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

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

LOUISIANA
IDENTITY THEFT RANKING BY STATE: Rank 28, 62.3 Complaints Per 100,000 Population, 2674 Complaints (2007)
Updated December 15, 2008

Current Laws: Identity theft is the intentional use or possession or transfer or attempted use with fraudulent intent by any person of any personal identifying information of another person to obtain, possess, or transfer, whether contemporaneously or not, credit, money, goods, services, or any thing else of value without the authorization or consent of the other person. These provisions do not apply to a person who obtains another person's driver's license or other form of identification solely for the purpose of misrepresenting his age. "Personal identifying information" includes but is not limited to an individual's: Social Security number, driver's license number, checking or savings account number, credit or debit card number, electronic identification number, digital signatures, birth certificate, date of birth, mother's maiden name, armed forces identification number, government issued identification number, or financial institution account number.

Identity theft penalties vary and are tied to the resulting loss involved. Penalties are increased for identity theft crimes against people 60 or older, 17 or under, and against the disabled, which is defined as a person who has a mental, physical, or developmental disability that substantially impairs the person's ability to provide adequately for his own care or protection. Multiple thefts may be aggregated to determine the grade of the offense.

Value of Theft	Maximum Penalty –Term of Imprisonment / Fine
$299 or less	6 months/$500
If victim 60 or older, 17 or under, or disabled	1 year / $500 Minimum sentence of 6 months
$300-$499	3 years/$3,000
If victim 60 or older, 17 or under, or disabled	Minimum sentence of 1 year
$500-$999	5 years/$5,000
If victim 60 or older, 17 or under, or disabled	Minimum sentence of 2 years
$1,000 or more	10 years/$10,000
If victim 60 or older, 17 or under, or disabled	Minimum sentence of 3 years

Upon a third or subsequent conviction of any of these provisions, the offender shall be imprisoned, with or without hard labor, for up to ten years, and/or fined up to $20,000.
Statute: §14.67-16: http://www.legis.state.la.us/lss/lss.asp?doc=78613

Jurisdiction: Identity theft can be prosecuted in either in the parish where the theft occurred or the parish where the victim resides.
CCRP 611: http://www.legis.state.la.us/lss/lss.asp?doc=112644

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 engage in conduct involving the fraudulent use or possession of another person's identifying information, from:

- Creating a Web page or Internet domain name that is represented as a legitimate online business without the authorization of the registered owner of the business.
- Using that Web page or a link to the Web page, that domain name, or another site on the Internet to induce, request, or solicit another person to provide identifying information for a purpose that the other person believes is legitimate.
- Sending or causing to be sent an electronic mail message that is falsely represented as being sent by a legitimate online business; refers or links the recipient of the message to a Web page that is represented as being associated with the legitimate online business; and directly or indirectly induces, requests, or solicits the recipient of the electronic mail message to provide identifying information for a purpose that the recipient believes is legitimate.

Victims can sue to recover three times actual damages or $5,000 per violation, whichever is greater. State law also allows Internet providers, legitimate Web page or trademark owners and the attorney general to file civil suits against violators. The penalties include restraining orders to stop the violator and would allow those damaged by the violations to recover either actual damages or $100,000 for each violation, whichever is more, plus reasonable attorney fees and court costs. A court can increase the award on actual damages to not more than three times the actual damage if the court finds the violations establish a pattern.
Statute: § R.S. 51:2021 through 2024: http://www.legis.state.la.us/lss/lss.asp?doc=411253 (must forward through to the other sections)

Access Cards: An access code includes any card, plate, account number, paper book, or any other device, issued to a person that authorizes the person to obtain credit, money, goods, services, or anything of value. It is considered theft for a person to directly or indirectly, with intent to defraud, to gain credit, money, goods, services, or anything else of value by:

- Using a forged or revoked access card;
- Making reference by number or other description to a nonexistent access card;
- Stealing or wrongfully appropriating an access card;
- Using an access card belonging to another person without authority

Violations are punishable based on the value of the misappropriation. Multiple thefts in a consecutive 90-day period may be aggregated. If the value is $500 or more, it is punishable by up to ten years in prison and/or a fine up to $5000; if $300 to $499, three years in prison and/or a fine up to $3000; and if under $300, up to six months in prison and/or a fine up to $1000. Upon a third or subsequent conviction of any of these provisions, the offender shall be imprisoned, with or without hard labor, for up to ten years, and/or fined up to $10,000.

Statute: §14:67.3: http://www.legis.state.la.us/lss/lss.asp?doc=78620

No person shall make or cause to be made, either directly or indirectly, any false statement as to his identity or that of any other person or entity for the purpose of procuring the issuance of a credit card. Violators will be guilty of fraudulent acquisition of a credit card and punished by up to ten years in prison and/or a fine up to $3000. Upon a third or subsequent conviction, the punishment increases to up to ten years in prison and/or a fine of up to $20,000. In addition, offenders must pay restitution to victims.
Statute: §14:67.22: http://www.legis.state.la.us/lss/lss.asp?doc=206243

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 without permission of the cardholder to defraud the authorized cardholder, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or 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 credit card. A reencoder is an electronic device that places encoded information from the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different card. Violations are punishable by up to five years in prison and/or a fine up to $5,000. If a person uses both a scanning device and a re-encoder with the intent to defraud will be punished by up to ten years in prison and/or a fine up to $10,000. Upon a third or subsequent conviction, the offender shall be imprisoned, with or without hard labor, for up to ten years, and/or fined up to $20,000.
Statute: §14:67.4: http://www.legis.state.la.us/lss/lss.asp?doc=78621

Victim Assistance:

Restitution: People convicted of crimes under the identity theft statutes must be ordered to make full restitution to the victim and any other person who has suffered a financial loss as a result of the offense. If a person ordered to make restitution is found to be indigent and therefore unable to make restitution in full at the time of conviction, the court must order a periodic payment plan consistent with the person's financial ability.
Statute: §14.67-16(E): http://www.legis.state.la.us/lss/lss.asp?doc=78613

Mandatory Police Reports: Any person who has learned or reasonably suspects that his personal identifying information has been unlawfully used by another may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over the area of his residence. The agency must take a police report of the matter from the victim, provide the complainant with a copy of the report, and begin an investigation of the facts. If the crime was committed in a different jurisdiction, the agency preparing the report should refer the matter, with a copy of the report, to the local law enforcement agency having jurisdiction over the area in which the alleged crime was committed for an investigation of the facts. State law also requires the law enforcement officer who investigates an alleged identity theft violation to make a written report of the investigation that includes the name of the victim; the name of the suspect, if known; the type of personal identifying information obtained, possessed, transferred, or used in violation of the identity theft laws; and the results of the investigation. This information can be provided to the victim, upon his request.

Statute: §14.67-16(G): http://www.legis.state.la.us/lss/lss.asp?doc=78613

Release of Offender Information: State law allows a victim of a crime of identity theft or fraud to obtain the identity of an alleged offender who is arrested for the crime. The victim must request in writing that the arresting law enforcement agency release the identity of the alleged offender to that person, and submit a form provided by the arresting agency.
Statute: §14.72.3:
http://www.legis.state.la.us/lss_doc/lss_house/RS%5C14%5CDoc%20206255.html

The law also requires creditors who grant credit to an identity thief to give victims all the information they need to undo the effects of the theft. This includes both application and transactional information.
Statute: §9.3568(B): http://www.legis.state.la.us/lss/lss.asp?doc=107686

Security Freeze: All Louisiana 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 a security freeze, and up to $8 to temporarily lift a freeze. However, victims of identity theft with a valid police report and people aged 62 or older may not be charged.

The reporting agency must place the freeze within ten business days after receiving the request, and within ten business days, must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time. Requests for a temporary unlocking of the freeze must be completed within three business days.
Statute: §9.3571(H) to (Y): http://www.legis.state.la.us/lss/lss.asp?doc=107688

Security Breach: State law requires any person or business that conducts business in the state and state and local government agencies that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system concerning the data to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A security breach occurs upon "the compromise of the security, confidentiality or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person."

Personal information means an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: Social Security number; driver's license; 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 the individual's financial account. Publicly available information is not included.

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. Notification is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers. 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 agency or business does 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 business's or agency's web site, and notification to major statewide media.
Statute: § R.S. 51:3071 through 3077: http://www.legis.state.la.us/lss/lss.asp?doc=322027 (must forward through the various sections).

Security Alerts: A consumer may place a security alert on their credit reports, signifying the fact that his identity may have been used without his consent to fraudulently obtain goods or services in the his name. The alert requires potential creditors to take reasonable steps to verify the consumer's identity, including contacting the consumer at a specified phone number, before extending credit. The credit reporting agency must comply within five business days of receiving a consumer's request to place a security alert, and must show it to those who request a consumer's credit report for 90 days. It can be extended for additional periods upon request. Creditors or credit reporting agencies who violate these provisions are liable to the identity theft victim for all document out-of-the-pocket expenses suffered by the victim as a result of the identity theft, plus reasonable attorney fees.
Statute: §9.3571.1: http://www.legis.state.la.us/lss/lss.asp?doc=107688
Statute: §9.3568: http://www.legis.state.la.us/lss/lss.asp?doc=107686

State Resources:

Office of the Attorney General: "Identity Theft"
(http://www.ag.state.la.us/Shared/ViewDoc.aspx?Type=3&Doc=80)

Homeland Security Emergency Preparedness, "How Not To Get Hooked by a Phishing Scam"
(http://ohsep.louisiana.gov/cybersecurity/phishingscams.htm)

"Security Freeze" (http://ag.state.la.us/Shared/ViewDoc.aspx?Type=2&Doc=113)

Legislation:

2008:
HB 1126 broadens the definition of a "disabled person" in the identity theft statute by removing the requirement that the disabled person be at least 18 years old.

HB 654 places stricter penalties on repeat identity theft offenders and requires them to make restitution to victims. A third or subsequent conviction of identity theft results in an automatic felony, regardless of the amount stolen. Upon a third or subsequent conviction, offenders will be sentenced to up to ten years in prison and/or a fine up to $20,000.

HB 751 amends the state racketeering statute to include identity theft.

HB 137 makes it illegal for a person to knowingly produce or possess fraudulent documents for identification purposes.

2007:
HB 460 adds enhanced penalties for identity theft crimes against people 17 or younger. There are currently enhanced penalties for people 60 or older and those who are disabled. The bill also increases the maximum minimum sentences for these crimes. If the value of the theft is over $1000, the offender would receive a minimum sentence of three years. If the theft were between $500 and $999, the minimum mandatory sentence would be two years in prison. If the theft were between $300 and $499, the minimum sentence would be one year.

2006:
HB 220 provides that the venue for identity theft can be either the parish where the theft occurred or the parish where the victim resides.

HB 798 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 sending state residents e-mail that looks like it is from a legitimate business but is not. The e-mail cannot legally refer or link to a Web page that misrepresents itself as a legitimate business, or directly or indirectly solicit the e-mail recipient to provide identifying information. Under the bill, victims can sue to recover three times actual damages or $5,000 per violation, whichever is greater.

HB 410 expands the definition of identity theft to include the possession or transfer of personal identifying information. The law previously prohibited the use or attempted use of such information. It also adds a government issued identification number and a financial institution account number to the types of personal identifying information covered under the identity theft statutes.

HB 1335 increases the penalties for the crime of identity theft against the disabled or people 60 years of age or older. A disabled person is defined as a person 18 years of age or older who has a mental, physical, or developmental disability that substantially impairs the person's ability to provide adequately for his own care or protection. It establishes minimum mandatory sentences

for all levels of identity theft. For example, if the value of the theft were over $1000, the offender would receive a minimum sentence of two years. If the theft were between $500 and $999, the minimum mandatory sentence would be one year in prison. If the theft were between $300 and $499, the minimum sentence would be six months.

2005:

SB 205 requires companies and government agencies to notify consumers if a security breach puts sensitive personal information at risk of identity theft. The notification requirement covers unencrypted computerized personal data, including Social Security numbers and numbers for driver licenses, birth dates, credit cards numbers and other financial accounts. The notification must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

SB 156 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 without permission of the cardholder to defraud the authorized cardholder, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or 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 credit card. A reencoder is an electronic device that places encoded information from the magnetic strip or stripe of a credit card onto the magnetic strip or stripe of a different card. Violations are punishable by up to five years in prison and/or a fine up to $5,000. If a person uses both a scanning device and a re-encoder with the intent to defraud will be punished by up to ten years in prison and/or a fine up to $10,000.

2004:

Under **HB 623**, consumers in Louisiana will have the right 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.

To obtain a freeze, a consumer must send a certified letter to the three credit reporting agencies, and pay a $10 fee to each of them. However, the fee is waived if a consumer is a victim of identity theft and has included a copy of the police report with the letter, or is 62 years or older. Once the credit reporting agencies receive a request for a security freeze, they must put in place the security freeze in 10 business days. The reporting agency must also provide, within 10 business days, a unique personal identification number or password that the account holder would use to authorize access of the credit report for a specific period of time. There is a charge of $8 to temporarily lift the freeze each time. The credit reporting agency has three business days to honor the request.

2003:

HB 973 seeks to aid consumers who are victims of identity theft. The bill makes several changes, including:

- Victims of identity theft will now be able to file reports with police departments where they live to better establish their own identity in dealing with credit agencies and others.
- Creditors who grant credit as a result of information that was obtained through identity theft will be required to make available to the victim any and all information in the possession of the creditor that the victim needs to undo the effects of the identity theft.
- Victims will be allowed to place security alerts on their credit, requiring credit firms to contact them before issuing any new credit.
- Creditors, credit reporting agencies and others who violate the law would be liable for expenses by those whose identity was stolen, plus attorney fees.

HB 111 allows a victim of a crime of identity theft or fraud to obtain the identity of an alleged offender who is arrested for the crime.