Unfortunately, fraud and identity theft are common occurrences in today's marketplace. Criminals and thieves use multiple tactics to obtain personal information about an individual which can later be used to commit fraud or identity theft. The effects can be crushing and take years to remedy.

Below are some of the most common ways in which criminals commit fraud and identity theft, and suggestions to help keep your information safe.

Fraud

In many fraud cases, the goal is to obtain access to a credit card or financial account, so that a criminal can steal someone else's money or make unauthorized purchases. If reported promptly, the damages are financially minimal as your credit card company will only hold you liable for a small portion (if any) of the unauthorized purchases.

Identity theft

Identity theft is when a criminal assumes someone else's identity. The goal is usually to commit fraud and the effects are very personal. Identity theft is potentially more devastating than other instances of fraud, such as having your credit card stolen. With true identity theft, the thief may open new accounts in your name, withdraw funds from existing accounts, or even change the address on your accounts so that you are unable to see fake charges on your statement. To correct identity theft, the process may take years and a significant financial investment on the part of the victim.

Unfortunately, statistics show that many incidents of credit card fraud and identity theft are committed by a family member or a friend of the victim. Following are some common tactics used to commit fraud and identity theft. It is wise to be careful in today's marketplace to protect your identity and financial accounts.

Common tactics used to commit fraud and identity theft:

Email phishing

Phishing emails look a lot like a legitimate email from a reputable company, or even a government agency, but actually originate from a criminal. The email usually directs you to a website that also looks legitimate where you are asked for sensitive personal information, such as your social security or account number. Typically, the goal of email phishing is to have the recipient provide sensitive personal information, such as financial account information or social security number, to commit further fraud.

If you receive a suspicious email, do not open it and do not click on any links in the email if you have opened it. Contact the sender and ask if they sent you the email. Never supply financial account information or your social security number in an email or in response to an email you have received.

For more detailed information on phishing, please see further information on our [website](#).

Telephone scams

Telephone scammers contact you by telephone and request that you provide some form of sensitive personal information, such as your account or payment information, to verify your identity or to sign you up for a new product. Any company you do business with that already has your personal information will not request the same information again if they contact you to discuss your account; although they may ask questions that may contain a portion of the information to verify your identity.
If you have any reservations about the request, it is always best to contact the business or agency by phone using the contact information you have already been provided, such as the number on the back of your credit card or your monthly statement, instead of any contact information the person on the phone may provide.

Stealing

A thief can obtain your credit card number or other sensitive information by simply stealing it. For example, a thief may steal the credit card number by personally handling the card when you make a purchase, or may steal your wallet or purse and use your financial cards. Also, some criminals may steal mail, which could contain bank statements, bills and other documents with your sensitive personal information.

If you are going to be away from home for an extended period of time, have the post office hold your mail or have a trusted friend or neighbor collect it for you. Don’t carry you social security card or other unnecessary personal documents in your purse or wallet if they are not needed. Always be careful when giving your credit and debit cards to someone to make a purchase. For example, if you pay for dinner at a restaurant, be cautious with where your credit or debit card is taken and that it is not out of sight for an unnecessarily long period of time. If you suspect any suspicious activity, contact your financial institution immediately. You can also request a credit report, and each consumer is entitled to three free reports a year, one from each of the three major credit bureaus.

Skimming

Criminals also use copying technology on point-of-sale or ATM terminals to obtain credit card numbers.

Be careful when swiping a credit or debit card for a purchase to ensure that no additional technology is attached to the machine. If you are unsure or hesitant, ask that the cashier swipe your card on the register, or pay with cash or check.

Dumpster diving

It is common for criminals to search through dumpsters looking for bills or other paper with your sensitive personal information on it. When organizations do not properly dispose of paper documents with information such as credit card number or social security number, a criminal is able to take that information and commit fraud or identity theft.

Always be careful in supplying sensitive information on a paper document. If you do, ask about the companies data destruction procedures and ensure that your sensitive information is properly shredded and disposed. Also, shred your own documents at home if they contain sensitive personal information. Criminals also rummage through individuals’ trash.

Resources

The Federal Trade Commission (FTC) is committed to educating consumers on protecting themselves from identity theft and other related crimes. Visit the FTC’s fighting back against identity theft website ftc.gov/bcp/edu/micro-sites/idtheft/ to learn more.

Credit bureaus

You may contact Equifax, Experian and TransUnion individually using the contact information provided below for your free credit report:

Equifax
Equifax Credit Information Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111 for general inquiries
1-888-766-0008 to place a fraud alert on your credit report

Experian
1-888-397-3742 for consumer credit center
1-866-200-6020 to request a credit report by mail

TransUnion
TransUnion Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1-877-322-8228 for your free credit report
1-800-680-7289 to report fraud

*NOTE: The information in this document is provided by Epsilon for general informational purposes only and not for the purpose of providing legal advice or giving a legal opinion. Readers should not act upon this information without first seeking professional legal counsel.

epsilon.com 888 309 0505 privacy@epsilon.com