

## *Identify Theft*

### **Avoid Identity Theft**

*What is identity theft?*

Identity theft occurs when someone uses your personal information to obtain credit cards and loans or conduct other financial transactions in your name. These fraudulent transactions can affect your credit rating and finances if they are not identified and handled immediately.

*How can you avoid identify theft?*

### **How to Minimize the Risk of Identity Theft**

#### **1. Protect your Social Security Number (SSN), credit card and debit card numbers, PINs (personal identification numbers), passwords, and other personal information.**

Never provide this information in response to an unwanted phone call, fax, letter, or email, no matter how friendly or official the circumstances may appear.

To minimize the harm that arises from a lost or stolen wallet, carry only the identification, checks, credit cards, and debit cards you really need. The rest, including your Social Security card, are best kept in a safe place at home. Also, be extra careful if you have housemates or if you let others into your house, because they may find personal information and use it without your knowledge.

Likewise, do not preprint your Social Security number, phone number, or driver's license number on your checks. It is easy for someone who sees your check to copy this personal information and even sell it to an identity (ID) thief. Remember that you have the right to refuse requests for your SSN from merchants, because they may have other ways to identify you. If your Social Security number is on your driver's license, ask to use another number.

#### **2. Protect your incoming and outgoing mail**

Chances are that your mail carrier will deliver a credit card or bank statement, an envelope containing a check, or other items that can be very valuable to a thief. Or perhaps you will mail a check or papers containing account numbers or other personal financial information.

*For incoming mail:* Try to use a locked mailbox or other secure location, such as a Post Office (P.O.) box. If your mailbox is not locked or in a secure location, try to promptly remove mail that has been delivered or move the mailbox to a safer place. When ordering new checks, ask about getting the boxes delivered to your bank branch instead of having them mailed to your home and running the risk of finding them sitting outside your front door.

*For outgoing mail containing a check or personal information:* Deposit it in a U.S. Postal Service blue collection box, hand it to a mail carrier, or take it to the post office instead of leaving it in your doorway or home mailbox. A mailbox that holds your outgoing bills is a prime target for thieves who cruise neighborhoods looking for account information. Even worse is putting up the flag on a mailbox to indicate that outgoing mail is sitting there.

### **3. Sign up for direct deposit**

Sign up for direct deposit of your paycheck or state or federal benefits, such as Social Security. Direct deposit prevents someone from stealing a check out of your mailbox and forging your signature to access your money.

### **4. Keep your financial trash "clean"**

Thieves known as "dumpster divers" pick through garbage looking for pieces of paper containing Social Security numbers, bank account information, and other details they can use to commit fraud. Examples of valuable trash include insurance information containing your SSN, blank checks mailed by financial institutions with offers to "write yourself a loan," canceled checks, and bank statements.

Your best protection against dumpster divers? Before tossing out these items, destroy them, preferably using a crosscut shredder that turns paper into confetti that cannot easily be reconstructed.

### **5. Keep a close watch on your bank account statements and credit card bills**

Monitor these statements each month and contact your financial institution immediately if there is a discrepancy in your records, or if you notice something suspicious such as a missing payment or an unauthorized withdrawal. While federal and state laws may limit your losses if you are a victim of fraud or theft, your protections may be stronger if you report the problem quickly and in writing. Contact your institution if a bank statement or credit card bill does not arrive on time. Such missing mail could be a sign someone has stolen your mail and/or account information and perhaps has changed your mailing address to run up big bills in your name from another location.

### **6. Avoid ID theft on the Internet**

"Hackers" and scam artists are finding ways to steal private information transmitted over the Internet or stored on computer systems. You can protect yourself while shopping, banking, emailing, or surfing the Web. For example, never provide bank account or other personal information in response to an unsolicited email or when visiting a Website that does not explain how your personal information will be protected.

"Phishing" scams that arrive by email typically ask you to "update" your account information. However, legitimate organizations would not ask you for these details because they already have the necessary information or can obtain it in other ways. Do not respond to these emails, and do not open any attachments unless you independently confirm the validity of the request by contacting the legitimate organization the way you usually would, *not* by using the email address, Website, or phone number provided in the email. If you believe the email is fraudulent, consider bringing it to the attention of the Federal Trade Commission (FTC). If you do open and respond to a phony email, contact your financial institution immediately.

To get more information about computer security and safeguarding personal information, visit the Federal Trade Commission's Website at [www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm](http://www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm). For more about avoiding phishing scams, or to obtain a brochure with tips on avoiding identity theft, visit [www.fdic.gov/consumers/theft/](http://www.fdic.gov/consumers/theft/).

## **7. Exercise your rights under the Fair and Accurate Credit Transactions Act (FACTA) to review your credit record and report fraudulent activity**

Your credit report, which is prepared by a credit bureau, summarizes your history of paying debts and other bills. Credit reports are used by lenders, employers, and others who have a legal and legitimate need for the information. FACTA allows you to get one free credit report each year from each of the three major credit bureaus that operate nationwide – Equifax, Experian, and TransUnion – with just a single phone call, letter, or electronic request. This is a change from previous law, because you can get a copy even if you do not suspect ID theft or any other problem with your credit report. (See more details at [www.annualcreditreport.com](http://www.annualcreditreport.com), or call 877-322-8228.)

After you get your credit report, look for warning signs of actual or potential ID theft. These include mention of a credit card, loan, or lease you never signed up for and requests for a copy of your credit record from someone you do not recognize (which could be a sign that a con artist is snooping around for personal information).

## **8. Get more information**

Visit the Federal Trade Commission Website: [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/), or call 877-IDTHEFT (438-4338)

## **What to Do if You Suspect You Are a Victim of Identity Theft**

The FTC recommends the following actions if you believe you are a victim of identity theft. You can also call the FTC's Identity Theft Hotline at 877-IDTHEFT (438-4338) or visit <http://www.ftc.gov/idtheft/>.