Fraud Prevention Guide

What you should know about fraud protection and prevention.

CIT Bank is dedicated to keeping your account safe, but we also want to make sure that you can protect yourself and your account. So here are some terms, tips, and more to help you defend yourself against fraud.

How to recognize fraud.

Fraud occurs in many different ways, and it's important to understand what they are and how they work. This guide includes information on various types of fraud. For more information, see the Additional Resources section at the end of this document.

Identity Theft

Identity Theft occurs when someone uses your personal information, such as your name, Social Security number, date of birth, driver's license number, online banking credentials (User ID and password), or account numbers without your permission to open accounts, access your existing accounts, or purchase items in your name.

Common Identity Theft scams.

Dumpster diving

Criminals go through your trash in an effort to find discarded personal information. By using information on junk mail, utility bills, receipts, old credit cards, and other correspondence, they are able to take over existing accounts or to open new ones. The best course of prevention is to shred all documents before discarding them.

Phishing, vishing, smishing

Phishing (fraudulent email), vishing (fraudulent phone call), and smishing (fraudulent text) are deceptive ways to trick you into revealing personal, financial, or account information. These communications resemble authentic materials from trusted and well-known companies to try to get you to reveal personal information, account or credit card numbers, or account passwords.

How to identify a phishing, vishing, or smishing scam:

Phishing	If you receive an email asking you to update your account information, activate your online account, or other similar requests by clicking a link, do not click. Instead, contact the company directly at the phone numbers provided on their websites; bank statements, or debit, credit, or ATM cards.
Vishing	Fake caller IDs can make it appear that a legitimate company is calling. If you receive a call that asks for personal information, hang up and call the actual company using the phone numbers provided on their websites; bank statements, or debit, credit, or ATM cards and report the call.
Smishing	If you receive a text that prompts you to call a phone number or submit information on a website to update account information, activate an online account, or other similar requests by calling a phone number or submitting information on a website, do not do so. Instead, contact the company directly at phone numbers provided on their websites; bank statements; or debit, credit, or ATM cards.

Malware

Malware is malicious software designed to damage or disable computer systems. Malware can gather personal information from your computer, including account numbers, passwords, online banking credentials, and key strokes, and can be present on your machine without you knowing or being alerted. Some indicators that your computer may be infected are computer performance problems, pop-ups, spam email, or unexplained actions (e.g., programs running that you did not initiate, new toolbars you did not install, etc.).

Bank Account Fraud

Bank Account Fraud occurs when you are asked to open a new account or use an existing account and make a fraudulent deposit in the form of either a check or ACH transfer. Once the deposit is available, you are asked to make transfers out, often with the offer to keep part of the deposit.

Those behind the scam want you to believe there is no risk in opening a bank account and that once a transaction has "cleared" it cannot be returned unpaid. However, fraudulent transactions can take up to 60 days to be returned. If the paying bank determines that the deposit is fraudulent, then the deposit will be reversed from your account and you will be responsible for the full amount.

Bank account fraud has many variations and typically targets individuals who are looking for employment, dating online, or selling items.

Common Bank Account Fraud scams.

Personal scams

Related to online dating, romances, friendship, and strangers in need. Often people will connect with targets at online dating/friendship sites and ultimately will ask you to open an account in your name so that they can have money deposited into it. They may also ask you to use an existing account or for your online banking credentials or other personal information. They will frequently have a story relating to some sort of financial difficulty justifying why they can't use their own account. The most difficult aspect of this fraud is the personal impact, because victims believe that they are close friends, sometimes even fiancés.

How to protect yourself from personal scams:

1. **NEVER** give your personal information or account information to an individual you've met online.
2. **NEVER** initiate transfers to or from an account that you do not own.
3. **NEVER** accept deposits on behalf of someone else.
4. Be suspicious of anyone who prefers to communicate via instant messaging (IM) or email as opposed to the site on which you met.
5. Be extra vigilant if anyone tries to discuss his or her finances with you.

Job scams

Related to work-at-home opportunities and fraudulent mystery shopping opportunities. Emails for job opportunities promise a paycheck (paper check or direct deposit) and extra money to purchase supplies. The "employer" will ask you to send a portion of the money to another account to cover one-time costs. Mystery shopping opportunities provide your first paycheck and the extra money you will need for your "first assignment," which is to evaluate the office of a well-known money transfer service. You are asked to wire money to another bank account and evaluate the office's customer service.

How to protect yourself:

1. **NEVER** accept an employment offer that involves processing checks, ACHs, or electronic payments through your personal account or an account in your name.
2. Verify that the mystery shopping company is in the Mystery Shopping Providers Database **(http://www.mysteryshop.org/)**.

Award scams

Often in the form of lotteries, sweepstakes, or government grants. Fraudsters provide a check or ask you to provide your routing and account number. You are then asked to send a portion of the award or grant back to pay taxes and fees.

How to recognize award scams:

1. Legitimate lotteries pay taxes directly to the government. Winners do not reimburse some of their proceeds for taxes.	**2.** It is against United States law to play foreign lotteries by mail or telephone.	**3.** United States government agencies do not award free grants that were not applied for by the recipient.	**4.** **DO NOT** give your account information to companies with whom you have not initiated business.	**5.** **DO NOT** deposit a check you weren't expecting to receive.

Sales and service scams

Often in the form of overpayment via an online auction. The buyer will claim it was a mistake and ask you to wire the difference.

If you are selling or renting an item, never accept payment for more than the purchase or rental amount.

How CIT Bank protects you.

Keeping your accounts and information safe is as important to us as it is to you. At CIT Bank we apply security controls and processes that meet industry best practices to help safeguard your information including, but not limited to, the following:

- Account activity monitoring to detect potential anomalies and indicators of compromise.
- Processes, procedures and access controls to ensure that only authorized people can access your account information.
- Industry recognized antivirus technology to help protect our computer systems from computer viruses and malware.
- Firewalls to segregate computer environments and help defend against internet threats.
- A minimum of 128-bit encryption is used to secure sessions in order to preserve your privacy when interacting with our systems.
- Secure messaging portal.
- Session security standards including automatic sign-out after a period of inactivity.

For questions about security, privacy, or your account, call us at 855-462-2652.

How you can protect yourself.

While we do all that we can to ensure your protection, please remember to exercise caution to avoid any potential scams.

Personal information

Never share any of your personal information or account information (including your User ID and password). Also, remember to:

- Monitor your credit report and look for unauthorized or inaccurate activity and accounts. You can get a free report from the government-sponsored site **www.annualcreditreport.com**
- Secure your personal information in a safe location that is only accessible to you at home and at work.
- Don't share personal information on social networking sites (e.g., DOB, phone number, place of birth, address, last 4 digits of Social Security number).
- Sign up for paperless statements. This way, fraudsters cannot obtain personal information by stealing your paper account statements.

Your accounts

Monitor your bank accounts regularly for unauthorized activity and transactions. Look for changes to your email address, physical and mailing address, and telephone numbers. Also ensure that you initiated all of the transactions on your statement. If you find unauthorized activity, notify CIT Bank immediately. Other measures to protect your accounts:

- Create strong passwords. Use upper-case and lower-case letters, special characters, and numbers. Most importantly, do not write your passwords down.
- Sign-out and close your browser after each online banking session.
- Bookmark the websites you use the most in your browser. Use your saved favorites to navigate to sites for your banks and credit cards.
- Check "Remember Me" on websites you visit regularly. A fraudulent (spoofed) website will not be able to auto-populate your User ID. **NOTE:** Do not set up "Remember Me" on public or shared computers.
- Only use sites that begin with "https" when entering a password, setting up an account, or purchasing something online. The "s" signifies that the browsing session is secure.

Your computer

Updating and maintaining your computer software is an important step in avoiding fraud:

- Install recent security software from a reputable company on your computer. This software should include antivirus, antispyware, and antimalware protection in addition to personal firewalls.
- Keep all of your software updated with the most recent versions and install manufacturer patches. This applies to all of the software on your computer, including your operating system, Web browser, security software, and other programs.
- Only download software, programs, and files from legitimate sources that are endorsed by the manufacturer.
- If possible, use two computers: the first for online banking and other sensitive applications and the second for things like Web browsing, social networking, and email.

Yourself

Remember to use common sense and take other steps:

- Be suspicious of people you meet online. Be wary of strangers or friends that want to discuss finances or financial opportunities.
- **NEVER** conduct transactions, make deposits, or open accounts at someone's request or on behalf of someone.
- Independently research and verify individuals and/or companies with whom you intend to do business. Contact companies that you already do business with, using verified contact information, such as the telephone number on your statement or card.
- Do not respond to emails or download files from suspicious sources or a source you do not know.

What to do if you're a victim of fraud.

Early detection and a swift response to fraud suspicions are important to remedy the situation and minimize impact. Please take the following steps if you experience fraud:

Identity Theft

1. Notify CIT Bank immediately. We will help you determine next steps based on your individual situation. It may be necessary to take additional steps and not just the ones listed below.
2. Contact the credit reporting bureaus to place a fraud alert on your profile and to order a report. You only need to contact one credit reporting bureau. The credit bureau you call is required to contact the other two. When you place a fraud alert on your credit profile, any new credit requests will receive careful review to ensure the applicant is you.
   - Equifax: **1-800-525-6285** • **www.equifax.com**
   - Experian: **1-888-397-3742** • **www.experian.com**
   - Trans Union: **1-800-680-7289** • **www.transunion.com**
3. Close any accounts in your name that were opened fraudulently.
4. Contact the Social Security Administration Fraud Hotline. **1-800-269-0271**
5. File a police report with your local law enforcement agency.
6. Report identity theft to the Federal Trade Commission so that law enforcement agencies across the country can use the information to help with their investigations. **Click here** or call **1-877-438-4338** (1-877-IDTHEFT).
7. Contact your local post office if you believe your mail was stolen or redirected. **www.usps.com**
8. Contact your local Department of Motor Vehicles if you believe someone is trying to get a driver's license or identification card using your name and information.

Bank Account Fraud

1. Notify CIT Bank immediately. We will help you determine next steps based on your individual situation. It may be necessary to take additional steps and not just the ones listed below.
2. File a police report with your local law enforcement agency.
3. File a complaint regarding Internet-related fraud with the Internet Crime Complaint Center. **www.ic3.gov**
4. Report scams to your state **Attorney General**.
5. Report bank account fraud to the Federal Trade Commission so that law enforcement agencies across the country can use the information to help with their investigations. **Click here** or call **1-877-382-4357**.

Contact information and resources

CIT Bank Fraud Prevention Department

Toll Free **1-855-370-6827** • **FraudPrevention@cit.com** • Fax Number **1-800-350-1142**

Additional resources for the latest on fraud and ways to protect yourself

- **www.onguardonline.gov**
  OnGuardOnline.gov is the federal government's website to help you be safe, secure, and responsible online. You can learn how to avoid scams, protect your computer, and protect your family online.
- **www.ic3.gov**
  The Internet Crime Complaint Center (IC3) was established by the federal government to serve as a vehicle to receive, develop, and refer complaints regarding cyber-crime.
- **www.ftc.gov/idtheft**
  This is the Federal Trade Commission's website on identity theft. You can find information on how to protect yourself from identity theft, the different types of identity theft, and what to do if you are a victim of identity theft.
- **www.fdic.gov/consumers/theft**
  The Federal Deposit Insurance Corporation (FDIC) provides information about scams and how to be safe online. They also provide additional links to other government sites about fraud.
- **www.staysafeonline.org**
  This site is sponsored by the National Cyber Security Alliance. It provides proactive tips to prevent fraud and to stay safe online.
- **www.stopfraud.gov**
  This site helps educate consumers on how to protect themselves from all types of fraud—not just financial fraud and cyber-crime—and how to report it.