order to enjoin the violation.
Statute: §16-9-152: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Disposal of Records: State law prohibits a business from discarding a consumer record containing personal information unless it shreds the customer's record, erases the personal information contained in the record, modifies the customer's record to make the personal information unreadable; or takes actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the customer's record for the period between the record's disposal and the record's destruction. A fine of up to $500 may be levied for each customer's record that contains personal information that is wrongfully disposed of or discarded, with a maximum total fine of up to $10,000.
Statute: §10-15-2: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Change of Address: State law requires a credit card issuer who mails an unsolicited offer to apply for a credit card and receives by mail a completed application that lists a different address than the one on the solicitation to take steps to verify the applicant's valid address before issuing the card.
Statute: §10-1-393-29.1: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Victim Assistance:

Mandatory Police Reports: A person who has learned or reasonably believes that he or she has been the victim of identity fraud may contact the local law enforcement agency with jurisdiction over his or her actual residence for the purpose of making an incident report. The law enforcement agency having jurisdiction over the complainant's residence must make a report of the complaint and provide the complainant with a copy of the report. Where jurisdiction for the investigation and prosecution of the complaint lies with another agency, the law enforcement

agency making the report must forward a copy to the agency having such jurisdiction and must advise the complainant that the report has been so forwarded. A report created pursuant to this section is not required to be counted as an open case file.
Statute: §16-9-125.1: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Restitution: Any person found guilty of identity fraud may be ordered by the court to make restitution to any consumer victim or any business victim of such fraud.
Statute: §16-9-126: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Court Orders: Upon a conviction of a violation of an identity fraud offense, the court may issue any order necessary to correct a public record that contains false information resulting from the actions that resulted in the conviction.
Statute: §16-9-126: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Civil Suits: Any business victim who is injured by reason of any identity fraud violation has a cause of action for the actual damages sustained and, where appropriate, punitive damages. A business victim may also recover attorney's fees in the trial and appellate courts and the costs of investigation and litigation reasonably incurred.
Statute: §16-9-129: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Any consumer victim who suffers injury or damages as a result of an identity fraud violation may bring an action individually or as a representative of a class against the person or persons engaged in the violations to seek equitable injunctive relief and to recover general and punitive damages sustained as a consequence. Punitive damages can be awarded only in cases of intentional violation. Courts can award attorney's fees and expenses of litigation. The court must award three times actual damage for an intentional violation.
Statute: §16-9-130: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Security Breach: State law requires information brokers and data collectors, including state and local agencies, to notify consumers when their unencrypted personal information is compromised during a security breach, putting them at risk of identity theft. Information brokers are defined as any person or entity who for monetary fees or dues engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties. A data collector is defined as any state or local agency or subdivision thereof, including any department, bureau, authority, public university or college, academy, commission, or other governmental entity. However, it does not apply to any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

A security breach occurs upon "unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker"

Personal information is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social Security number, driver's license number or state identification card number, account number, credit, or debit card number, if circumstances exist where such a number could be used without additional identifying information, access codes, or passwords; account passwords or personal identification numbers or other access codes; or any of the previously mentioned items when not in combination with the individual's first name or initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised. It does not include publicly available information.

Disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. If the breach affects more than 10,000 people, the entity must also notify the consumer reporting agencies.

Notification can be provided to the affected persons by mail, e-mail, or telephone. If the cost of providing regular notice would exceed $50,000, the amount of people to be notified exceeds 100,000, or the information broker or data collector does not have sufficient contact information to provide written or electronic notice, substitute notice may be provided. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the information broker's or data collector's web site, and notification to major statewide media.
Statute: §10-1-911 through 912: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

Security Freeze: State law allows all Georgia 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 by certified mail to the credit reporting agencies. In addition, the consumer credit reporting agencies must make available to consumer an Internet-based method of requesting a security freeze and a toll-free telephone number for consumers to use to place a security freeze, temporarily lift a security freeze, or completely remove a security freeze.

The reporting agency must place the freeze within three business days after receiving the written request, and within ten business days of placing the freeze 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. If the request for temporary unlocking of the freezes is made by telephone or other electronic means, the unlocking must be done with 15 minutes, if the request is received during normal business hours.

A consumer reporting agency may charge up to $3 to place, remove, or temporarily suspend a security freeze. Victims of identity theft and people 65 or older will not be charged any fees in connection with the placing, removing, or temporary lifting of a security freeze.
Statute: §10-1-913 through 914: (Statutes available at http://www.lexis-nexis.com/hottopics/gacode/)

State Resources:

Office of Consumer Affairs, "Identity Theft"
(http://consumer.georgia.gov/00/article/0,2086,5426814_39039081_38690684,00.html)

"Identity Theft – Instructions for Victims"
(http://consumer.georgia.gov/00/article/0,2086,5426814_39039081_39480072,00.html)
This comprehensive site includes advice to victims on the steps they should take, based on what information has been compromised. It directs victims to: "***Report the crime immediately to your local police*** *and, if you believe the crime took place in a different locale, to law enforcement officials there. Since the Official Code of Georgia Annotated Section 16-9-121 makes identity theft a felony in Georgia, you should ask the police to issue a police report pursuant to the theft of your personal identification information. Give them as much information as possible and copies of all your documentation. Get a copy of the report for your files. Creditors, banks, credit reporting-agencies and insurance companies may require a police report to verify the crime of identity theft*."

"Georgia Consumer's Guide to Identity Theft" (http://www2.state.ga.us/GaOCA/broidtheft.htm)

Department of Banking and Finance, "Identity Theft"
(http://dbf.georgia.gov/00/article/0,2086,43414745_46389324_67825090,00.html)

"Phishing and Identity Theft"
(http://dbf.georgia.gov/00/article/0,2086,43414745_43418327_69079842,00.html)

Georgia Security Council, "Identity Theft Prevention"
(http://www.georgiasecuritycouncil.org/Default.aspx?tabid=71)
This site is a partnership between the Office of the Attorney General and the Georgia Stop Identity Theft Network. It includes numerous prevention tips for consumers.

Legislation:

2008:
HB 130 allows Georgians to freeze their credit to thwart identity thieves. Residents can place a freeze on their credit for $3, and anyone 65 or older may place such a freeze for free. It allows identity theft victims and anyone 65 or older to place a freeze for free. When a freeze is in place, it prevents credit reporting agencies from releasing a resident's information without written permission. It also allows residents to temporarily unfreeze the account if they choose.

SB 24 protects Georgia's consumers by increasing the penalties against identity theft by the use of Internet phishing, a method criminals use to steal an individual's identity through the Internet. Under the law, phishing is now a felony.

SB 388 establishes the Georgia Bureau of Investigation (GBI) Identity Theft Task Force and transfers the authority to investigate identity theft from the Governor's Office of Consumer Affairs to the GBI.

2007:
SB 236 makes several changes to the state's identity theft laws. The bill:

- Expands the security breach notification laws to include state and local government agencies, including public universities and colleges.
- Requires law enforcement agencies to take and provide a police report to any person who lives in their jurisdiction who has learned or reasonably believes that he or she has been the victim of identity fraud. Where jurisdiction for the investigation and prosecution of the complaint lies with another agency, the law enforcement agency making the report must forward a copy to the agency having jurisdiction and advise the complainant that the report has been so forwarded.
- Clarifies the definition of identity fraud as the willful and fraudulent use, possession or intent to fraudulently use, of identification data of anyone under 18, a deceased person or a fictitious entity. The recipient of such illicit data would also be guilty of identity fraud and subject to the same punishment.

2005:
SB 230 requires information brokers that keep confidential personal information about consumers to notify those consumers if that information has been compromised by an unauthorized disclosure or security breach.

SB 127 seeks to provide the government and the Internet service provider industry the legal tools needed to better protect consumers from Internet spyware, computer programs that are unknowingly or deceptively written to an Internet user's computer. They often transfer information from a user's computer to another system on the Internet. Some spyware programs simply track the Internet usage of a user, while others go as far as stealing data, including private personal identifying information from the computer and sending it across the Internet without the user's knowledge. It makes it a felony, punishable by one to three years in prison, to take possession of another's computer, to divert Internet browsers to unauthorized websites, modify settings, collect personally identifiable information through keystroke logging, interfere with downloads, install or uninstall software without authorization, falsify an identity to obtain personal information, or mislead computer users in other ways.

2004:
HB 656 requires a credit card issuer who mails an unsolicited offer to apply for a credit card and receives by mail a completed application that lists a different address than the one on the solicitation to take steps to verify the applicant's valid address before issuing the card.

2003:
HB 213 prohibits the use of a scanning device or reencoder that is used to obtain or record encoded information from the magnetic strip of a payment card to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A reencoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are punishable by one to three years in prison and/or a fine up to $10,000. A second or subsequent offense is punishable by three to ten years in prison and/or a fine up to $50,000. Violators can also be ordered to make restitution to any consumer or business victim.

2002:
SB 475 increases penalties for identity theft, making it a felony, punishable by up to ten years in prison, to steal and use someone's identification. Previously, it was illegal to manufacture and sell false identification documents. The new law outlaws the possession and use of false documents as well. Simple possession of a false document is still a misdemeanor, as is the first offense of making or distributing false identification. Under the law, a second offense is a felony punishable by fines and imprisonment for at least a year. In addition, the law requires businesses that maintain confidential data about customers to ensure that it is destroyed or rendered unusable before it is discarded.