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

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

FLORIDA
IDENTITY THEFT RANKING BY STATE: Rank 5, 105.6 Complaints Per 100,000 Population, 19,270 Complaints (2007)
Updated November 30, 2008

Current Laws: A person commits the offense of fraudulent use of personal identification information if he willfully and without authorization, fraudulently uses or possesses with intent to fraudulently use personal identification information concerning an individual without first obtaining the individual's consent. Violations are a felony of the third degree, punishable by up five years in prison and/or a fine up to $5,000.

The penalty is increased to a second-degree felony, punishable by three to fifteen years in prison and/or a fine up $10,000, if the pecuniary benefit, value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $5,000 or more; or if the person fraudulently uses the personal identification information of ten to nineteen individuals without their consent.

It is a first-degree felony if the pecuniary benefit, value of the services received, the payment sought to be avoided, or the amount of the injury or fraud perpetrated is $50,000 or more; or the person fraudulently uses the personal identification of twenty to twenty nine individuals.
It is punishable by five to thirty years in prison and/or a fine up to $10,000. If the value is over $100,000, or if the person fraudulently uses the personal identification information of thirty or more individuals without their consent, there is a mandatory minimum sentence of ten years in prison.

Any person who willfully and without authorization possesses, uses, or attempts to use personal identification information concerning an individual without first obtaining that individual's consent, and who does so for the purpose of harassing that individual, commits the offense of harassment by use of personal identification information, which is a misdemeanor of the first degree, punishable up to one year in prison and/or a fine up to $1,000.

If an offense was facilitated or furthered by the use of a public record, it is reclassified to the next higher degree as follows: a misdemeanor of the first degree is reclassified as a third-degree felony; a third-degree felony becomes a second-degree felony, and a second-degree felony is reclassified as a first-degree felony.

A person who willfully and without authorization fraudulently uses personal identification information concerning an individual under 18 years of age without first obtaining the consent o the individual or his legal guardian commits a second-degree felony. If a parent or legal guardian uses the personal identification of the minor, it is also a second-degree felony.

Fraudulent use or possession with intent to use personal information of a deceased individual is third-degree felony. If the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of injury or fraud perpetrated is $5,000 or more, or if the person fraudulently uses the personal identification information of 10 or more but fewer than 20 deceased individuals, it is second-degree felony, with a mandatory minimum sentence of three years.

A person commits the offense of aggravated fraudulent use of the personal identification information of multiple deceased individuals, a first-degree felony, if the pecuniary benefit, the value of the services received, the payment sought to be avoided, or the amount of injury or fraud perpetrated is $50,000 or more; or if the person fraudulently uses the personal identification information of 20 to 29 deceased individuals. If the value is over $100,000 or more or if the person fraudulently uses the personal identification information of 30 or more deceased individuals, the minimum sentence is 10 years.

Any person who willfully and fraudulently creates or uses, or possesses with intent to fraudulently use, counterfeit or fictitious personal identification information concerning a fictitious individual, or concerning a real individual without first obtaining that real individual's consent, with intent to use such counterfeit or fictitious personal identification information for the purpose of committing or facilitating the commission of a fraud on another person, commits the offense of fraudulent creation or use, or possession with intent to fraudulently use, counterfeit or fictitious personal identification information, a third-degree felony.

If a person commits any of the above offenses and for the purpose of obtaining or using personal identification information, misrepresents himself or herself to be a law enforcement officer; an employee or representative of a bank, credit card company, credit counseling company, or credit reporting agency; or any person who wrongfully represents that he or she is seeking to assist the victim with a problem with the victim's credit history, the offense will be reclassified as follows: In the case of a misdemeanor, the offense is reclassified as a felony of the third degree; in the case of a felony of the third degree, the offense is reclassified as a felony of the second degree; in the case of a felony of the second degree, the offense is reclassified as a felony of the first degree; a felony of the first degree may be reclassified as a life felony.

A prosecutor may ask for a reduced or suspend sentence for a person convicted of an identity theft violation if he provides substantial assistance in the identification, arrest, or conviction of his accomplices, accessories, co-conspirators, or principals or any other person engaged in fraudulent possession or use of personal identification information.

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

- Name, postal or electronic mail address, telephone number, Social Security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;

- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code;
- Medical records;
- Telecommunication identifying information or access device; or
- Other number or information that can be used to access a person's financial resources.

Statute: §817.568:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC568.HTM&Title=-%3E2002-%3ECh0817-%3ESection%20568

Jurisdiction: Venue for prosecution and trial may be commenced and maintained in any county in which an element of the offense occurred, including the county where the victim generally resides.
Statute: §817.568:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC568.HTM&Title=-%3E2002-%3ECh0817-%3ESection%20568

Statute of Limitations: A prosecution must be commenced within three years after the offense occurred. However, a prosecution may be commenced within one year after discovery of the offense by an aggrieved party if the prosecution is commenced within five years after the violation occurred.
Statute: §817.568:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC568.HTM&Title=-%3E2002-%3ECh0817-%3ESection%20568

Payment Cards: It is unlawful for a person to make or cause to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false and with intent that it be relied on respecting his or her identity or that of any other person, firm, or corporation or his or her financial condition or that of any other person, firm, or corporation, for the purpose of procuring the issuance of a credit card. Violations are a first-degree misdemeanor.
Statute: §817.59:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC59.HTM&Title=-%3E2006-%3ECh0817-%3ESection%2059#0817.59

It is a first-degree misdemeanor to:
- Take a credit card from the person, possession, custody, or control of another without the cardholder's consent; or with knowledge that it has been so taken, receives the card with intent to use, sell, or transfer it to another person.
- Receive a credit card that a person knows to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder, and retain possession with intent to use, sell, or transfer it.
- For a person other than the issuer to sell a credit card; or to buy a credit card from a person other than issuer.

- For a person other than the cardholder or a person authorized by him, to sign a credit card with the intent to defraud the issuer or a person or organization providing money, goods, services, or anything else of value or any other person.

It is a third-degree felony for a person, other than the issuer, to receive during any 12-month period two or more credit cards in the name or names of different cardholders that he has reason to know were taken or retained under circumstances that constitute credit card theft.
Statute: §817.60:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC60.HTM&Title=-%3E2006-%3ECh0817-%3ESection%2060#0817.60

A person commits the crime of fraudulent use of a credit card if he, with intent to defraud the issuer or 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 credit card obtained or retained fraudulently or any credit card that he knows is forged; or to represent himself, without consent of the cardholder, that he is the holder of a specified card. Violations are a first-degree misdemeanor if in any six-month period, a person uses a credit card in violation two or fewer times, or obtains money, goods, services, or anything else in violation the value of which is less than $100. It is a third-degree misdemeanor if he uses a card more than two times or obtains goods valued over $100.
Statute: §817.61:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC61.HTM&Title=-%3E2006-%3ECh0817-%3ESection%2061#0817.61

Scanning Devices: State law prohibits the use of a scanning device or re-encoder that is used to obtain or record encoded information from the magnetic strip of a payment card without the authorization of the authorized user and with the intent 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 re-encoder 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 a third-degree felony. Second or subsequent offenses are a second-degree felony.
Statute: §817.625:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC625.HTM&Title=-%3E2006-%3ECh0817-%3ESection%20625#0817.625

Caller Identification Fraud: Under state law, a caller may not knowingly insert false information into a caller identification system with the intent to mislead, defraud or deceive the recipient of a telephone call. A caller identification system means a listing of a caller's name, telephone number, or name and telephone number that is shown to a recipient of a call when the recipient answers. This provision does not apply to any blocking of caller identification information; any law enforcement agency, or any intelligence or security agencies of the federal government. Violations are a misdemeanor in the first degree.

Text of Legislation: http://www.flsenate.gov/cgi-bin/view_page.pl?Tab=session&Submenu=1&FT=D&File=hb022502er.html&Directory=session/2008/House/bills/billtext/html/

Victim Assistance:

Restitution: A court may order a defendant convicted of an identity theft offense to make restitution to any victim of the offense. In addition to the victim's out-of-pocket costs, restitution may include payment of any other costs, including attorney's fees incurred by the victim in clearing the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as the result of the actions of the defendant.
Statute: §817.568:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC568.HTM&Title=-%3E2002-%3ECh0817-%3ESection%20568

Court Orders: Upon conviction of an identity theft offense, the court may issue such orders as necessary to correct any public record that contains false information resulting from the actions that resulted in the conviction.
Statute: §817.568:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC568.HTM&Title=-%3E2002-%3ECh0817-%3ESection%20568

Security Freeze: All Florida 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 $10 to place or temporarily lift a security freeze. However, victims of identity theft with a valid police report or investigative complaint and people 65 years of age or older may not be charged.

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. A consumer reporting agency must select and develop a secure electronic contact method, which may include the use of telephone, fax, the Internet, or other secure electronic means, by which to receive and process requests from consumers to temporarily lift a freeze.
Statute: 501.005:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0501/SEC005.HTM&Title=-%3E2006-%3ECh0501-%3ESection%20005#0501.005

How to Place a Credit Freeze in Florida:
http://www.consumersunion.org/pdf/security/securityFL.pdf

Credit Report Security Freezes: http://www.800helpfla.com/scams/securityfreeze.html

Security Breach: State law requires individuals and businesses doing business in the state to notify state residents when their unencrypted personal information was or is reasonably believed to have been acquired during a security breach, putting them at risk of identity theft. A security breach is defined as "unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information."

Notice must be made without unreasonable delay, no later than 45 days following the determination of the breach, although it can be delayed upon request by a law enforcement agency or to determine the scope of the breach and to restore the reasonable integrity of the data system. Notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for five years.

Personal information is defined as an individual's first name or first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements, when the data elements are not encrypted: Social Security number; driver's license number or Florida Identification Card number; or an account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. It does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Notification can be provided 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 business 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 business's web site, and notification to major statewide media. When a breach involves more than 1,000 people, the business must also notify the consumer reporting agencies.
Statute: §817.5681:
http://www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0817/SEC5681.HTM&Title=-%3E2006-%3ECh0817-%3ESection%205681#0817.5681

State Resources:

Office of the Attorney General, "Identity Theft" (http://myfloridalegal.com/identitytheft)

"ID Theft Victim Kit" (http://myfloridalegal.com/idkitprintable.pdf)
This comprehensive document includes checklists for victims of identity theft. It directs victims to: "*Report the incident to law enforcement. Contact your local police department or sheriffs office to file a report. Under Florida law, the report may be filed in the location in which the offense occurred, or, the city or county in which you reside. When you file the report, provide as*

much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit. Request a copy of the police report. Some creditors will request to see the report to remove the debts created by the identity thief."

"Identity Crime Incident Detail Form"(http://myfloridalegal.com/idform.pdf)
"*Please fill out this form and return it to the Police Department as soon as possible, or bring it to the meeting with the detective assigned to your case. The information you provide will be used to understand what occurred, organize the investigative case, determine where evidence might be found, develop a theory of how the identity crime occurred, and determine what financial institutions should be contacted in the course of the investigation."*

"Chart Your Course of Action" Form (http://myfloridalegal.com/courseofaction.pdf)
Victims can use this form to record the steps they have taken to report the fraudulent use of their identity.

"Working With Law Enforcement"
(http://myfloridalegal.com/pages.nsf/Main/E248B44F8E20DCCE85256DBB0045CDA2?OpenDocument)
"If you are a victim of identity theft you should contact your local police department or sheriff's office first to file a report. Under Florida's identity theft law, the report may be filed in the location in which the offense occurred, or, the county in which you reside. It is important to remember to get a copy of the police report. Very often, the bank, credit card company, or others need proof of the crime in order to erase the debts created by the identity thief. If you can't get a copy of the report, at least get the report number."

The site also provides tips on filing a police report, including: "***Provide documentation.*** *Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, your notarized ID Theft Affidavit, and other evidence of fraudulent activity can help the police file a complete report.* ***Be persistent.*** *Local authorities may tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Also remind them that under their voluntary "Police Report Initiative," 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.* ***Be a motivating force.*** *Ask law enforcement to search the FTC's Consumer Sentinel ID Theft database for other complaints in your community. You may not be the first or only victim of this identity thief. If there is a pattern of cases, local authorities may give your case more consideration*."

"About Identity Theft Crimes"
(http://myfloridalegal.com/pages.nsf/Main/932BC47213C29D3385256DBB0048479D?OpenDocument)

"Preventing Identity Theft"
(http://myfloridalegal.com/pages.nsf/Main/D859138D3EB2051D85256DBA007188A5?OpenDocument)

Florida Department of Law Enforcement, "Identity Theft"
(http://www.fdle.state.fl.us/Fc3/idtheft.html)

"Identity Theft: The Long Road to Resolution"
(http://www.fdle.state.fl.us/Publications/Identity_Theft.pdf)
This comprehensive document provides an overview of the steps required to restore your identity after a theft.

"Compromised Identity Services" (http://www.fdle.state.fl.us/CompID/)
This site provides information for people who are concerned that their personal identifiers may have been used in an arrest record. It explains that such victims can request a public records check or initiate a compromised identity claim. The claim is only for individuals who believe they are victims of identity theft and/or have had their personal identification information stolen or misused and believe their information may have been used in a Florida criminal history file. Based on a fingerprint comparison of state criminal history files, it can determine what, if any, criminal history belongs to a victim, and if any arrest records have been falsely associated with him/her as a result of someone using his/her identity. If a fingerprint check determines a person is an identity theft victim, FDLE will work with local law enforcement agencies to attempt to clear fraudulent data from the criminal history files and provide the victim with a Compromised Identity Certificate.

- Request a public records check (http://www.fdle.state.fl.us/CriminalHistory/)
- Compromised Identity Review Claim Form (http://www.fdle.state.fl.us/CompID/claim_form.pdf)

Florida Department of Agriculture and Consumer Affairs, "Identity Theft: Don't Be Left in the Dark" (http://www.800helpfla.com/identity.html)

"Phishing: Don't Take the Bait" (http://www.800helpfla.com/scams/phishing.html)

Department of Highway Safety and Motor Vehicles, "Identity Theft Information"
(http://www.hsmv.state.fl.us/IDtheft.html)

"Identity Theft Report Form" (http://www.hsmv.state.fl.us/72068.pdf)
This form is used to report driver license fraud or identity theft.

Legislation:

2008:
HB 225 targets the practice of caller ID spoofing, a phone scam that allows a caller to hide his or her true identity by modifying caller ID information with the intent to mislead, defraud or deceive the recipient of the telephone call. The bill makes it a first-degree misdemeanor for a caller to knowingly insert false information into a caller identification system with the intent to mislead, defraud or deceive the recipient of a telephone call.

2006:
HB 37 allows Florida consumers to put a security freeze on their credit files to prevent identity thieves from opening new credit accounts in their names. A security freeze enables a consumer to prevent anyone from looking at his or her own credit reporting file for purposes of granting credit unless the consumer chooses to let that particular business look at the information. This gives consumers control over who has access to their information needed to process a credit application and effectively prevents others from opening new accounts in their name. When the consumer is applying for credit, the security freeze can be lifted temporarily so the application can be processed.

2005:
HB 481 broadens the scope of the state's laws regarding criminal use of personal identification information (identity theft). Under the bill, any person who willfully and fraudulently uses, or possesses with intent to use, personal identification information concerning a deceased individual, commits a third degree felony, and imposes three, five, and ten year minimum mandatory sentences depending on the value of the pecuniary benefit or injury or the number of deceased individuals whose personal identification information is used. The bill also creates a third-degree felony offense for willfully and fraudulently creating or using, or possessing with the intent to use, counterfeit or fictitious personal identification information for the purpose of committing a fraud upon another person.

The bill also provides for the reclassification of an identity theft offense committed by a person who misrepresents themselves as a law enforcement officer; employee of a bank, credit card company, credit counseling company, or credit reporting agency; or any person who wrongfully represents that he or she is seeking to assist a victim with a problem with the victim's credit history. This will have the effect of increasing the maximum sentence that can be imposed for these offenses.

The bill also requires a person who conducts business in Florida and maintains personal information in a computerized data system to disclose a breach in the security of the data to any resident of this State subject to certain exceptions. When a disclosure is required, it must be made without unreasonable delay, and no later than forty-five days following the determination that unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person and the acquired information materially compromises the security, confidentiality, or integrity of personal information. Any person who fails to make the required disclosure is subject to an administrative fine.

2003:
SB 1072 elevates certain identity theft crimes to a second-degree felony punishable by a maximum of 15 years in prison. The mandatory minimum sentence is 3 years in prison. This penalty applies if the fraud is valued at $5000 or more or if the person fraudulently uses the information of 10 or more people. If the amount is $50,000 or more or if the identification information of 20 or more people, the mandatory minimum is five years. If the identity fraud adds up to more than $100,000, or if the person uses the personal information of 30 or more individuals, it will be a first-degree felony carrying a 30-year maximum prison sentence, with a minimum sentence of 10 years.

2001:
HB 1845 creates the criminal offense of identity theft and categorizes it as a second-degree felony if $75,000 worth of services or more is stolen with another person's identity. In addition, the law provides for increased penalties when an offender unlawfully uses public record information to commit an identity theft crime.

SB 1282 makes it a felony to use a scanning device or re-encoder to obtain or record encoded information from the magnetic strip of a payment card without the authorization of the authorized user and with the intent 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 re-encoder 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 a third-degree felony. Second or subsequent offenses are a second-degree felony.