IDENTITY THEFT

OUTSMARTING THE CROOKS

DVD Companion Learning Guide

How to Use This Learning Guide

This learning guide is a companion to the *DVD*, "Identity Theft: Outsmarting the Crooks"

- **It can be used to guide classroom discussion of the material presented in the *DVD***

--or--

- ***As general reference materials.***

We All Have a Role to Play In Combating Identity Theft

The fight against Identity Theft involves cooperation by:

- Federal and State government
- Law enforcement
- Financial institutions and businesses
- Technology innovators
- Consumers

IDENTITY THEFT

OUTSMARTING THE CROOKS

What is Identity Theft?

A Legal Definition

- Under the Fair and Accurate Credit Transactions Act of 2003, Identity Theft means:

"A fraud committed or attempted using the identifying information of another person without authority."

16 CFR § 603.2

Scope of Identity Theft

- In 2004, victims spent nearly 250 million hours trying to sort out bogus accounts and set their credit records straight

Common Types of Identity Theft or Financial Fraud

- Unauthorized transactions on existing accounts (e.g., unauthorized charges on a credit card or checks on a checking account) – often more easily corrected than the others
- Takeover of existing accounts (e.g., prolonged use or emptying of a financial account)
- Creation of new accounts

Warning Signs

- A financial institution may call if a transaction seems out of the ordinary
- You may see unauthorized charges on a credit card or checking account statement
- You may see an account that you did not open on your credit report
- You may get a call from a collection agency asking why you have not paid a bill

Identity Thieves Look For:

- Name
- Address
- Date of birth
- Social Security number
- Driver's license number
- Mother's maiden name
- Account numbers
- Card expiration dates
- Internet passwords
- Personal identification numbers
- User IDs for online account access
- Security codes from the back of credit and debit cards
- Other identifying information

How Your Identity Can Be Stolen

- Loss or theft of your wallet, purse, or credit card
- Mail theft
- Skimming information from the magnetic strip on credit or debit cards
- “Dumpster diving” through the trash
- “Shoulder surfing,” looking over your shoulder when you are entering a PIN or password

How Your Identity Can Be Stolen

- Eavesdropping
- Impersonation
- Scam phone calls where a stranger asks for personal or financial information
- Computer hacking
- “Phishing” e-mails
- Spyware

Phishing

Uses spam or junk e-mails that:

- Seek to obtain the same kind of information that any ID thief wants (see page 9)
- May mimic:
  - Financial institutions
  - Government agencies
  - Computer software companies
  - e-Commerce sites
  - Other legitimate businesses
- May ask you to go to a Web site to verify and enter your personal information
- May contain a link that takes you to a Web site that looks just like your bank's

Phishing and Spyware

More on Phishing:

- At the fake Web site, crooks copy, or "spoof," graphics from real Web sites
- The message may include an excuse (*e.g.*, the bank is undergoing a computer upgrade), or sound urgent or intimidating (*e.g.*, you will lose access to your account if you don't provide the information promptly)

Spyware software:

- Monitors your online activity and diverts information while you are using legitimate Web sites
- May be installed on your computer when you visit deceptive Web sites, download seemingly innocent games or other software, or open e-mails that may have spyware attached

What Financial Institutions are Doing to Fight Back

Financial institutions are:

- Developing and implementing new technologies to improve online and physical security of information and communication
- Complying with new regulatory requirements and enhancing procedures to prevent, find and fight Identity Theft
- Educating consumers about how to protect themselves
- Providing assistance to victims of Identity Theft
- Cooperating with local, state and federal law enforcement to investigate the crime and prosecute the thieves

What Law Enforcement is Doing to Stop the Thieves

Law enforcement is:

- Working closely with business, the financial sector, and consumers to identify and investigate the crimes and criminals
- Breaking up crime rings – domestic and international
- Shutting down Web sites used by criminals
- Training more officers at all levels, including local police officers, to recognize and follow up on identity theft

What Law Enforcement is Doing to Stop the Thieves

- Prosecuting criminals, including more felony prosecutions

- Obtaining longer sentences

  The Identity Theft Penalty Enhancement Act allows for a minimum 2 year Identity Theft sentence in addition to sentences for the other underlying offenses (*i.e.*, mail fraud)

IDENTITY THEFT

OUTSMARTING THE CROOKS

What You Can Do To Protect Yourself

Check Your Credit Report

- Check your credit report at least once a year
  - To see whether accounts have been opened in your name without your knowledge
  - To spot unexpected delinquency on established accounts
  - To review your credit report before making a major purchase

- These reports can be free and are easy to get

  Contact: www.AnnualCreditReport.com for a free credit report once every 12 months from each of the three nationwide consumer reporting agencies *(i.e.,* "credit bureaus"): Equifax, Experian, TransUnion

Steps to Catch Identity Thieves

- Monitor your online financial accounts frequently
- Promptly review your other bank statements, credit card statements, and other bills
- Quickly call the financial institution or company if you see anything suspicious and follow up in writing
- Sign your new credit and debit cards promptly

Protect Your Information

- Do not leave a lot of financial records lying around your house for prying eyes to see
- Do not keep information that you don't need in your purse or wallet
- Do not leave credit or debit card receipts at the ATM, gas pump, or anywhere else
- Do not keep personal identification numbers attached to credit, debit, or ATM cards

Protect Your Information

- Shred personal records or get rid of them as effectively as possible
- Beware of giving information to anyone over the phone or Internet unless you initiate the contact
- Remember that your bank or credit card issuers already have your account numbers, PINs, access codes, passwords, Social Security numbers and other information they need. They won't phone or e-mail you to ask for it.
- Protect your mail – send and receive it safely

Protect Your Social Security Number

- Do not carry around your Social Security number
- Do not give the number to others just because a merchant or someone else says he or she needs it
- Ask questions before deciding whether to give it out - Why it is needed? How it will be protected?
- Remember, financial institutions will need your Social Security number – for tax reporting and other identifying purposes

Income Tax-Related Identity Theft

- Your Social Security number can be used by identity thieves to file a false tax return and get a refund using your name
- Your Social Security number could be used by someone to get a job and report income that you didn't know about
- If you do not prepare your own income tax return, be very careful in choosing a tax preparer

Income Tax-Related Identity Theft

- If you receive a notice from the IRS that leads you to believe someone may have used your social security number fraudulently, respond immediately either by phone or in writing as directed in that notice
- IRS tax examiners will work with you and other agencies such as the Social Security Administration to help resolve these problems
- **www.irs.gov**
- 1-877-777-4778

On-Line Safety

- Generally, you can operate safely on the Internet, but you need to use common sense
- Protect your computer like you would protect your personal financial information.
- Turn it off when you walk away from the computer so that no one else can gain access while you are not there
- Use a firewall
- Make sure that your operating system and software are updated on a frequent basis (keep patches current)

On-Line Safety

- Make sure that you have anti-spam software—many phishing attacks come as a result of spam
- Use strong passwords
  - Words or numbers that are not easy to guess
  - Use a combination of numbers, letters, and other characters
- Do not use the same password for every account. Consider changing your passwords periodically.

On-Line Safety

- Know the Web address—or “URL”—of the Web site that you are going to visit
- Read and learn how the Web site is going to protect and use your personal information
- Clean your hard drive before you dispose of an old computer

Protect Yourself from Phishing

- Update your browers, spam filters, anti-virus and anti-spyware software regularly
- Use parental controls
- Visit a Web site by typing the Web address - or URL – into your Web browser yourself, not by clicking a link
- Look for the “s” in “https” when engaging in financial transactions because it indicates scrambling or encryption of the communication (don’t just copy a link that appears to have an “s” in “https”)
- Look for the lock icon in the lower right corner of the screen when engaging in financial or other sensitive transactions because the lock signifies an encrypted session (Spoofed phishing sites may have fake locks, so beware)
- More information on Phishing is available at:
  - **www.SecretService.gov**
  - **www.Antiphishing.org**
  - **www.FTC.gov**

Spyware

- To fight spyware, use anti-spyware software
- Set parental controls so the user has to log in on that setting to protect children
- Keep current with other software updates and patches

Avoid Mail Theft

- Many American mailboxes are vulnerable because they have no locks and are located at the end of a drive or walkway, or at the curbside
- Identity thieves know that unsecured mail boxes may contain easy and valuable pickings for them because the mail may include:
  - Credit cards
  - Credit card statements
  - Bank statements
  - Bank checks
  - Credit card convenience checks
  - Insurance policies
  - Mortgage documents
  - Driver's licenses
  - Other material with important information

Secure Your Mail

- Take your incoming mail out of the mailbox as soon as possible
- Consider getting a mail box with a lock or using a Post Office box (P.O. Box)
- Put your outgoing mail in a blue, United States Postal Service collection box on a street corner, or
- Hand it to your letter carrier directly, or
- Bring it to the Post Office
- If you put it in your mailbox, remember that putting the red flag up alerts the thieves as well as the mail carrier that there is outgoing mail
- If you think you are an identity theft victim and the mail is involved, contact www.usps.com/postalinspectors

What To Do If You Are, Or Think You May Be, A Victim

"Must Do" List – Act Quickly

1. Contact the financial institutions or the companies where the information about you has been misused and let them know that you're a victim of Identity Theft

2. Contact the credit reporting agencies (Equifax, Experian, TransUnion) to report your suspicions about Identity Theft, and request a fraud alert

"Must Do" List – Act Quickly

3. Contact your local police department to report the crime, and get a copy of your police report

4. Contact the Federal Trade Commission for helpful information and because the FTC tracks incidents of Identity Theft

Contact a Financial Institution

- Most financial institutions have specially trained agents to help you
- They will investigate the circumstances
- They should take the suspect charges off the account, pending investigation
- They will reissue cards, PINs, access codes and passwords, and close accounts, as necessary
- They will need a written report of what you are claiming

Contact the Credit Bureaus

- Contact the credit bureaus immediately when you find out you are a victim of Identity Theft to place a fraud alert in your credit report
- You also may want to contact the credit bureaus to place a fraud alert if you feel like you may become a victim of Identity Theft (*e.g.*, your wallet containing identifying information has been stolen)
- The fraud alert on your credit file signals to would-be creditors to do extra verification before they grant credit in your name

Contact the Credit Bureaus

- You only need to notify one of the three nationwide credit bureaus; it will notify the other two to place a fraud alert
- Carefully review your credit reports to make sure that there are no fraudulent accounts opened in your name or other errors
- After the fraud alert is in place, the credit bureaus will also make available to you a free copy of your credit report

Fraud Alert Contact Information

For fraud alerts:

www.equifax.com

1-888-766-0008

www.experian.com

1-888-397-3742

www.transunion.com

1-800-680-7289

- Full contact information available at the end of the Companion Learning Guide

Contact Law Enforcement

- File a police report with the local police or sheriff to document your situation
- Be persistent. Consider contacting State or Federal law enforcement, if necessary
- Provide any evidence you may have when you contact the police
- Get a copy of your police report to establish that you are a victim of a crime and to help you repair your credit record

Contact the FTC

- The Federal Trade Commission has a wealth of information for consumers who find themselves victimized by Identity Theft **www.consumer.gov/idtheft**

- The FTC shares collected data with 1400 law enforcement agencies around the country. To report the crime by phone, call 1-877-IDTHEFT

Active Duty Alert

A consumer in military service who is on active duty or is a reservist performing duty under a call or order to active duty and is assigned to service away from the consumer's usual duty station is permitted to place an active duty alert in his or her consumer report maintained by a nationwide consumer reporting agency for 12 months, with the possibility of renewal.

- One call to one of the three nationwide credit bureaus will be sufficient to place active duty alerts with all three
- The alert will signal to lenders, insurers, or employers to scrutinize any applications carefully to ensure that it comes from the consumer and not an imposter
- The active duty alert can prevent pre-screened offers of credit and insurance being sent while the consumer is away on active duty

Public Law 108-159

16 CFR §613.1

Tips for Identity Theft Victims

- Keep good records (e.g., the names and telephone numbers of the people you talk to, summaries of conversations, documentary evidence of the crime)
- Consider using the FTC's standard affidavit and sample form letters for contacting credit reporting agencies, available at: www.consumer.gov/idtheft
- Filing the police report also allows you to block the identity theft accounts in your credit report, and makes it easier to get documents used to open the fraudulent identity theft accounts
- The police report will support your request for the 7-year fraud alert available to proven victims

Debt Collection

- Sometimes people find out that they are a victim of Identity Theft when they are contacted by a debt collector
- Ascertain the details about the debt and the collector (i.e., who is calling and the nature of the debt)
- Determine the company that referred the debt to the debt collector

Debt Collection

- Contact both the debt collector and the company on whose behalf they are collecting and dispute the account
- You will probably have to send them a copy of the police report
- Document that they have resolved the debt and that you are no longer being held liable for the account on which they are trying to collect

IDENTITY THEFT

OUTSMARTING THE CROOKS

How To Get Credit Reports

Obtain Your Credit Report

Free Annual Credit Report available once every 12 months via a centralized contact point:

- www.AnnualCreditReport.com
- 1-877-FACT ACT or 1-877-322-8228
- Annual Credit Report Request Service
  P.O. Box 105281
  Atlanta, GA 30348-5281

- See Web site, FTC Brochure, or Resource Library for the necessary form for a postal request

More About How To Get Credit Reports

- Other conditions under which you can request a free report from any credit bureau:
  - If you are unemployed and seeking employment,
  - If you receive public welfare assistance, or
  - If you believe information in your credit file is incorrect due to fraud
- Request a free report for these reasons from any consumer reporting agency by contacting them directly

Adverse Action Notices

- If your application for credit or insurance is denied, the company that denied the application based in whole or in part on information contained in a credit report must provide an adverse action notice
- The notice will tell you how you can request a free credit report from the appropriate credit bureau

More About Credit Reports

- You can buy your credit report at any time
- You can subscribe to credit monitoring services

Obtain Your Credit Report

Equifax:

Free Reports, due to: •adverse action •unemployment •receiving public benefits •errors due to fraud •State law provision	*One-Call Fraud Alerts, Active Duty Military Alerts, and Access to Free Credit Report*	*Purchase Your Credit Report*
www.equifax.com **1-800-685-1111** **Equifax Information Services LLC** **P.O. Box 740241** **Atlanta, GA 30374**	**www.equifax.com** **1-888-766-0008** **Equifax Credit Information Services** **Consumer Fraud Division** **P.O. Box 740256** **Atlanta, GA 30374**	**www.equifax.com** **1-800-685-1111** **Equifax Information Services LLC** **P.O. Box 740241** **Atlanta, GA 30374**

Obtain Your Credit Report

Experian:

Free Reports, due to:	*One-Call Fraud Alerts, Active Duty Military Alerts, and Access to Free Credit Report*	*Purchase Your Credit Report*
•adverse action •unemployment •receiving public benefits •errors due to fraud •State law provision		
www.experian.com **1-866-200-6020** **Experian** **P.O. Box 2104** **Allen, TX 75013**	**www.experian.com** **1-888-397-3742** **Experian's National Consumer Assistance** **P.O. Box 2002** **Allen, TX 75013**	**www.experian.com** **1-888-397-3742** **Experian** **P.O. Box 2104** **Allen, TX 75013**

Obtain Your Credit Report

TransUnion:

Free Reports, due to:	*One-Call Fraud Alerts, Active Duty Military Alerts, and Access to Free Credit Report*	*Purchase Your Credit Report*
•adverse action •unemployment •receiving public benefits •errors due to fraud •State law provision		
www.transunion.com **1-800-888-4213** **P.O. Box 1000** **Chester, PA 19022**	**www.transunion.com** **1-800-680-7289** **Fraud Victim Assistance Department** **P.O. Box 6790** **Fullerton, CA 92834**	**www.transunion.com** **1-800-888-4213** **P.O. Box 1000** **Chester, PA 19022**

The FACT Act

The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act" or "FACTA") provides new tools to help consumers combat and recover from Identity Theft. These include:

- Free credit reports if you believe you are a victim of Identity Theft or may become one
- Placing a fraud alert or active duty alert on your credit report
- Stopping information that is the result of Identity Theft from being passed along by credit bureaus, financial institutions, businesses, and debt collectors

See the Resource Library for more information on the FACT Act