



Protect Your Credit and Identity

Identity theft has become a problem anyone may have to deal with. Identity theft occurs when thieves steal personal identification, such as Social Security, bank account and credit card numbers and use them as their own. Thieves obtain the information easily by sorting through a person's trash, accessing public records, overhearing numbers given in a phone conversation or stealing from mailboxes. They use the information to open credit card accounts, make withdrawals from ATM's, make charges on credit cards and make down payments or deposits on a car or house.

To reduce the risk of identity theft and the problems that can result, take the following precautions.

- Don't carry Social Security card, birth certificate or passport in a purse or wallet except when needed.
- Don't print Social Security or driver's license numbers on checks.
- Photocopy both the front and back of all credit cards and keep in a safe location.
- Sign all credit cards as soon as they arrive.
- Don't leave credit card bills, credit card and ATM transaction receipts, store receipts, bank account statements out in the open.
- Dispose of papers with account numbers on them, mailings indicating pre-approval or offering credit by tearing them in small pieces or shredding them before putting in the trash or recycling.
- Don't give out credit card or Social Security numbers over the phone or Internet, unless you make the call or know it is definitely a reputable company.
- Keep credit/debit receipts and check them against the monthly statement.

If a credit card is stolen immediately notify the credit card company. If the missing card is reported to the issuer before it is used by someone else, the cardholder owes nothing. If charges are run up before the card is reported, the cardholder may be liable for \$50.

If a person suspects someone else is using his or her Social Security number it is important to contact the Social Security Administration office at (800) 269-0271.

Taking precautions can reduce the risk of identity theft, but should it happen, promptly reporting the crime can minimize the consequences.

A Word On Social Security Numbers

Your employer and financial institution will likely need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check, like when you apply for a loan, rent an apartment, or sign up for utilities. Sometimes, however, they simply want your SSN for general record keeping. You don't have to give a business your SSN just because they ask for it. If someone asks for your SSN, ask the following questions:

- Why do you need my SSN?
- How will my SSN be used?
- What law requires me to give you my SSN?
- What will happen if I don't give you my SSN?

Sometimes a business may not provide you with the service or benefit you're seeking if you don't provide your SSN. Getting answers to these questions will help you decide whether you want to share your SSN with the business. Remember—the decision is yours.

If you think your identity has been stolen, here's what to do:

- Contact the fraud departments of any one of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three credit reports will be sent to you free of charge.
- Close the accounts that you know or believe have been tampered with or opened fraudulently. Use the ID Theft Affidavit when disputing new unauthorized accounts.
- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.
- File your complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps them learn more about identity theft and the problems victims are having so that they can better assist you. The FTC's Identify Theft Hotline toll-free number is 1-877-IDTHEFT (438-4338).

Credit Card Users Should Avoid Scams



While credit provides convenience and added buying power to America's pocket books, it also has become a fertile ground for scams and deceptions so it's important those who use credit know how to avoid being taken advantage of.

Through the Truth in Lending, Fair Credit Reporting, Fair Debt Collection Practices and other federal acts, credit users are promised certain lending conditions. Liability limits on credit cards, timely payment processing and non-threatening debt-collection, are 11 rights promised to credit users, but none of the rights can guarantee against credit scams. By following a few suggestions, borrowers can avoid and correct credit problems. One of the best ways for individuals to avoid credit problems is paying attention to the small print before signing anything. Lenders are required to give certain information, such as the annual interest rate and the total finance charge, so borrowers should make sure they read and understand all of the information given before they ac-

cept credit offers.

Another way to avoid credit scams is for credit card users to protect the privacy of their card number. Any unused credit card information such as new applications, outdated cards and cash advance checks should be destroyed.

If something unknown appears on a credit card statement, individuals should make sure to find out what it is.

Fraudulent charges often can be eliminated or reduced if they are handled promptly.

One final way to avoid scams is for credit users to remember credit problems cannot be erased from credit histories. Often advertised are "credit repair clinics," which promise to rebuild credit. In reality, there is nothing these companies can do to change negative information on a credit report. While those seeking to escape from bad credit may find these advertisements appealing, borrowers should remember nothing the company might do can take away what the borrower himself has already done.

How ID Thieves GET Personal Information

They steal wallets and purses containing your identification and credit and bank cards.

They steal your mail, including your bank and credit card statements, pre-approved credit offers, new checks, and tax information.

They complete a "change of address form" to divert your mail to another location.

They rummage through your trash, or the trash of businesses, for personal data in a practice known as "dumpster diving."

They fraudulently obtain your credit report by posing as a landlord, employer or someone else who may have a legitimate need for and legal

right to the information.

They find personal information in your home.

They use personal information you share on the Internet.

They scam you, often through email, by posing as legitimate companies or government agencies you do business with.

They get your information from the workplace in a practice known as "business record theft" by: stealing files out of offices where you're a customer, employee, patient or student; bribing an employee who has access to your files; or "hacking" into electronic files.

How ID Thieves USE Your Personal Information

They call to your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to the new address, it may take some time before you realize there's a problem.

They open a new credit card account, using your name, date of birth and SSN. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.

They establish phone or wireless service in your name.

They open a bank account in

your name and write bad checks on that account.

They file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.

They counterfeit checks or debit cards, and drain your bank account.

They buy cars by taking out auto loans in your name.

They give your name to the police during an arrest. If they're released from police custody, but don't show up for their court date, an arrest warrant is issued in your name.

The Identity Theft and Assumption Deterrence Act

Enacted by Congress in October 1998 (and codified, in part, at 18 U.S.C. §1028) is the federal law making identity theft a crime.

The Identity Theft and Assumption Deterrence Act of 1998 makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

Under the Act, a name or SSN is considered a "means of identification." So is a credit card number, cellular telephone electronic serial number or any other piece of information that may be used alone

or in conjunction with other information to identify a specific individual.

Violations of the Act are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and SSA's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Dept. of Justice.

In most instances, a conviction for identity theft carries a maximum penalty of 15 years imprisonment, a fine and forfeiture of any personal property used or intended to be used to commit the crime. Pursuant to the Act, the U.S. Sentencing Commission has developed federal sentencing guidelines to provide appropriate penalties for those persons convicted of identity theft.

Schemes to commit identify theft or fraud also may involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud or Social Security fraud. Each of these federal offenses is a felony and carries substantial penalties—in some cases, as high as 30 years in prison as well as fines and criminal forfeiture.

State Laws— Many states have passed laws related to identify theft; others are considering such legislation. Where specific identify theft laws do not exist, the practices may be prohibited under other laws. Contact your State Attorney General's office or local consumer protection agency for laws related to identify theft or visit www.consumer.gov/idtheft



Credit Bureaus

- Equifax**
1-800-525-6285
www.equifax.com
- Experian**
1-888-397-3742
www.experian.com
- TransUnion**
1-800-680-7289
www.tuc.com