



IDENTITY THEFT

PROTECTING YOUR IDENTITY

Northern Trust will never send e-mail requiring customers to send personal information to us via e-mail or pop-up windows.

By understanding exactly what identity theft is, how it happens and how it affects you, you will be better able to prevent and, if necessary, resolve identity theft.

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone illegally obtains your personal information – such as your Social Security number, bank account number or other identification – and uses it to open new accounts or initiate transactions in your name. For example, someone might use your name and personal information to perform one or any combination of the following: open new credit cards, establish new bank accounts, forge checks, even apply for loans. This can cause financial loss and damage your credit, which can lead to a lengthy resolution process.

HOW DOES IDENTITY THEFT HAPPEN?

Identity theft is often portrayed as a high-tech crime affecting only those people who shop, communicate or do business online. However, while thieves can obtain personal information via online methods, identity theft often occurs offline. Stealing wallets and purses, intercepting or rerouting your mail and rummaging through your garbage are some of the common tactics that thieves can use to obtain personal information. The good news is that the more information you have about identity theft the better your defense.

Online scams. Online fraud occurs when a fraudster poses as a legitimate company to obtain sensitive personal data and illegally conducts transactions on your existing accounts. Often called “phishing” or “spoofing,” the most current methods of online fraud are fake e-mail, web sites and pop-up windows, or any combination of these.

Note: Any unsolicited request for Northern Trust account information you receive through e-mail, web sites or pop-up windows should be considered fraudulent and reported immediately.

A few tips about fake e-mail and websites. Fake e-mail will often appear to be from a legitimate source. While some e-mail is easy to identify as fraudulent, others may appear to be from an authentic address and trusted online source. Do not rely on the name or address in the “From” field, as this can be easily altered.

Fake e-mail often contains telephone numbers that are tied to the fraudsters. Never call a number featured on an e-mail you suspect is fraudulent, and be sure to double-check any numbers you do call. Contrarily, some of the telephone numbers listed in fake e-mails may be legitimate, connecting to actual companies. Just like with links, fraudsters include the real phone numbers in an effort to make the e-mail appear legitimate.

CONTINUED



Most fraud and identity thefts happen as a result of mail and garbage theft.

PREVENTION MATTERS – KNOWLEDGE IS THE KEY TO PREVENTION.

While Northern Trust works continuously to make sure your account and personal information are safe, here are some simple steps you can take to further reduce your susceptibility.

- **Do not provide your Social Security number unless absolutely necessary.** When a Social Security number is requested to sign-up for a service, confirm that it is actually needed rather than some other means of identification. In addition, do not put Social Security, driver's license or telephone numbers on personal checks.
- **Shred documents containing personal or financial information before discarding.** Most fraud and identity thefts happen as a result of mail and garbage theft.
- **Review your credit report.** Look over your credit report regularly – at least once a year – for any inaccuracies. As part of the Fair and Accurate Credit Transactions Act (FACT), you can obtain a free annual copy of your credit report. Refer to the website www.annualcreditreport.com for more information and to order a report. The following companies also can provide you with a copy of your credit report.
 - Equifax: 1-800-685-1111 or www.equifax.com
 - Experian: 1-888-397-3742 or www.experian.com
 - TransUnion: 1-800-916-8800 or www.transunion.com
- **Limit the use of paper bills.** A paperless environment reduces the chance of identity theft. When you sign-up for free online account access with Northern Trust Private Passport you can take advantage of electronic bill payment service. The fewer personal documents sent through the mail, the less chance there is for possible fraud.
- **Limit the credit offers you receive.** If you would like to reduce the number of credit offers you receive and the information companies share about you, contact the National Consumer Credit Reporting Agencies at 1-888-5-OPTOUT (1-888-567-8688).
- **Protect your passwords.** Memorize your passwords. Do not write them down or share them with anyone. Change them regularly and use combinations of letters and numbers. Do not use your Social Security number as a username or password. Never use the “Save ID and password” option on your computer.
- **Be wary of suspicious e-mail.** An e-mail requesting your account information and password should be scrutinized carefully, particularly if the information is needed to “award a prize” or “verify a statement.” Immediately delete any questionable e-mail. If you have opened an e-mail, do not open any attachments or links it may contain, and delete it.
 - Properly dispose of old computers and ensure that all sensitive information has been removed from the hard drive.
 - Maintain and run updated virus and spyware security software on your computer. Review your e-mail and Internet security settings.

If you have been a victim of identity theft, recovery services are available for you through The Identity Theft Assistance Center.

WHAT TO DO IF YOU SUSPECT YOU'RE A VICTIM OF IDENTITY THEFT

Notice suspicious account activity? Here are suggested steps you can take to address the issue.

If the fraudulent activity is limited to your Northern Trust account(s): Contact your Relationship Manager immediately. Northern Trust is a founding member of The Identity Theft Assistance Center (ITAC). This free program will assist in completing the appropriate affidavit, obtaining your credit report, contacting other institutions if suspicious activity is detected, as well as placing fraud alerts to protect your credit.

If you believe you are a victim of identity theft that extends beyond your Northern Trust account(s):

- **File a report with the local police.** Contact your local police department if you suspect that your personal information was stolen. A police report will lend weight to your case when dealing with creditors who may require proof of criminal activity.
- **Contact other creditors.** Contact your credit card and phone companies, as well as banks and other lenders, to notify them of potential fraud. Always follow-up any telephone conversations with a letter. Close any accounts that have been breached and reopen them with new account numbers and passwords. Never use your Social Security number as either a user name or password.
- **Report the criminal activity to the Federal Trade Commission (FTC).** Call the toll-free hotline at 1-877-ID THEFT (1-877-438-4338) to speak with a trained identity theft counselor. Or enter information about your complaint into a secure FTC online database at www.consumer.gov/idtheft. Your information may be shared with other law enforcement agencies investigating identity theft.
- **Contact other agencies as appropriate.**
 - Postal Inspection Service at www.usps.com/postalinspectors. If you believe your mail was stolen or redirected, notify the Postal Inspector at your local post office.
 - Social Security Fraud Hotline at 1-800-269-0271. If you suspect someone is using your Social Security number for fraudulent purposes, call the hotline.
 - Department of Motor Vehicles (DMV) at www.dmv.org. If you believe someone is trying to get a driver's license or identification card using your name and information, contact your local DMV.
 - US Department of Justice at www.usdoj.gov
 - US Department of Treasury at www.treas.gov
 - Federal Deposit Insurance Corp at www.fdic.gov
- **Carefully review all your accounts.** Since identity theft takes time to completely resolve, you should continue to carefully review all charges and transactions appearing on account statements and online. Any discrepancies should be reported immediately.

We are providing this information as education on a topic that has received national attention. Please contact your Relationship Manager or Northern Trust Corporate Fraud Unit at 312-444-4648 for additional information.

northerntrust.com

MEMBERS FDIC EQUAL HOUSING LENDERS



Northern Trust

Q16757 (11/06)