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

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

OKLAHOMA
IDENTITY THEFT RANKING BY STATE: Rank 25, 63.9 Complaints Per 100,000 Population, 2312 Complaints (2007)
Updated January 10, 2009

Current Laws: It is unlawful for any person to "willfully and with fraudulent intent" obtain certain personal identifying information about another with the intent to obtain or attempt to obtain money, credit, goods, property, or service in the name of the other person without his/her consent. This identifying information includes: the name, address, social security number, date of birth, place of business or employment, debit, credit or account numbers, driver license number, or any other personal identifying information of another person, living or dead.

State law also prohibits a person from willfully creating, modifying, altering, or changing any personal identifying information of another person with fraudulent intent to obtain any money, credit, goods, property, service or any benefit or thing of value, or to control, use, waste, hinder or encumber another person's credit, accounts, goods, property, title, interests, benefits or entitlements without the consent of that person. Identity theft is a felony offense punishable by one to five years in prison and/or a fine of up to $100,000.
Statute: §21:1533.1:
http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=439306

Phishing: State law prohibits phishing, a form of identity theft when someone sends an e-mail that looks official but is used to trick the recipient into giving away personal information that can be used to access a person's financial accounts or obtain goods and services. The law prohibits a person from knowingly sending e-mails that falsely represent another legitimate business and prohibits linking or sending the e-mail recipient to a false Web page in order to collect identifying information. It is also unlawful to obtain identifying information from the e-mail recipient, directly or indirectly, for activities the recipient thinks is valid.

State law allows Internet providers and legitimate Web page or trademark owners to file civil actions against violators. The penalties include injunctive relief to stop the violator and allows 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: §15.776.8 through 776.12:
http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=446389 (must use the "Next Section" link on the red menu bar at the top of the page to move through the five sections)
Statute: §15.776.1: http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=104277

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, punishable by up to one year in county jail and/or a fine up to $10,000.
Statute: §15.776.20 through 776.23:
http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=449670
(must use the "Next Section" link on the red menu bar at the top of the page to move through the four sections)

Payment Cards: It is a misdemeanor for a person to knowingly use or attempt to use a credit or debit card that has not been issued to him/her or which is not used with the consent of the person to whom the card has been issued to obtain credit; purchase goods, property, or services; for the purpose of obtaining cash advances; or to deposit, obtain, or transfer funds. Violations are punishable by up to thirty days in jail and/or a fine up to $500, if the amount of the credit or purchase or funds deposited, obtained, or transferred is under $500. If it is over $500, it is punishable by up to one year in jail and/or a fine up to $1000.
Statute: §21:550.2: http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=69952

It is illegal for any person to try to obtain credit or purchase goods, property or services, cash advances, or obtain or transfer funds by knowingly using or attempting to use in person, by telephone, or by the Internet, a credit or debit card that has not been issued to him, is used without consent of the owner, or is false, counterfeit, or nonexistent. If the amount of credit, purchase, or funds obtained transferred is under $500, it is a misdemeanor punishable by up to one year in jail and/or a fine up to $1000. If the amount is over $500, it is a felony punishable by up to five years in prison and/or a fine up to $5000.
Statute: §21.1550.2:
http://www.oscn.net/applications/OCISWeb/DeliverDocument.asp?CiteID=69952

Financial Institutions: It is a felony, punishable by up to ten years in prison, for any person to obtain or attempt to obtain another person's personal, financial, or other information of a financial institution by means of a false or fraudulent statement made to an employee of the institution, or to present false or fraudulent information to obtain information or commit a crime.
Statute: §21-1533.2:
http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=439318

Victim Assistance:

Mandatory Police Reports: Even if the jurisdiction may lie elsewhere for investigation and prosecution of a crime of identity theft, victims of identity theft have the right to contact the local law enforcement agency where the victim resides and have an incident report about the identity theft prepared and filed. The local law enforcement agency that prepares and files the incident report must, upon request, provide the victim with a copy of the incident report. The law

enforcement agency may share the incident report with law enforcement agencies located in other jurisdictions. An incident report prepared and filed pursuant to this section shall not be an open case for purposes of compiling open case statistics.
Statute: §1533.3:
http://www.oscn.net/applications/oscn/deliverdocument.asp?lookup=Next&listorder=106405&dbCode=STOKST21&year=

Restitution: State law provides that restitution to the victim of identity theft may be ordered in addition to any criminal penalty imposed by the court.
Statute: §21.1533.1:
http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=439306

Civil Suits: Victims may also bring a civil action for damages against any person participating in furthering the crime or attempted crime of identity theft.
Statute: §21.1533.1:
http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=439306

Credit Freeze: All Oklahoma 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 investigative or incident report or complaint with a law enforcement agency about the unlawful use of the victim's identifying information by another person 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 of receipt of the request, 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: §24:149-159:
http://www.oscn.net/applications/OCISWeb/DeliverDocument.asp?CiteID=446738 (must use the "Next Section" link on the red menu bar at the top of the page to move through the eleven sections).
How to Place a Security Freeze: http://www.consumersunion.org/pdf/security/securityOK.pdf

Expungement: Victims may apply for an expungement of their criminal records if the criminal acts were committed by someone who has assumed their identity. Expungement is available for a person who has been charged or arrested or is the subject of an arrest warrant for a crime that was committed by another person who has appropriated or used the person's name or other identification without the person's consent or authorization.
Statute: §22:18(9): http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=440214

Identity Theft Passport: Victims may apply for an identity theft passport, which can be presented to law enforcement to help prevent arrest or detention for an offense committed by another person. (Financial institutions are not required to honor an identity theft passport as proof of identity or proof of identity theft). The Oklahoma State Bureau of Investigation, which administers the program, notifies the state Department of Public Safety whenever a passport is issued and shares the passport records with law enforcement agencies upon request. The records are available only to law enforcement and are sealed to the public.

To obtain a passport, victims apply to the Oklahoma State Bureau of Investigation (OSBI), and must:

- Obtain and submit an Order of Expungement (see above); or
- Submit a copy of a identity theft report, filed with a federal, state, or local law enforcement agency, indicating the report of the applicant being a victim of identity theft; a copy of an identity theft affidavit (http://www.consumer.gov/idtheft/pdf/affidavit.pdf) that was submitted to one or more of the three national recognized consumer reporting agencies; and a copy of the certified mail delivery receipt showing the affidavit was received by the reporting bureaus.

Passport Application Form:
http://www.ok.gov/osbi/documents/Identity%20Theft%20Passport%20Request%20Form%20draft%206-28-041.pdf
Statute: §22:19b: http://www.oscn.net/applications/oscn/DeliverDocument.asp?CiteID=440216
http://www2.lsb.state.ok.us/os/os%5F22%2D19b.rtf

Security Breach: State law requires businesses and state government agencies that own or license computerized data that includes personal information to disclose any breach of security of the system to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the 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.

Personal information is defined as an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted: Social Security number; driver's license number; or a financial 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. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Notification can be provided 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 entity 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 any two of the following: e-mail notice, conspicuous posting on the agency's web site, and notification to major statewide media.

Statute: §24:161 through 165:
http://www.oscn.net/applications/OCISWeb/deliverdocument.asp?lookup=Next&listorder=10400&dbCode=STOKST24&year= (must use the "Next Section" link on the red menu bar at the top of the page to move through the sections).

State Resources:

Oklahoma State Bureau of Investigation, "Preventing Identity Theft" (http://www.ok.gov/osbi/Criminal_History/Identity_Theft_Passport_Program/Identity_Theft_Prevention_-_Steps_You_Can_Take.html)

Oklahoma Department of Libraries, "Identity Theft" (http://www.odl.state.ok.us/usinfo/pubs/idtheft.pdf)
This document directs victims to "*File a report with your local police department*."

University of Oklahoma Police Department, "ID Theft: Has Some Clown Taken Over Your Good Name?" (http://www.ou.edu/oupd/idtheft.htm)
This comprehensive web site includes information on prevention and steps victims should take. It instructs victims to "*File a police report with your local police or the police in the community where the identity theft took place."* It further instructs victims to: "*Get a copy of the report to submit to your creditors and others that may require proof of the crime."* It also provides the following tips on filing a police report:

- *"Provide documentation. Furnish as much documentation as you can to prove your case. **COPIES** of debt collection letters, credit reports, your notarized Identity Theft Affidavit, and other evidence of fraudulent activity can help the police file a complete report. (Keep originals for your own files; you may need more copies.)*
- *Be persistent! —In 2003, over 60 percent of fraud victims who filed FTC complaints indicated they **didn't** notify their local police department. 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. If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police. If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead.*
- ***Be a motivating force.** Ask your police department to search the FTC's Consumer Sentinel 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. That's an important reason to file a complaint with the FTC. Law enforcement agencies use complaints filed with the FTC to aggregate cases, spot patterns, and track growth in identity theft. This information can then be used to improve investigations and victim assistance."*

Legislation:

2008:
HB 2245 expands the state's security breach law to include businesses and other organizations. Previously, only state governmental agencies were required to disclose breaches of security of databases of electronic data that include personal information to disclose any breach of security.

2007:
HB 1329 increases the penalty for identity theft to one to five years in prison. Previously, it was punishable by up to two years in prison.

Under **SB 567,** victims of identity theft will have the right to contact the local law enforcement agency where they live and have an incident report about the identity theft prepared and filed, even if the jurisdiction may lie elsewhere for investigation and prosecution. The local law enforcement agency that prepares and files the incident report must, upon request, provide the victim with a copy of the incident report. The law enforcement agency may share the incident report with law enforcement agencies located in other jurisdictions.

SB 714 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 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:
SB 1748 allows consumers to place a security freeze on their credit reports. A security freeze prohibits, with certain specific exceptions, credit reporting agencies from releasing the consumer's credit report or any information from it without the express authorization of the consumer, preventing identity thieves from opening new accounts. To place a freeze, consumers must request one in writing by certified mail to the credit reporting agencies. The agencies are permitted to charge a fee of $10 for each placing, removing or temporary lifting of a security freeze. However, agencies may not charge a fee to senior citizens 65 years or older or to identity theft victims who submit an investigative report or complaint to a law enforcement agency about unlawful use of personal information by another person.

HB 2473 outlaws a scam commonly called "phishing," where someone sends an e mail that looks official but is used to trick the recipient into giving away personal information. The bill prohibits a person from knowingly sending e-mails that falsely represent another legitimate business and prohibits linking or sending the e-mail recipient to a false Web page in order to collect identifying information. The bill also makes it illegal to obtain identifying information from the e-mail recipient, directly or indirectly, for activities the recipient thinks is valid.

The law also outlines options for those claiming to fall victim under the Anti-Phishing Act, including seeking an injunction on the alleged violator, recovering actual damages or recovering $100,000 for each violation.

The bill also expands the list of protected identifying information covered by the identity theft statutes to include Social Security numbers, date of birth, fingerprints, voiceprints and bank account information obtained through online phishing.

HB 2357 requires government agencies to notify their clients if the agencies' computer systems are breached, exposing individuals' personal information to identity thieves.

2004:
SB 1164 seeks to help keep victims of identity theft from being penalized for criminal acts committed by someone who has assumed their identity. Under the bill, victims of identity theft could have their criminal records cleared if they have been arrested, or are facing arrest, for crimes committed by someone who seized their name or identification. The legislation also would create a special passport for victims of identity theft to use with law enforcement and other public safety authorities. The Oklahoma State Bureau of Investigation would administer the Oklahoma Identity Theft Passport Program and maintain records of requests for passports. OSBI would notify the state Department of Public Safety whenever a passport is issued and share the passport records with law enforcement agencies upon request. The records would be available only to law enforcement and would be sealed to the public. To qualify for the passport, the victim must file an identity theft report with a federal, state or local law enforcement agency and provide the report, an identity theft affidavit and supporting documentation to a consumer reporting agency.

SB 1168 expands the crime of identity theft to include and increases the maximum fine from $10,000 to $100,000. It adds place of business or employment, debit, credit or account numbers, and driver license numbers to the list of personal identifying information covered by the statute. Also, identity thieves will now be required to make restitution to their victims, in addition to any criminal penalty imposed by the court. Victims may also bring a civil action for damages against any person participating in furthering the crime or attempted crime of identity theft.