

- ▶ **Changing Your Address.** They divert your billing statements to another location by completing a change-of-address form.
- ▶ **Stealing.** They take wallets and purses. From mailboxes, they take bank and credit card statements, preapproved credit offers, new checks and tax information. They also take personnel records from their employers, or bribe employees who have access to these records.

Learn More

The Federal Trade Commission is the source for the information provided in this communication.

To learn more about identity theft and how to deter, detect and defend against it, visit ftc.gov/idtheft. Or request copies of identity theft resources by writing to:

Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave., NW, H-130
Washington, DC 20580



For more information:

Please stop in any conveniently located NBT Bank office.

Call **1-800-NBT-BANK (1-800-628-2265)**

Visit our website at nbtbank.com

E-mail our customer service representatives at customerservice@nbtbank.com

fighting identity theft



don't be the next victim...protect yourself

Fighting 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. The best way to fight identity theft is to follow these three steps: deter, detect and defend.

Deter

Deter identity thieves by safeguarding your information:



- ▶ **Shred financial documents** and paperwork containing 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.
- ▶ **Never click on links sent in unsolicited e-mails.** Instead, stick with web addresses you know and trust. Use firewall, antispyware and antivirus software to protect your home computer (and keep this software updated). Visit OnGuardOnline.gov for more information.
- ▶ **Don't use an obvious password**, such as 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

Detect suspicious activity by routinely monitoring your financial accounts and billing statements. Be alert to signs that require immediate attention:



- ▶ **Bills** that don't arrive as expected
- ▶ **Unexpected credit cards** or account statements

- ▶ **Denials of credit** for no apparent reason
- ▶ **Calls or letters** about purchases you didn't make

On a regular basis, 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 consumer-reporting companies—Equifax, Experian and TransUnion—to give you a free copy of your credit report each year if you ask for it.
 - Visit AnnualCreditReport.com, a service created by the three companies mentioned above, to order your free credit reports each year. You can also call 1-877-322-8228 or write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- ▶ **Your financial statements.** Review financial accounts and billing statements frequently, looking for charges you didn't make.

Defend

Defend against identity theft as soon as you suspect it:



- ▶ Place a "fraud alert" on your credit reports, and review these 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 of these companies is sufficient:

- Equifax: 1-800-525-6285
- Experian: 1-888-EXPERIAN (1-888-397-3742)
- TransUnion: 1-800-680-7289

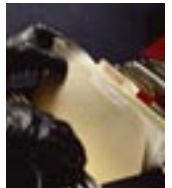
Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open and debts on your

accounts that you can't explain. If you notice these or other suspicious activities, do the following:

- ▶ **Close accounts.** Close any accounts that have been tampered with or established fraudulently.
 - Call the security or fraud departments of each company where an account was opened or changed without your approval. Follow up, in writing, with copies of supporting documents.
 - Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement.
 - Ask for verification that the disputed account has been closed 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 agencies to help you with creditors who may want proof of the crime.
- ▶ **Report the theft to the Federal Trade Commission.** Your report helps law enforcement agencies across the country in their investigations.
 - Online: ftc.gov/idtheft
 - By phone: 1-877-ID-THEFT (1-877-438-4338); the TTY number is 1-866-653-4261
 - By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

Common Identity Theft Techniques

Identity thieves use a variety of methods to steal your personal information, including:



- ▶ **"Dumpster Diving."** They rummage through trash looking for bills or other documents containing your personal information.
- ▶ **Skimming.** They steal credit card or debit card numbers by using a special storage device when processing your card.
- ▶ **Phishing.** They pretend to be financial institutions or companies and send spam (unsolicited e-mail) or pop-up messages to get you to reveal your personal information.