



ATTORNEY GENERAL OF TEXAS
GREG ABBOTT

**Consumer Alert: Attorney General Abbott Advises
Attention to Identity Theft**

**Texans need to protect their personally identifying information,
watch for signs of fraud**

According to the Federal Trade Commission, Texas ranks second in the nation for identity theft complaints, so Texans should carefully guard their identities and credit ratings. In 2008, nearly 32,000 Texans were identity theft victims and as a result, lost thousands of dollars and hours of time attempting to correct their credit ratings and personal financial history.

Identity theft is a crime that occurs when a criminal illegally uses someone else's personal information – whether it's another's name, address, driver's license number, Social Security number, credit card number – to commit fraud or other crimes. Sometimes identity theft is detected quickly, but other times it may take years before it surfaces. As a result, a victim may not recognize the theft until his or her credit has been destroyed. No one, including children, is immune to this crime.

The average victim loss runs into hundreds of dollars, with victims forced to spend hours cleaning up the damage. But the worst cases can cost thousands of dollars and take years to fully repair. To help prevent identity theft, the OAG conducts public education efforts and pursues vendors that fail to protect their customers' personal information.

Identity thieves obtain their victims' personal information in several ways. Here are just a few:

- **Dumpster diving.** Thieves retrieve bills and other documents out of the trash. Although Texas law prohibits vendors from simply throwing away documents that contain their customers' sensitive information, when a store or office makes a mistake, identity thieves can recover large caches of personal information from publicly accessible dumpsters. To prevent thieves from obtaining usable personal information from the trash, Texans should use a cross-cut shredder to destroy financial documents and paperwork with personal information.

- **Skimming.** Some identity thieves use an economical storage device to copy credit/debit card numbers when credit cards are processed by vendors. Texans can avoid falling victim to this tactic by keeping an eye on their credit card statements.
- **Phishing.** Thieves pretending to be financial institutions or online retailers often send official-looking e-mails in an attempt to trick Internet users into revealing their personal information. Texans can avoid falling victim to this tactic by refusing to provide their passwords or sensitive information (personal or account details) through e-mail or in response to unsolicited phone calls.
- **Pretexting.** Like phishing, this scheme employs false pretenses to obtain personal information from financial institutions, telephone companies, and other sources. Texans can avoid falling victim to this tactic by refusing to provide their passwords or sensitive information (personal or account details) through e-mail or in response to unsolicited phone calls.
- **Phony job offers.** Identity thieves place fake employment ads and ask respondents to fill out applications that include their personal information. Texans can avoid falling victim to this tactic by researching a company before providing any personal information. Job applicants should only apply at a reputable business's known physical location or Web site.
- **Change of address.** Identity thieves use change of address forms to divert a consumer's mail to another location by completing a change-of-address form. The U.S. Postal Service now sends a "Move Validation Letter" to both an old and new address when a change of address is filed. If Texans receive one of these letters but did not apply for a change of address, they should call their post office immediately.
- **Regular stealing.** By stealing items like wallets, PDAs, laptops, purses, new checks, tax information or personnel records, identity thieves can have access to the personal information they need to commit identity theft. Texans can avoid falling victim to identity theft by guarding these sensitive records with care, and only carrying those records that they need. If records are lost or stolen, Texans should cancel the lost or stolen credit cards and alert their banks.
- **Shoulder surfing.** By literally looking over a victim's shoulder, identity thieves can obtain personal information, such as at an ATM, for example. Texans can avoid to this tactic by being aware of their surroundings and carefully concealing personal information and PIN numbers.

- Hacking. Hackers gain information by breaking into computer systems. Texans can avoid hackers by using anti-virus software, firewalls and other methods to keep your computer secure. Texans should keep all such software updated to ensure they receive the latest protections.
- Working in your home. Residential contractors or other workers may misuse personal information they find in plain view. Texans can avoid this tactic by keeping sensitive documents in a secure place and limit unsupervised unknown workers in their homes.

Texans should review their financial statements regularly and look for unusual activity. They should also request and review their credit report each year. To get a free copy of the “big three” credit reports, visit www.AnnualCreditReport.com, call (877) 322-8228 or write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, Ga. 30348-5281.

Texans who believe their identity has been stolen can follow these steps to minimize their losses:

First request a credit report “Fraud Alert,” which requires that creditors follow special procedures before creating new accounts or making changes to existing accounts. A call to any of the three nationwide consumer reporting companies can initiate a 90-day fraud alert.

Fraud alerts entitle credit card holders to free copies of their credit reports. Potential identity theft victims should look for credit inquiries from companies they have not contacted, accounts they did not open, and debts on their accounts that they cannot explain.

Identity theft victims should file complaints with the OAG and the Federal Trade Commission. A printed FTC complaint, which is available online, in conjunction with a police report, can constitute an identity theft report and entitle a victim to certain protections. The identity theft report can be used to:

- permanently block fraudulent information from appearing on a credit report;
- ensure that improper debts do not reappear on a credit report;
- prevent a company from continuing to collect debts that result from identity theft; and
- place an extended fraud alert on a credit report.

The OAG identity theft Web site, www.texasfightsidtheft.gov contains a wealth of helpful information for identity theft victims, including an Identity Theft Kit. Information at www.texasfightsidtheft.gov will help stop a perpetrator from continuing to use a stolen identity and help a victim recover from the effects. The site explains how to report the crime, work with businesses, close fraudulent

accounts, and place a security alert and/or freeze on a credit report. For more information about how to recover from identity theft and steps Texans can take to protect their personal information, visit www.protectyouridnow.org or www.texasfightstheft.gov.

Other Resources:

Office of Attorney General

(800) 621-0508

Federal Trade Commission

Identity Theft Hotline: (877) ID-THEFT (438-4338)

TTY: (866) 653-4261

FTC Identity Theft Clearinghouse

600 Pennsylvania Avenue, NW

Washington, DC 20580

www.ftc.gov

www.consumer.gov

Consumer Credit Reporting Companies

Equifax: (800) 525-6285

Experian: (888) EXPERIAN (397-3742)

TransUnion: (800) 680-7289

Better Business Bureau

www.bbb.org