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

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

TENNESSEE
IDENTITY THEFT RANKING BY STATE: Rank 24, 64.7 Complaints Per 100,000 Population, 3986 Complaints (2007)
Updated January 11, 2009

Current Laws:
Identity Theft: A person commits the offense of identity theft if he knowingly obtains, possesses, buys, or uses the personal identifying information of another, with the intent to commit any unlawful act, including but not limited to, obtaining or attempting to obtain credit, goods, services, or medical information in the name of the other person, without his/her consent or without the lawful authority to obtain, possess, buy or use that identifying information.

A person commits the offense of identity theft trafficking if he knowingly sells, transfers, gives, trades, loans or delivers, or possesses with the intent to sell, transfer, give, trade, loan or deliver, the personal identifying information of another, with the intent that the information will be used by someone else to commit the offense of identity theft, as defined above. If the defendant simultaneously possesses the personal identifying information of five or more different individuals, it may be inferred that he had intent to traffic in the information.

Personal identifying information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including:

- Name, Social Security number, date of birth, official state or government issued driver license or identification number, alien registration number, passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, routing code or other personal identifying data which enables an individual to obtain merchandise or service or to otherwise financially encumber the legitimate possessor of the identifying data; or
- Telecommunication identifying information or access device.

Identity theft is a class D felony, punishable by a range of 1.8 years in prison, of which only 20% must be served, to 12 years in prison, of which 60% must be served, depending on the number of prior offenses committed by the defendant, and a fine up to $5000. Trafficking in identity theft is a class C felony, punishable by a range of 2.7 years in jail, of which only 20% must be served, to 15 years in jail, of which 60% must be served, depending on the number of prior offenses committed by the defendant, and a fine of up to $10,000. In addition, a person found guilty will forfeit any lawful claim to the identifying information, property, or other realized benefit of the other person as a result of such violation.
Statute: §39-14-150:
http://www.michie.com/tennessee/lpext.dll/tncode/11662/11bd7/11be1/11ce5?fn=document-

frame.htm&f=templates&2.0#

A person commits the offense of criminal impersonation when he, with intent to injure or defraud another person, assumes a false identity; pretends to be a representative of some person or organization; pretends to be an officer or employee of the government; or pretends to have a handicap or disability. This is a class B misdemeanor, punishable by six months in jail and/or a $500 fine.
Statute: §39-16-301:
http://www.michie.com/tennessee/lpext.dll/tncode/11662/11f41/11f81/11f85?fn=document-frame.htm&f=templates&2.0#

Using false identification for the purpose of obtaining goods, services, or privileges to which the person is not otherwise entitled or eligible is a class C misdemeanor, punishable by 30 days in jail and/or a fine of $50. This does not include violations where a person under 21 uses the false identification to buy alcohol, or a person under 18 uses the identification to purchase tobacco or other item or service that is limited by age.
Statute: §39-16-303:
http://www.michie.com/tennessee/lpext.dll/tncode/11662/11f41/11f81/11f8f?fn=document-frame.htm&f=templates&2.0#

Payment Cards: A person commits the crime of illegal possession of a credit or debit card if he, knowing that he does not have the consent of the owner or issuer, takes, exercises control over or otherwise uses that card or information from that card.

Fraudulent use of a credit or debit card occurs when a person uses or allows to be used a credit or debit card, or the information from that card, for the purpose of obtaining property, credit, services or anything of value with knowledge that the card is forged or stolen; the card has been revoked or cancelled; the card has expired and is used with fraudulent intent; or for any other reason the use of the card is unauthorized by either the issuer or the person to whom the card is issued. It is punishable as theft pursuant to §39-14-105, depending on the amount of property, credit, goods, or services obtained:

- Class A misdemeanor if the value of the property or services obtained is $500 or less (punishable by up to one year in prison and a $2500 fine);
- A Class E felony if the value of the property or services obtained is more than $500 but less than $1,000 (punishable by a range of .9 years in prison, of which 20% must be served, to 6 years in prison, of which 60% must be served, and a fine of up to $3000);
- A Class D felony if the value of the property or services obtained is $1,000 or more but less than $10,000 (punishable by a range of 1.8 years in prison, of which only 20% must be served, to 12 years in prison, of which 60% must be served, and a fine up to $5000);
- A Class C felony if the value of the property or services obtained is $10,000 or more but less than $60,000 (punishable by a range of 2.7 years in jail, of which only 20% must be served, to 15 years in jail, of which 60% must be served, depending on the number of prior offenses committed by the defendant, and a fine of up to $10,000); and
- A Class B felony if the value of the property or services obtained is $60,000 or more (punishable by a range of 7.2 years in jail, of which only 20% must be served, to 30 years in jail, of which 60% must be served, depending on the number of prior offenses committed by

the defendant, and a fine of up to $50,000)
- If no property, credit, goods, or services are actually received or obtained, illegal possession or fraudulent use of a credit card is a Class B misdemeanor.

Statute: §39-14-118:
http://www.michie.com/tennessee/lpext.dll/tncode/11662/11bd7/11be1/11c60?fn=document-frame.htm&f=templates&2.0#

Government-Issued Photo Identification: It is a Class C misdemeanor for any person to:
- Display or possess any cancelled, revoked, suspended, or fraudulently altered government-issued photo identification document;
- Lend a government-issued photo identification document to any other person or knowingly permit the use by another person;
- Permit or commit any unlawful use of a government-issued photo identification document issued to such person;
- Represent as one's own any government-issued photo identification document not issued to such person; or
- Display or possess any unauthorized reproduction of a government-issued photo identification document.

It is also an offense for any person to reproduce a government-issued photo identification document in such a manner that it could be mistaken for a valid license; or unlawfully issue, sell, or cause to be sold a government-issued photo identification document or facsimile thereof.

A violation of the prohibitions against reproducing, issuing, or selling a government-issued photo identification document is a Class A misdemeanor. A second or subsequent violation is a Class E felony, with suspension of driving privileges for a period of one to five years, or for a period of time commensurate with the sentence imposed. A violation in connection with an act of terrorism is a Class B felony, with a permanent and irrevocable suspension of driving privileges.
Statute: §55-50-602:
http://www.michie.com/tennessee/lpext.dll/tncode/1eade/1fd2a/1fe82/1fe8c?fn=document-frame.htm&f=templates&2.0#

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. It prohibits using the Internet, e-mails, or other electronic means, including wireless communication, with the intent to defraud, to:
Obtain, record or access identifying information that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits of such other person;
Obtain goods or services through the use of identifying information of such other person; or
Obtain identification documents in such other person's name.

Internet service providers, Web site owners, or trademark owners can bring a civil action to stop the violations, and to recover the greater of actual damages or $500,000. Victims can sue to recover three times actual damages or $5,000 per violation, whichever is greater. The attorney general or district attorney may also bring an action to stop future violations and to recover a civil penalty of up to $2500 per violation. In addition, a court may triple the damages and award

costs of the suit and reasonable attorney's fees in cases where the defendant has established a pattern and practice of violating the anti-phishing law.

Statute: §47-18-5201 through 05
http://www.michie.com/tennessee/lpext.dll?f=FifLink&t=document-frame.htm&l=jump&iid=23c30640.1f31d1c5.0.0&nid=9a41#JD_t47ch18p52

Social Security Numbers: State law places limits on the use and dissemination of Social Security numbers (SSNs). The law will prohibit the public posting or display of an individual's SSN, and prohibit the SSN from being printed on any materials mailed to a consumer, unless it is required by law or the document is a form or application. The law will also prohibit requiring a person to transmit a SSN over the Internet, unless the Internet connection is secure and the SSN is encrypted. It is also prohibited to require consumers to use their SSNs to log onto or access a Web site, unless it is used in combination with a password or other authentication device. Violations of these provisions will be a Class B misdemeanor after Jan. 1, 2009, allowing for a one-year grace period.
Statute: §47-18-2110:
http://www.michie.com/tennessee/lpext.dll/tncode/17279/1838f/187a9/187e1?fn=document-frame.htm&f=templates&2.0#

Disposal of Records: To prevent identity theft, state law restricts how businesses can dispose of records with personal identifying information about individuals. The law requires businesses to destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business, by shredding, burning, erasing, or otherwise modifying the personal information in the records to make them unreadable. Personal identifying information includes a customer's Social Security number, driver's license number, bank account numbers, complete credit or debit card numbers, PIN numbers or passwords, health insurance identification numbers, or unique biometric data. Violations are punishable by a civil penalty of $500 for each violation, with a maximum penalty of $10,000 for any one customer.
Statute: §39-14-150:
http://www.michie.com/tennessee/lpext.dll/tncode/11662/11bd7/11be1/11ce5?fn=document-frame.htm&f=templates&2.0#

Victim Assistance:

Restitution: The court must order restitution be made to the person or persons whose identity was stolen for any identifiable losses resulting from the offense.
Statute: §39-14-150:
http://www.michie.com/tennessee/lpext.dll/tncode/11662/11bd7/11be1/11ce5?fn=document-frame.htm&f=templates&2.0#

Identity Theft Passport: The Office of the Attorney General may issue an identity theft passport to a person who is a victim of identity theft. Victims may present the passport to a law enforcement agency, for the purpose of preventing arrest or detention for an offense committed by someone other than the victim using the victim's identity; or to any of the victim's creditors,

for the purpose of assisting in that creditor's investigation and establishment of whether fraudulent charges were made against accounts in the victim's name or whether accounts were opened using the victim's identity. The passport may also be presented to a consumer reporting agency, which must accept the passport as an official notice of a dispute and must include notice of the dispute in all future reports that contain disputed information caused by the identity theft. A law enforcement or creditor has discretion on whether to accept or reject the passport.

A person who has filed a police report alleging identity theft may apply for an identity theft passport through any law enforcement agency. The agency will send a copy of the application and the supporting police report to the Office of the Attorney General. After processing the application and police report, the office of the attorney general and reporter may issue to the victim an identity theft passport in the form of a card or certificate.

Acceptance or rejection of an identity theft passport is at the discretion of the law enforcement agency or creditor. In making a decision regarding acceptance or rejection, a law enforcement agency or creditor may consider the surrounding circumstances and available information regarding the offense of identity theft alleged by the victim.
Legislation: http://www.capitol.tn.gov/legislation/Archives/105GA/bills/BillText/SB0161.pdf

Security Freeze: Consumers are allowed 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 obtain a freeze, a consumer must request one in writing by certified mail or, beginning on January 31, 2009, through electronic means, to the credit reporting agencies. The agencies may charge up to $7.50 to place the freeze, but there is no charge for temporarily unlocking the freeze. However, there is no charge for victims of identity theft who present a police report or other official document detailing the theft.

The reporting agency must place the freeze within three business days after receiving the request, and within ten 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 fifteen minutes, currently the shortest time period in any state.
Statute: §47-18-2108:
http://www.michie.com/tennessee/lpext.dll/tncode/16db6/17e98/1829c/182cf?fn=document-frame.htm&f=templates&2.0#

Security Breach: State law requires state and local government agencies and businesses operating in the state that that own or license computerized data that includes personal information 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 "unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder." Personal identifying information includes an individual's first name or first initial and

last name in combination with one or more of the following unencrypted data elements: Social Security number, driver's license number, or bank, credit or debit card number in combination with any required access code. Publicly available information is not included.
Disclosure must occur to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an authorized person. The disclosure must be made in the most expedient time possible, and without unreasonable delay, consistent with legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Notification can be provided to the affected persons by mail or e-mail. If the cost of providing regular notice would exceed $250,000, the amount of people to be notified exceeds 500,000, or the entity or business not have sufficient contact information, 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 entity's web site, and notification to major statewide media. The consumer reporting agencies must also be notified when the breach is disclosed to more than 1,000 people at a time.
Statute: §47-18-2107:
http://www.michie.com/tennessee/lpext.dll/tncode/17279/1838f/187a9/187d2?fn=document-frame.htm&f=templates&2.0#

Civil Suits: Victims of identity theft may bring a civil action against the perpetrator to recover three times the actual damages. The action may be brought in the county where the identity theft took place, or in the county in which the person resides or has his principal place of business.
Statute: §47-18-2104:
http://www.michie.com/tennessee/lpext.dll/tncode/17279/1838f/187a9/187c3?fn=document-frame.htm&f=templates&2.0#

State Resources:

Tennessee Highway Patrol, "You Are a Victim of Identity Theft: What To Do If It Happens To You" (http://tennessee.gov/safety/cididtheft.htm)
This Web site directs victims of identity theft to: "*Report the crime to the law enforcement agency with jurisdiction in your case. Give them as much documented evidence as possible. Get a copy of your police report. Keep the report number of your police report handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report to verify the crime. Some police departments have been known to resist writing reports on such crimes…Some police departments have not yet received training in the new laws of Identity Theft. Be persistent!"*

Office of the Attorney General, "Identity Theft"
(http://www.attorneygeneral.state.tn.us/cpro/idtheft.htm)

Protecting Yourself from Identity Theft" (http://www.attorneygeneral.state.tn.us/cpro/ptheft.htm)
This site directs victims to: "*File reports of the theft with law enforcement and the Federal Trade Commission. Many creditors will require you to provide them with a police report to document*

the crime. It is important to contact law enforcement as soon as possible and that you be prepared to provide them with any documentation you have of the fraud. The FTC maintains a database of identity theft cases used by law enforcement for investigations. Filing a complaint will help the FTC learn more about identity theft and the problems that victims encounter."

Consumer Affairs Division, "Identity Theft"
(http://tennessee.gov/consumer/documents/IDTheftFlyer_001.pdf)
This document has prevention tips and information for victims.

Legislation:

2008:
SB 2852 amends the state's security freeze law to prohibit a consumer credit reporting agency from making any changes to a person's credit report if a security freeze is in place without sending a written confirmation to the consumer within 30 days.

2007:
Passage of **SB 161** allows Tennessee 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. Consumers may place a freeze, for a fee of up to $7.50 from each credit reporting agency. Applications must be done by mail until January 31, 2009, when online access will begin. A person who needs their credit report temporarily unfrozen, such as to make a major purchase requiring a credit check, can lift the freeze. There is no charge for temporarily unfreezing access or reinstating it, but there can be a levy of up to $5 to permanently lift the freeze. A personal security code, given by the credit bureaus, is necessary for a consumer to unlock their credit report.

In addition, the bill increases protections of Social Security numbers. Businesses and nonprofits will be prohibited from posting SSNs or displaying them in public. They are also forbidden from printing SSNs on mailers unless required by law. The bill also targets the use of Social Security numbers on the Internet. Web sites are banned from requiring SSNs to be used to gain access unless it is in combination with a password and the number is encrypted. Violation of the Social Security provisions of the act will be a Class B misdemeanor after Jan. 1, 2009, allowing a one-year grace period.

The bill also authorizes the attorney general to issue identity theft passports to victims of the crime. The passport can be presented to a law enforcement agency, for the purpose of preventing arrest or detention for an offense committed by someone other than the victim using the victim's identity; or to any of the victim's creditors, for the purpose of assisting in that creditor's investigation and establishment of whether fraudulent charges were made against accounts in the victim's name or whether accounts were opened using the victim's identity. The passport may also be presented to a consumer reporting agency, which must accept the passport as an official notice of a dispute and must include notice of the dispute in all future reports that contain

disputed information caused by the identity theft. A law enforcement or creditor has discretion on whether to accept or reject the passport.

SB 767 extends the laws related to use of a driver license and unlawful reproduction of a driver license, to the use of any certificate of driving or other government-issued photo identification document.

2006:
SB 2575 criminalizes the fraudulent use of the Internet or other electronic means to obtain personal identifying information, a practice known as "phishing."

2005:
SB 2220 requires state and local government agencies and any company that lawfully collects and maintains computerized records containing consumer's personal information to notify affected consumers in the event that personal data is compromised.

2004:
HB 3403 creates the crime of identity theft (a class D felony) and identity theft trafficking (a class C felony). The bill also declares that anyone whose identity is unlawfully obtained is a victim of crime. In addition, the bill requires businesses to destroy records containing a customer's personal information that is no longer needed. Customer records containing private personal information must be shredded, erased, or otherwise modified to make personal information unreadable.