# Fraud & Identity Theft

**DISCOVER THE MOST COMMON FRAUD AND IDENTITY THEFT TACTICS AND SUGGESTIONS TO HELP KEEP YOUR INFORMATION SAFE.**

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 that 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, suggestions that will help you keep your information safe and useful contact information.

**Email phishing**
A phishing email looks a lot like a legitimate email from a reputable company, or even a government agency, but actually originates 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 so the sender can 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 Epsilon's consumer information on phishing.

**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; however, 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 on your monthly statement, instead of any contact information the person on the phone may provide.

**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 for their own use or make unauthorized purchases. If reported promptly, the damages are financially minimal as your credit card company will hold you liable for only 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. Below 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.

**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 they 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 U.S. Postal Service 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.



EPSILON®

# Fraud & Identity Theft

**Skimming**
Criminals also use copying technology on point-of-sale terminals and 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 numbers or Social Security numbers, 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 company's data destruction procedures and ensure that your sensitive information is properly shredded and disposed of. Also, shred your own documents at home if they contain sensitive personal information. Criminals also rummage through individuals' trash.

**Federal Trade Commission (FTC)**
The FTC is committed to educating consumers on protecting themselves from identity theft and other related crimes. Visit the FTC's Identity Theft webpage at consumer.ftc.gov/features/feature-0014-identity-theft 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 Fraud Victim Assistance Department**
P.O. Box 2000
Chester, PA 19016

1 877 322 8228 (for your free credit report)
1 800 680 7289 (to report fraud)

**Consumer Information on Phishing**
Phishing is a scam in which fraudsters send spam email to get personal and financial information.

According to the Federal Trade Commission, phishing is when internet fraudsters send spam email messages to lure unsuspecting victims into providing personal and financial information, including credit card numbers, bank account information, Social Security numbers, passwords or other sensitive information.

These types of emails claim to be from a business or organization that you may have a relationship with, such as a bank, online payment service or even a government agency.

The message may ask you to update, validate or confirm your account information. The message then directs you to a website that looks just like a legitimate site, but it isn't. It's a bogus site whose sole purpose is to trick you into divulging personal information so the operators can steal your identity and withdraw money, run up bills or commit crimes in your name.

Attackers can also lure clients and consumers to malicious websites through scare tactics. The sites will look legitimate and offer a tool or download to determine if your information has been compromised.



EPSILON

# Fraud & Identity Theft

## OTHER USEFUL INFORMATION

**Examples of phishing language**
"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

**Tips to help you avoid getting hooked**

- Don't follow links from unsolicited emails, even when they appear to come from a person or organization you are familiar with. If you are unsure of the authenticity of an email communication, call the organization in question directly or access their page by typing the URL into your browser.
- Don't reply to email messages that ask for personal or financial information. Delete any emails that ask you to confirm or divulge your financial information. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new internet browser session and type in the company's correct web address yourself.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins with "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Be cautious about opening any attachment or downloading any files from emails you receive — regardless of who sent them.
- Don't cut and paste a link from the message into your web browser — phishers can make links look like they go one place but actually send you to a different site.
- Check the "from" field. Phishers can easily spoof authentic email addresses, making it appear that an email is coming from an authentic, trusted sender, but checking the "from" field can at least help you identify unsophisticated phishers. If the "from" field contains excessive characters, has spelling mistakes or does not share the same domain as the company (e.g., @companycustomershelp.com [illegitimate] versus @ company.com [legitimate]) you might have found a phish.
- Look for grammatical errors and spelling mistakes. A lot of phishing activity originates from outside the U.S. where English is not the first language; so when these emails are crafted, there are often grammatical errors or spelling mistakes — errors your real bank would never make in a professional customer email.
- Don't call phone numbers provided in suspicious emails. Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice over Internet Protocol technology, the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. Some phishing emails contain software that can harm your computer or track your activities on the internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. A firewall helps make you invisible on the internet and blocks all communications from unauthorized sources.

**What to do if you've been phished or scammed**
Forward phishing emails to spam@uce.gov and to the legitimate company that is being misrepresented in the phishing email. You also may report phishing emails to reportphishing@antiphishing.org. The Anti-Phishing Working Group, a consortium of internet service providers, security vendors, financial institutions and law enforcement agencies, uses these reports to fight phishing.

If you've been scammed, visit the Identity Theft page on the Federal Trade Commission's website at consumer.ftc.gov/topics/identity-theft and file a report with the Federal Trade Commission at ftccomplaintassistant.gov.



EPSILON®