

Banking Safely

Reminder: Home National Bank will never ask for your PIN or password over the telephone or by e-mail.

EMAIL FRAUD

Phishing (pronounced "fishing") is a form of criminal activity that employs social engineering techniques to acquire sensitive information such as passwords and credit card details. By masquerading as a trustworthy person or business in an apparently official electronic communication like e-mail, criminals use sophisticated lures to "fish" for users' financial information and passwords.

How to avoid getting hooked:

- ❑ Don't reply to email or click on pop-up messages that ask for personal or financial information and do not click on links in the message. Don't cut and paste a link from the message into our Web browser-the links may look as if they go one place, but actually it sends you to a different site. I site where they can get you hooked.
- ❑ 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". If you need to reach an organization or company that you do business with, call the number you have on record, the back of statements, or back of your card.
- ❑ Use anti-virus and anti-spy ware software, as well as a firewall, and update them regularly.
- ❑ Don't email personal or financial information period
- ❑ Review bank and credit card statements as soon as possible for any unauthorized transactions
- ❑ Be cautious about opening any attachments or downloading any files from emails you receive.
- ❑ If you have been scammed, visit the Federal Trade Commission's Identity Theft website at www.ftc.gov/idtheft

IDENTITY THEFT

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

Each year, millions of Americans have their identity stolen. While there is no foolproof way to avoid ID theft, there are steps you can take to minimize your chance of becoming a victim, and steps to take to minimize the damage should a theft occur.

The Federal Trade Commission, the nation's consumer protection agency, wants you to have the information you need to protect yourself against identity theft. This information is summed up in the FTC's clear and concise message on identity theft: **Deter, Detect, Defend.**

Deter identity thieves by safeguarding your information.

- Shred financial documents** and paperwork with personal information before you discard them.
- Protect your Social Security number.** Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information** on the phone, through the mail or over the Internet unless you know whom you are dealing with. Avoid disclosing personal financial information when using public wireless connections.
- Never click on links sent in unsolicited emails;** instead, type in a web address you know. Use firewalls, anti-spy ware and anti-virus software to protect your home computer; keep them up-to-date. If you use peer-to-peer file sharing, check the settings to make sure you're not sharing other sensitive private files. Visit **www.OnGuardOnline.gov** for more information.
- Don't use an obvious password** like your birth date, your mother's maiden name or the last four digits of your Social Security number.
- Keep your personal information in a secure place** at home, especially if you have roommates, employ outside help or are having work done in your house.

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make
- Charges on your financial statements that you *don't* recognize

Inspect: Your credit report. Credit reports contain information about you, including what accounts you have and your bill paying history.

The law requires the major nationwide credit reporting companies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report every 12 months if you ask for it. Visit • **www.AnnualCreditReport.com** or call 1-877-322-8228, a service created by these three companies, to order your free annual credit report. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

If you see accounts or addresses you don't recognize or information that is inaccurate, contact the credit reporting company and the information provider.

Defend against ID theft as soon as you suspect it.

- ❑ **Place a “Fraud Alert” on your credit reports, and review the reports carefully.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient:

Experian: • 1-888-EXPERIAN (397-3742)

TransUnion: • 1-800-680-7289

Equifax: 1-800-525-6285

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open and debts on your accounts that you can't explain.

- ❑ **Contact the security or fraud departments of each company** where an account was opened or charged without your okay.
Follow up in writing, with copies of supporting documents.
Use the ID Theft Affidavit at www.ftc.gov/idtheft to support your written statement.
Ask for verification that the disputed account has been dealt with and the fraudulent debts discharged.
Keep copies of documents and records of your conversations about the theft.
- ❑ **File a police report.** File a report with law enforcement officials to help you correct your credit report and deal with creditors who may want proof of the crime.
- ❑ **Report the theft to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.
Online: www.ftc.gov/idtheft
By phone: 1-877-ID-THEFT (438-4338) • or TTY, 1-866-653-4261
By mail: Identity Theft Clearinghouse, • Federal Trade Commission, Washington, DC 20580

Identity Theft Victims' Statement of Rights

Several federal laws protect victims of identity theft. These laws have to do with documenting the theft; dealing with credit reporting companies; dealing with creditors, debt collectors, and merchants; and limiting your financial losses caused by the theft of your identity. Here is a brief summary of the rights of identity theft victims, with links to websites that provide more information.

Documenting the Theft

You have the right to:

- File a report with a law enforcement agency and ask for a copy of it to show how your identity has been misused. This report is often called a [police report](#).

An [identity theft report](#) is a second kind of report. It is a police report with more detail. To be an identity theft report, it should have enough information about the crime that the credit reporting companies and the businesses involved can verify that you're a victim, and know which accounts or information have been affected. It's the report that will give you access to many of the rights described here.

The FTC's [ID theft complaint form](#) is a good place to start documenting the theft of your identity. This form asks you for the kind of detail that the identity theft report requires. Once you fill out this form online and print it, you can use it with the police report to create your [identity theft report](#).

Dealing with Credit Reporting Companies

You have the right to:

- Place a 90-day [initial fraud alert](#) on your credit files. You would do this if you think you are — or may become — the victim of identity theft. A fraud alert tells users of your credit report that they must take reasonable steps to verify who is applying for credit in your name. To place a 90-day fraud alert, contact just one of the three nationwide [credit reporting companies](#). The one you contact has to notify the other two.
- Place a seven-year [extended fraud alert](#) on your credit files. You would do this if you know you are a victim of identity theft. You will need to give an [identity theft report to each of the credit reporting companies](#). Each credit reporting company will ask you to give them some way for potential creditors to reach you, like a phone number. They will place this contact information on the extended fraud alert as a signal to those who use your credit report that they must contact you before they can issue credit in your name.
- [Get one free copy of your credit report](#) and a summary of your rights from each [credit reporting company](#). You can get these when you place a 90-day initial fraud alert on your credit reports. When you place an extended fraud alert with any credit reporting company, you have the right to two copies of that credit report during a 12-month period. These credit reports are in addition to the [free credit report](#) that all consumers are entitled to each year.
- Ask the credit reporting companies to [block fraudulent information](#) from appearing on your credit report. To do this, you must submit a copy of a valid [identity theft report](#). The credit reporting companies then must tell any creditors who gave them fraudulent information that it resulted from identity theft. The creditors may not then turn the fraudulent debts over to debt collectors.
- [Dispute fraudulent or inaccurate information](#) on your credit report with a credit reporting company. The credit reporting company must investigate your charges, and fix your report if they find that the information is fraudulent.

In many states, you have the right to restrict access to your credit report through a [credit freeze](#). A credit freeze makes it more difficult for an identity thief to open a new account in your name. Your [state attorney general's office](#) has information about using a credit freeze where you live.

Dealing with Creditors, Debt Collectors, and Merchants

You have the right to:

- Have a credit report free of fraudulent accounts. Once you give creditors and debt collectors a copy of a valid identity theft report, they may [not report fraudulent accounts](#) to the credit reporting companies.
- [Get copies of documents related to the theft of your identity](#) — for example, applications used to open new accounts or transaction records — if you give the company a valid [police report](#). You also can tell the company to give the documents to a specific law enforcement agency; that agency doesn't have to get a subpoena for the records.
- [Stop the collection of fraudulent debts](#). You may ask debt collectors to stop contacting you to collect on fraudulent debts. You also may ask them to give you information related to the debt, like the names of the creditors and the amounts of the debts.

In many states, you have the right to be notified by a business or organization that has lost or misplaced certain types of personal information. Contact your [state attorney general's office](#) for more information.

Limiting Your Loss From Identity Theft

Various laws limit your liability for fraudulent debts caused by identity theft.

- [Fraudulent Credit Card Charges](#): You cannot be held liable for more than \$50 for fraudulent purchases made with your credit card, as long as you let the credit card company know within 60 days of when the credit card statement with the fraudulent charges was sent to you. Some credit card issuers say cardholders who are victims of fraudulent transactions on their accounts have no liability for them at all.
- [Lost or Stolen ATM/Debit Card](#): If your ATM or debit card is lost or stolen, you may not be held liable for more than \$50 for the misuse of your card, as long as you notify the bank or credit union within two business days after you realize the card is missing. If you do not report the loss of your card promptly, your liability may increase.
- [Fraudulent Electronic Withdrawals](#): If fraudulent electronic withdrawals are made from your bank or credit union account, and your ATM or debit card has not been lost or stolen, you are not liable, as long as you notify the bank or credit union in writing of the error within 60 days of the date the bank or credit union account statement with the fraudulent withdrawals was sent to you.
- [Fraudulent Checks](#): Under most state laws, you are liable for just a limited amount for fraudulent checks issued on your bank or credit union account, as long as you notify the bank or credit union promptly. Contact your state banking or consumer protection agency for more information.
- **Fraudulent New Accounts**: Under most state laws, you are not liable for any debt incurred on fraudulent accounts opened in your name and without your permission. Contact your [state attorney general's office](#) for more information.

Other Federal Rights

Identity theft victims have other rights when the identity thief is being prosecuted in federal court. For example, under the Justice for All Act, the U.S. Department of Justice says identity theft victims have the right:

- To be reasonably protected from the accused;
- To reasonable, accurate, and timely notice of any public court proceeding, any parole proceeding involving the crime, or any release or escape of the accused;
- To not be excluded from any such public court proceeding unless the court determines that the identity theft victim's testimony would be materially altered if he or she heard other testimony at that proceeding;
- To be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding;
- To confer with the attorney for the government in the case;
- To full and timely restitution as provided in law;
- To proceedings free from unreasonable delay; and
- To be treated with fairness and with respect for his or her dignity and privacy.

