

# IDENTITY THEFT AND FRAUD

## *DETER, DETECT, PREVENT*

As one of the fastest growing crimes in the U.S., identity theft is a significant issue for financial institutions and a risk that every NASB employee and customer must be constantly aware of and continuously seeking to deter and detect.

Identity theft is a federal crime. It occurs when one person's identification (which can include name, social security number, or any account number) is used or transferred by another person for unlawful activities.

### *What Identity Thieves Do with Your Information*

Identity thieves seek to open new accounts in your name. They often apply for new credit cards using their victim's personal information, make charges, and leave the bills unpaid. It is also common for them to set up telephone or utility service in their victim's name and not pay for it. Some victims have found that identity thieves applied for loans, apartments, and mortgages. Thieves have also been known to print counterfeit checks in a victim's name.

Identity thieves also seek to gain access to your existing accounts. They want to steal money from your bank accounts, make charges on your credit cards, and use your checks and credit to make down payments for cars, furniture, and other expensive items. They may even file for government benefits including unemployment insurance and tax refunds using your social security number.

### *How Identity Theft Happens*

It is not uncommon for identity theft to go undetected for months and even years. Victims of identity theft may not realize that their identity has been stolen until they are denied credit or until a creditor attempts to collect an unpaid bill. Most victims have no idea how the identity thief obtained their personal information.

## **PURSE/WALLET THEFT**

Among those who think they know what happened, many believe the identity theft occurred when their purse or wallet was stolen or lost.

## **DUMPSTER DIVING**

Dumpster diving involves rummaging through trash to obtain your personal information. Identity thieves can rummage through interior office trash cans or through exterior dumpsters. Either way, the objective is to gather information that has been carelessly thrown away.

## **SHOULDER SURFING**

Shoulder surfers are identity thieves that acquire personal information through eavesdropping. They may be listening when you provide your account number or

**This information will help you understand what identity theft is, how it happens, how to protect yourself, and what steps to take if your identity is stolen.**

Social Security Number to the bank teller. They may stand behind your desk and observe your computer screen when you log in to Online Banking.

## **MAIL THEFT**

Thieves steal mail from unlocked mailboxes to obtain newly issued debit cards, bank or insurance statements, investment reports, benefits documents or tax information. Unfortunately, even locked mailboxes may not stop the most determined thief.

## **GROUP THEFT**

Group identity theft has become a major problem for consumers. A thief gains access to a place that keeps records for many people. Targets have included stores, fitness centers, car dealers, schools, hospitals, and even credit bureaus. Thieves may either use the stolen identities themselves or sell them to other criminals.

## **PERSONS KNOWN TO YOU**

Victims of identity theft often find that someone they know has committed the crime. Roommates, hired help, and landlords all have access to your home, and it is possible for them to access private information. Identity theft within families is also fairly common. This causes particular difficulties, because victims may be reluctant to notify the authorities or press charges. People are especially vulnerable to identity theft when ending relationships with roommates and spouses.

## **PRETEXT CALLING**

Pretext calling is the act of creating and using an invented scenario (the pretext) to persuade the victim to release confidential information or perform an action. Identity thieves will contact you through the mail, telephone, or e-mail, and attempt to get you to reveal your personal information, usually by asking you to "verify" some data.

Pretext callers may even go so far as to use a Caller ID spoofing service to adopt the phone number of the business or person they are attempting to impersonate.

## ***Types of Online Fraud***

With the growth of online banking comes online fraud. These schemes vary from web sites that "look" like the actual financial institution to email asking for personal banking information.

## **PHISHING/VISHING SCAMS**

Phishing involves identity thieves sending a seemingly legitimate e-mail request for account information, often under the guise of asking you to verify or reconfirm confidential personal information such as account numbers, social security numbers, passwords and other sensitive information. Many times a sense of "urgency" is added to the e-mail by including a statement that your account will be terminated unless a response is made.

Similar to phishing, vishing involves sending a seemingly legitimate e-mail or text message, indicating you should contact the bank to, for example, reactivate your debit card. On calling the telephone number, you are greeted with a welcome message and asked to enter your social security number and/or debit card number in order to resolve a 'pending security issue'.

The ultimate goal of phishing and vishing is to use the information you provided to gain unauthorized access to your bank account or to engage in illegal acts such as opening a new account in your name.

## **SPYWARE/MALWARE**

Home computers can be infected with viruses that transmit your data to cyber-thieves using a software application that is remotely installed on your computer without you knowing. This special snoopware lets the thief access everything you do online, including your user ids and passwords. Be wary of email attachments and websites you don't know.

## ***How to Avoid Being a Victim of Identity Theft***

### **PROTECT YOURSELF**

- (1) Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. E-mails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you did not initiate the communication, you should not provide any information.
- (2) If you believe the contact may be legitimate, contact the financial institution yourself. You can find phone numbers and Web sites on the monthly statements you receive from your financial institution, or you can look the company up in a phone book or on the Internet. The key is that you should be the one to initiate the contact, using contact information that you have verified yourself.
- (3) Never provide your password over the phone or in response to an unsolicited Internet request. A financial institution would never ask you to verify your account information online. Thieves armed with this information and your account number can help themselves to your savings.
- (4) Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving, call your financial institution to find out why. If your financial institution offers electronic account access, periodically review activity online to catch suspicious activity.
- (5) Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.
- (6) Never click on the link provided in an e-mail you believe is fraudulent. It may contain a virus that can contaminate your computer.
- (7) Do not be intimidated by an e-mail or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- (8) If you believe the contact is legitimate, go to the company's Web site by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the e-mail.
- (9) Report suspicious e-mails or calls to the Federal Trade Commission through the Internet at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or by calling 1-877-IDTHEFT.

## *What to do if you suspect you're a victim*

If you fall victim to an attack, act immediately to protect yourself.

- (1) **Alert your financial institution.**
- (2) **Learn more about identity theft and how to protect yourself** by visiting the U.S. Federal Trade Commission's (FTC) website at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or, by calling their toll-free number at (877) 438-4338.
- (3) **Monitor your credit files** by requesting a free copy of your credit report by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), or by calling (877) 322-8228, or by writing Annual Credit Report Request Service at P.O. Box 105281, Atlanta, GA 30348-5281.
- (4) **Carefully examine account statements** to verify charges and activity. If anything looks suspicious, promptly report the incident to the financial institution as suspected identity theft.
- (5) If you have disclosed sensitive information in a phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to **place a fraud alert on your file**, which will help prevent thieves from opening a new account in your name. Here is the contact information for each bureau's fraud division:

Equifax  
800-525-6285  
P.O. Box 740250  
Atlanta, GA 30374

Experian  
888-397-3742  
P.O. Box 1017  
Allen, TX 75013

TransUnion  
800-680-7289  
P.O. Box 6790  
Fullerton, CA 92634



Report all suspicious contacts to the Federal Trade Commission through the Internet at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or by calling 1-877-IDTHEFT.