TALKING ABOUT IDENTITY THEFT:
A HOW-TO GUIDE

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

TABLE OF CONTENTS

TALKING ABOUT IDENTITY THEFT: A HOW-TO GUIDE

1. GUIDE OVERVIEW

1. GUIDE OVERVIEW

Talking About Identity Theft: A How-To Guide contains step-by-step instructions for **any** organization—large or small, business, community or social—to help its members, employees or audience learn more about identity theft.

This guide was developed by the Federal Trade Commission (FTC), the nation's consumer protection agency, as part of its ongoing work to educate consumers about identity theft. You may find it helpful to first view the guide's companion DVD, *Deter, Detect, Defend*, a brief video that provides an informative overview. This effort focuses on what each of us can do to make a difference, and specifically what you can do to make a difference.

While there are no guarantees about avoiding identity theft, it's important for you to know how to:

- **Deter** identity thieves by safeguarding your personal information.
- **Detect** suspicious activity by routinely monitoring your financial accounts and billing statements.
- **Defend** against identity theft as soon as you suspect a problem.

Awareness is among the most powerful tools in the fight against identity theft. And that's where you play an important role.

The more you know how to protect your identity and what to do if a problem occurs, the harder it is for identity thieves to commit their crimes.

By educating audiences at work, in your community, at your place of worship or anywhere else, you can help the people you care about:

- Save time and money by reducing their risk of being victimized, detecting any problems quickly and knowing what to do.
- Avoid or reduce the emotional stress that often comes with identity theft.
- Enjoy the peace of mind that comes from better understanding this issue, and knowing how to **take action**.

Talking About Identity Theft: A How-To Guide provides you with what you need to be an effective communicator about identity theft.

Here, you will find advice and guidance on how to get the word out by organizing a meeting and by reaching out to your local media, and the materials you need, from speeches and presentations to press releases.

All the materials, including the guide itself, are available in both English and Spanish.

Talking About Identity Theft: A How-To Guide is one part of the FTC's ID Theft Consumer Education Kit. The kit also includes:

- *Deter, Detect, Defend*, an educational DVD
- *Deter, Detect, Defend*, a consumer brochure
- *Take Charge: Fighting Back Against Identity Theft*, a guide for ID theft victims

In addition, the FTC has more comprehensive information available for consumers at **ftc.gov/idtheft**. Please refer to section 9 of this booklet, *Additional Resources*, for more information.

2. IDENTITY THEFT: AN INTRODUCTION

2. IDENTITY THEFT: AN INTRODUCTION

a. What is identity theft?

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

The Federal Trade Commission (FTC) estimates that as many as 10 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft.

Maybe thieves rummaged through your trash, found a bank statement, and misused your checking account. Or, maybe they rented an apartment using your name. Maybe someone got a credit card using your identity and credit history, and bought expensive stereo equipment. The crime takes many forms.

And maybe you found out about it months later, when your loan application was rejected or when you noticed charges on your credit card statement that you didn't make.

Identity theft is serious. People whose identities have been stolen can spend hundreds of dollars and dozens of hours cleaning up the mess thieves have made of their good name and credit record.

Consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports. They may even be arrested for crimes they did not commit. The potential for damage, loss, and stress is considerable.

b. How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information—your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.

Skilled identity thieves may use a variety of methods to get hold of your information:

- They may steal your mail, wallet or purse.
- They may get personal information from you by posing as legitimate companies through email, in a practice known as "phishing." Or they might lie to you on the phone.
- They may take your information from businesses or other institutions by stealing personnel records, bribing or conning an employee who has access to these records, or breaking into your records electronically.

Some identity theft victims even report that their information has been stolen by someone they know.

c. What do thieves do with a stolen identity?

Once they have your personal information, identity thieves go about their business in a variety of ways.

Credit card fraud:

- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear under your name—on your credit report.

- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

Phone or utilities fraud:
- They may open a phone or wireless account, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

Bank/finance fraud:
- They may open a bank account in your name and write bad checks.
- They may authorize electronic transfers in your name from your accounts, and drain your savings.
- They may take out a loan in your name.

Government documents fraud:
- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name to get government benefits.
- They may file a fraudulent tax return using your information.

Other fraud:
- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

d. How can you find out if your identity was stolen?

Many consumers learn that their identity has been stolen **after** some damage has been done.
- You may find out when bill collection agencies contact you for overdue debts—debts you never incurred.
- You may find out when you apply for a mortgage or car loan—and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft.

e. What should you do if your identity is stolen?

Repairing the damage caused by identity thieves may take time and money. Filing a police report, notifying creditors, and disputing any unauthorized transactions are steps you **must** take to restore your good name. More specific information on what to do is in section 4 of this guide, and in the FTC's guide, *Take Charge: Fighting Back Against Identity Theft*. Repairing the damage can be a costly, time-consuming, and stressful process.

And the more time that goes by before you detect the problem, the more time it may require to resolve it.

f. What can you do to help fight identity theft?

A great deal.

Awareness is an effective weapon against identity theft. Awareness of how information is stolen—and what you can do to protect yours. Awareness of the need to monitor your personal information to uncover any problems—quickly. And, awareness of what to do when you suspect your identity has been stolen.

Armed with the knowledge of how to protect yourself and take action, you can make identity thieves' jobs much more difficult. The following sections of this guide give specific steps you can take to protect your information, as well as ways you can help educate others.

3. WHAT EVERYONE SHOULD KNOW: DETER, DETECT, DEFEND

While nothing can guarantee that you won't become a victim of identity theft, you can take specific steps to minimize your risk, and minimize the damage if a problem develops. These steps make it more difficult for identity thieves to steal your identity.

It's about following the "3 D's" of identity theft protection—*Deter, Detect, Defend*.

DETER

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 have initiated the contact and know who you are dealing with.
- **Never click** on links sent in unsolicited emails; instead, type in a Web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit **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

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

Be alert to signs that require immediate attention:

- Mail or 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

Inspect:

- **Your credit report.** Credit reports have 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 **www.AnnualCreditReport.com** or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

DEFEND

Defend against identity theft as soon as you suspect a problem.

- **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 certain 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:
  - **Equifax:** 1-800-525-6285
  - **Experian:** 1-888-EXPERIAN (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.

- **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 okay. 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 written 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 officials to help you with creditors who may want proof of the crime.

- **Report your complaint to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.
  - Online: **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

4. WHAT YOU CAN DO: DETER, DETECT, DEFEND

4. WHAT YOU CAN DO: DETER, DETECT, DEFEND

Deter, Detect, Defend is a phrase that can help the people you care about remember how to guard against identity theft.

Raising awareness about these three actions—and the steps involved—can make it more difficult for identity thieves to target people, whether they're at your office, in your neighborhood, within your favorite organization, or at your place of worship. Whether you share this information with five people or 50, you will make a difference.

How much you do is up to you. Want to give a speech? Grab the enclosed speech and go! Don't like public speaking much? Pop in the DVD included in this kit and hit play. Only have a minute at the end of a busy meeting on another subject? Hand out photocopies of the consumer brochure. **Whatever** action you take can help fight identity theft.

The people you reach will have a better understanding of how identity thieves work, how to reduce their risk of identity theft, and what to do if they suspect a problem. They will appreciate your leadership and effort.

You can promote Deter, Detect, Defend in many ways at work, in your community, or through the media. The following three sections of this guide will show you how to get the word out.

5. GETTING THE WORD OUT—AT WORK

5. GETTING THE WORD OUT—AT WORK

You have identified your workplace as one way to get the word out on identity theft. Here are step-by-step instructions on how to educate your fellow employees to *Deter, Detect, Defend* against identity theft.

1 STEP ONE: Check with your employer

Before undertaking any program to educate your colleagues at work, it's important to check in with your employer or supervisor.

Let your employer know that you are interested in sharing information with others in your organization about reducing their risk of identity theft, and learning what to do if they suspect a problem.

For those who have had their identities stolen, the recovery process can take time and cause considerable stress. The process of "restoring your good name" can result in a loss of time and productivity at work. Helping employees fight identity theft makes good business sense.

2 STEP TWO: Send a *Deter, Detect, Defend* email

Depending on where you work, email can be a quick and effective way to educate others about identity theft:

- Pick a time when people may be focused on their finances, such as the start of a new year, the return to work after a holiday or summer vacation, or "tax day," April 15th. Or, keep an eye on the news for a major identity theft story in the headlines.
- Using a season, a day, or an event as a "hook," send an email to your fellow employees on identity theft and ways to reduce their risk (*Deter, Detect, Defend*). See sample *Email to Employees*, in section 8 of this guide.
- Include a web link in the email where employees can get more information: **ftc.gov/idtheft**.

3 STEP THREE: Distribute the *Deter, Detect, Defend* brochure

- Order additional copies of the brochure—free of charge—from the FTC, at **ftc.gov/order**.
- Make your own copies of the brochure on a copy machine.
- Once you have sufficient copies of the brochure for your audience, arrange for each employee to receive one.

4 STEP FOUR: Post the *Deter, Detect, Defend* brochure

Posting information in a common area at your workplace is a great way to educate your fellow employees on how to Deter, Detect, and Defend against identity theft, and encourage conversations about the subject.

- Pick a place that has heavy traffic—a lunch or break room, kitchen, library, restroom, or a waiting area.
- Use the *Deter, Detect, Defend* brochure (included in the ID Theft Consumer Education Kit) as your "poster." The brochure has information on both sides, so you'll need to copy the back side to display all the information.
- Put your business card near the brochure, or write your phone number on it to let others know you are available as a resource.

5 STEP FIVE: Host a meeting at work

Identity theft is an important issue. People are interested in learning more—in particular, more about what they can do to minimize their risk and any potential damage.

You can plan a meeting that will raise awareness among one group of people, at the right time, with the right message.

a. Choosing the place:

Chances are you attend many meetings at work. If so, you know that the first step is choosing and reserving the meeting location room. When you try to find a meeting space, consider:

- How many people are likely to attend?
- When is it available and for how long on a single, specific day?
- Will your event work best with auditorium-style seating (rows of chairs facing the front of the room) or is it small enough to accommodate a discussion-style arrangement, like a circle of chairs?
- What technology does the room have? Does it allow you to use a PowerPoint presentation or video? Does it have a sound system? If your business has an information technology (IT) specialist, he or she may be able to help you with these questions.

b. Choosing the time:

The timing of an event is as important as the location. Think about the people at your business who are likely to attend. Consider:

- What are the most busy or least busy times of day?
- Do people prefer meetings before, during, or after work? What about the company's management?
- Is anything else going on that might compete for attention, such as a major project deadline?

Quick Tip—If you are unsure about timing, check with a few people who are part of your business. Sound them out on what time would be best for the group overall.

Quick Tip—In general, working an identity theft educational session into an existing, regularly scheduled meeting (such as a lecture series or monthly staff meeting) delivers the greatest impact with the least effort.

c. Announcing the meeting:

Many activities can build interest in your identity theft meeting. For example:

- Distribute flyers or e-vites to your fellow employees. See sample *Meeting Invitation Flyer*, in section 8.

Quick Tip—Think about how you hear about meetings or other events—and what works best in your organization. Most people look to one to two different sources for information and updates: Make sure you take advantage of those.

- Place a notice in your company's newsletter or bulletin, two to three weeks before the event, with a follow-up reminder as close to the event as possible. See sample *Newsletter Blurb,* in section 8.
- Send an email announcement two weeks in advance, with a reminder the day before. See sample *Email Invitation to Meeting*, in section 8.
- Place a notice on your website or your organization's "Intranet." See sample *Website Posting*, in section 8.

d. Organizing the meeting:

Once you know when and where you're going to hold your meeting, decide how you want it to unfold:

- Create an agenda and assign a period of time for each item. (See below, *Organizing the presentation and sample agenda*.)
- Think about logistics:
  - Is the meeting large enough that different people within your organization need to be assigned specific responsibilities?
  - Do you need signs to direct people to the location?
  - Should you have a sign near the door with the name of your event?
  - Will you need programs or agendas?
  - Will you offer additional literature for people to pick up after the program?

e. Organizing the presentation and sample agenda:

Everything you need for an engaging, informative presentation is in this guide:

- A ten-minute video (on DVD) that presents an overview of the issue and outlines the steps consumers can take—*Deter, Detect, Defend.*

Quick Tip—If you do not wish to give a speech or presentation, showing the video and holding a brief discussion can make a major difference.

- A five-minute speech you can deliver about identity theft with specific steps your audience can take to reduce their risk or minimize the damage.
- Presentation slides with similar information as the speech.
- A brochure that outlines the steps to *Deter, Detect, and Defend* against identity theft.

A sample agenda might look like this:

12:30 p.m. Welcome, call to order
12:35 p.m. Presentation
12:55 p.m. Discussion
1:30 p.m. End meeting

6. GETTING THE WORD OUT—IN YOUR COMMUNITY

6. GETTING THE WORD OUT—IN YOUR COMMUNITY

Consumers often look to community leaders for more information on important issues. Usually they turn to an organization that is important to them personally—a neighborhood group, civic association, social club, or place of worship. If you're interested in raising awareness to help fight identity theft, these community organizations are an effective way to reach the people you care about.

1 STEP ONE: Identify the right community organizations

Many people participate in activities outside work that bring them into contact with others. These activities often involve organizations with regularly scheduled meetings, newsletters or other forms of communication.

To help the people you care about take action against identity theft, think about all the organizations you support or with which you are involved. They may include:

- Community or neighborhood associations
- Volunteer and/or charitable organizations
- Civic organizations, local business groups, or chambers of commerce
- Places of worship—churches, synagogues, etc.
- Professional associations (outside the workplace)
- High school or college alumni groups

Once you've identified the groups with which you're involved, narrow the list to those that can best help you spread the word. Focus your efforts on groups that:

- Have regular meetings and/or a place to hold meetings
- Have newsletters, email distribution lists, a website or other ways to share information

2 STEP TWO: Place the *Deter, Detect, Defend* brochure in a public meeting area

One way to spread the word within your community organization is to post a copy of the brochure on a bulletin board at the organization's meeting place or center.

- Use the *Deter, Detect, Defend* brochure included in the ID Theft Consumer Education Kit as your "poster." As the brochure has information on both sides, you'll need to copy the back and front sides to display all the information.

- Order additional copies of the brochure—free of charge—from the FTC, by visiting **ftc.gov/order**.

- Put your business card near the brochure or write your phone number or email address on it to let others know you are available as a resource.

3 STEP THREE: Place an article in your community organization's newsletter

Perhaps your organization has a newsletter or email service to communicate with its members. To place an article in this publication:

- Look for an editor's name, email address, or phone number so you can send an article.
- Use the sample *Newsletter Blurb*, in section 8, to develop a short, concise piece for your own newsletter.
- Send the article to the newsletter editor, along with a cover note identifying yourself as a member of the organization, and explaining why this information is important.

4 STEP FOUR: Post information on your community organization's website

If your organization has its own website, consider posting a news item on identity theft. To place something on the website:

- Identify the site "webmaster" or content editor. This is the person to whom you will send material to post online. For many community websites, the content editor for the website is someone with other responsibilities.
- Use the sample *Website Posting* in section 8, to submit content.
- Try to use a season, date, or news event as a timely "hook" to interest members of your organization or community.

5 STEP FIVE: Put together a meeting

Community groups, civic associations, and other community organizations often sponsor regular meetings to discuss important issues. Some even offer facilities for members to use to organize meetings on their own. Either way, organizing a meeting can help you reach many people with important information on how they can take action on identity theft.

Identity theft is an important issue. People generally are interested in learning more—in particular, more about what they can do to minimize their risk. A meeting likely will draw interest from your community.

By taking these steps, you can plan an event that will raise awareness about identity theft.

6. GETTING THE WORD OUT—IN YOUR COMMUNITY

a. Choosing the place:

The first step in organizing an event is to find the right place. Consider:

- A space operated by your organization (a church meeting hall, a banquet facility or meeting room)
- The number of people likely to attend
- The facilities you can use to accommodate that many people
- Any restrictions on the use of that facility
- Whether it is available, and for how long, on a given day
- Whether your event will work best with auditorium-style seating or a discussion-style arrangement, like a circle of chairs
- Available technology or equipment. Can you use a PowerPoint presentation or video?
- Parking

Quick Tip—Choose a location that is convenient and large enough to accommodate your audience, has parking, is well-lit and is accessible by public transportation.

b. Choosing the time:

The timing of an event is as important as the location. Think about the people in your group, club or association who are likely to attend.

- What is the busiest time of day? The least busy?
- Do they prefer meetings before or after work, or during the weekend?
- Will onsite childcare be available for people attending the event?
- Is there a regularly scheduled meeting that already draws a good crowd?
- What else is going on at the same time that might compete for attention?
- If bad weather may be a factor, make sure you have an alternative date.

Quick Tip—If you are unsure about timing, check with the organization's leadership. Sound them out on when would be best for the group overall.

c. Announcing the meeting:

Many activities can build interest in your event. For example:

- Distribute flyers or e-vites to your organization's members. See sample *Meeting Invitation Flyer*, in section 8.

- Place a notice in your organization's newsletter or bulletin, or on its website. Time it to appear two to three weeks before the event, and send a follow-up reminder as close to the event as possible. See sample *Newsletter Blurb*, in section 8.

d. Organizing the meeting:

Once you know where and when you're going to hold the meeting, decide how you want it to unfold:

- Create an agenda and assign a period of time for each item. (See below, *Organizing the presentation and sample agenda*.)

- Think about logistics:
  - Will you register attendees beforehand? If so, does someone need to handle registration? Will you give out name tags?

- Think about how your event will look:
  - Do you need signs to direct people to a specific room within a large facility?
  - Should you have a banner or sign near the door?
  - Will you need programs or agendas?
  - Will you offer additional literature for people to pick up after the program?

e. Organizing the presentation and sample agenda:

Everything you need to deliver an engaging, informative presentation is included in this guide:

- A ten-minute video (on DVD) that presents an overview of the issue and outlines the steps consumers can take—*Deter, Detect, Defend*

Quick Tip—If you do not wish to give a speech or presentation, simply showing the video and holding a brief discussion can make a major difference.

- A five-minute speech you can deliver about identity theft with specific steps your audience can take to reduce their risk or minimize the damage if they suspect a problem

- Presentation slides with similar information as the speech

A sample agenda for a one-hour meeting might look like this:

6:30 p.m. Welcome, call to order
6:35 p.m. Presentation
6:55 p.m. Discussion
7:30 p.m. End meeting

7. GETTING THE WORD OUT—THROUGH THE MEDIA

Many people learn about identity theft through newspaper, television and radio reports. Whether it's a network news show or your community newspaper, the media play an important role in helping to educate people in your community by raising awareness about the problem and the steps they can take to minimize their risk and potential losses.

You can work with your local media to spread the word about identity theft, and the *Deter, Detect, Defend* message. Reporters want to hear about identity theft. And people in your community who read the newspapers, watch the evening news, or listen to the radio want to learn what they can do.

Here are several ways to work with the media.

a. Place a "Calendar Listing" with your local newspaper

If you're organizing a meeting that is open to the public, consider placing a "calendar listing" in your local newspaper. Every newspaper has a list of upcoming events, along with a contact name and address.

Send a copy of the announcement of the event (the same one you are distributing to your organization's members)—at least three weeks in advance—and it likely will appear in the calendar listings.

b. Send a press release to your local media

Reporters get news from many sources, including "news announcements" (also known as "press releases") that give them information about events, local developments, and other happenings. Sending a press release to your local newspaper, radio and/or TV station highlighting how your organization is educating people on identity theft may interest the reporter and result in an article. An article, in turn, helps get the word out—and helps more members of your community reduce their risk of having their identities stolen.

To send a news announcement:

- Read your local newspaper for several days to see which reporters are writing about identity theft, consumer fraud, or related business issues. Jot down the names of these reporters so you know who should receive your news announcement.

- If you don't see any particular name, contact the newspaper's "news desk" and ask for the name of the reporter who should receive information about identity theft.

- Use the sample *Press Release* in section 8, *Sample Materials*, to develop your own announcement for your organization.

- Once you've customized the press release, send it to the reporter(s) you've identified.

- About three or four days after sending the press release, call the reporter before 2:00 PM to check on whether he or she received your information. Let him or her know that this is an important issue to you and your organization, and why.

c. Send a copy of the *Deter, Detect, Defend* brochure to reporters

If you read your newspaper and see articles on identity theft or other consumer fraud issues, consider sending a copy of the *Deter, Detect, Defend* brochure to the reporter.

Attach a note expressing your support for helping residents of your community protect themselves from identity theft. Let the reporter know that you and others are taking action—to make your community more aware of how people can reduce their risk of identity theft, and minimize the damage should it occur.

8. MATERIALS YOU CAN USE

A. SPEECH

Good morning/afternoon/evening.

Thank you for joining us today/this evening.

I want to talk to you today about a problem that has affected millions of Americans, including Oprah Winfrey, Bill Gates, and Tiger Woods. Chances are it's hurt someone in this room.

The problem is identity theft.

Let's see...
- Raise your hand if you carry a wallet, or a purse
- Now, raise your hand if you have a credit card or a Social Security number

Guess what? Everyone here is at risk for identity theft!

But don't worry, I'm here to help you learn how to protect your identity, and minimize your chances of an identity theft.

So what **is** identity theft? It's what happens when someone uses your personal information—like your name and social security number or your credit card number—to commit fraud in your name.

Identity thieves can do a lot of damage...
- They can go on spending sprees using your credit card
- They can open a new credit card account, using your name and Social Security number
- They can get cell phone service in your name with your credit history
- They could even get arrested, and give your name to the police

People whose identities are stolen frequently spend lots of time and money cleaning up the mess the thieves have made of their good name and credit records.

They may lose out on job opportunities, loans for education, housing or cars. And they may even be arrested for crimes they didn't commit.

Now, just a few more questions—to help all of us assess our "ID IQ."

Each of these questions involves a yes or no answer. But this time, I don't want you to raise your hand or say your answer out loud. Just keep track of how many times you answered "yes" or "no."

Question one: Do you shred or destroy every bill, credit card statement, and bank statement that comes to your home before you throw it out?

Question two: Have you ever seen a copy of your credit report?

Question three: Do you know what a "fraud alert" is?

A. SPEECH

If you answered yes to all three, then you know some of the important steps to protect your identity and reduce the potential damage from identity theft.

If you answered yes to two out of three, then you're definitely "cramping the style" of many identity thieves. But there is still more you can do to minimize the chance of an ID theft, and the toll it can take.

If you answered yes to only one of the questions, or if you didn't answer yes to any of them... Well, you have company. Many of us just don't know that a few steps can make a real difference in reducing the risk of identity theft.

Hopefully, you'll leave here today knowing how to better protect one of your most important assets—your identity.

Identity theft is a serious crime: law enforcement and government agencies are devoting greater resources to the problem. One agency—the Federal Trade Commission, the nation's consumer protection agency—has prepared a brief video on the problem, and what you can do to protect yourself.

Let's take a look.

(Roll video)
(Pick up after video ends)

As the video shows, identity theft comes in many forms.

How do thieves steal your identity? Unfortunately, there are a lot of ways—from sophisticated computer hacking to low-tech "dumpster diving" into your trash, to plain, old-fashioned stealing your wallet or purse.

But you can take some practical steps to minimize your risk and to reduce the damage if your identity is stolen.

To help all of us in the fight against identity theft, the Federal Trade Commission has embarked upon a national outreach campaign. The campaign's theme is summed up in three key words—Deter, Detect, Defend.

First, Deter.

We all know the old saying that an ounce of prevention is worth a pound of cure. The same holds true for identity theft: making your personal information hard for thieves to get their hands on can reduce your risk. Here are the key steps to deter an identity theft:

- **Don't** give out personal information over the phone, through the mail, or over the Internet unless you are sure who you are dealing with. Sometimes this is a judgement call.
- **Safeguard** your personal information in a secure place at home, especially if you have roommates, employ outside help or are having work done in your home.
- **Shred** financial documents and paperwork with personal information on it before you throw them out.
- **Protect** your Social Security number. Don't carry your card in your wallet or write it on a check.

Now for the second part of the three-step action plan... Detect.

With identity theft, early detection is key. In addition to taking the preventive steps I just mentioned, detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Doing so can help you catch a potential problem before it gets out of hand. For instance:

- Read your credit card statements and financial accounts carefully, looking for any charges you did not make.

- Check your credit report regularly. For those of you not familiar with the term, your credit report has information about you, including accounts you have and how you pay your bills. It helps banks and other businesses decide whether to extend you credit or insurance, and on what terms.

The three major consumer reporting companies are required by law to give you a free copy of your credit report each year if you ask for it. The companies are: Experian, TransUnion and Equifax.

www.AnnualCreditReport.com is a central website, run by these three companies, where you can get your free credit report. I have a handout with the information.

Finally, the third part of the three-step strategy... Defend.

I've talked about how you can reduce your risk. But what if it's too late? What if you are already a victim?

The answer: act quickly.

- Contact the fraud department at any of the three nationwide credit reporting companies and ask them to place a "fraud alert" on your credit report. A fraud alert tells creditors to follow certain procedures to protect you before they open new accounts or make certain changes to an existing account. Each of the three nationwide consumer reporting companies has toll-free numbers to place a fraud alert. But you just need to place one call, because the company you call is required by law to notify the other two.

  Once you place a fraud alert on your file, you can get a free copy of your credit report from each of the three nationwide consumer reporting companies. Review your credit reports carefully, so you can figure out what fraudulent accounts may have been opened. And then, close them.

- File a police report and get a copy. Your creditors may require it for documentation. Plus, a police report will help you get information from creditors about the fraudulent accounts.

- Close all the accounts that were opened or used fraudulently. After you speak to someone in the company's fraud department about closing the account, follow up in writing and send copies of the documents that support your claim. I repeat: send copies, not originals. You can use the FTC's ID Theft Affidavit to simplify the process.

A. SPEECH

- After you've resolved a disputed charge with a company, ask for a letter stating that the matter has been closed. Keep copies of your papers and correspondence, and a record of all your conversations with companies where accounts were opened or used fraudulently.

- Finally, file a complaint with the Federal Trade Commission. You can go to **ftc.gov/idtheft** or call 1-877-ID-THEFT. Reporting your complaint can help law enforcement officials across the country with their investigations.

These are just the basic steps you can take to protect yourself from identity theft or repair the damage that has already occurred. There are others.

To learn more about other actions you can take, check out the Federal Trade Commission website at **ftc.gov/idtheft**. Take a look at *Take Charge: Fighting Back Against Identity Theft* the FTC's comprehensive guide. Or order a copy. It's free.

Now, I promised you some hand-outs that will be helpful resources, too.

Right now, as I speak, criminals are out there, looking for identity information to steal. They like identity theft because it can be such a so-called "easy" crime. They do their best work when no one is paying attention, when information is easy to get, because they think the damage will go undetected.

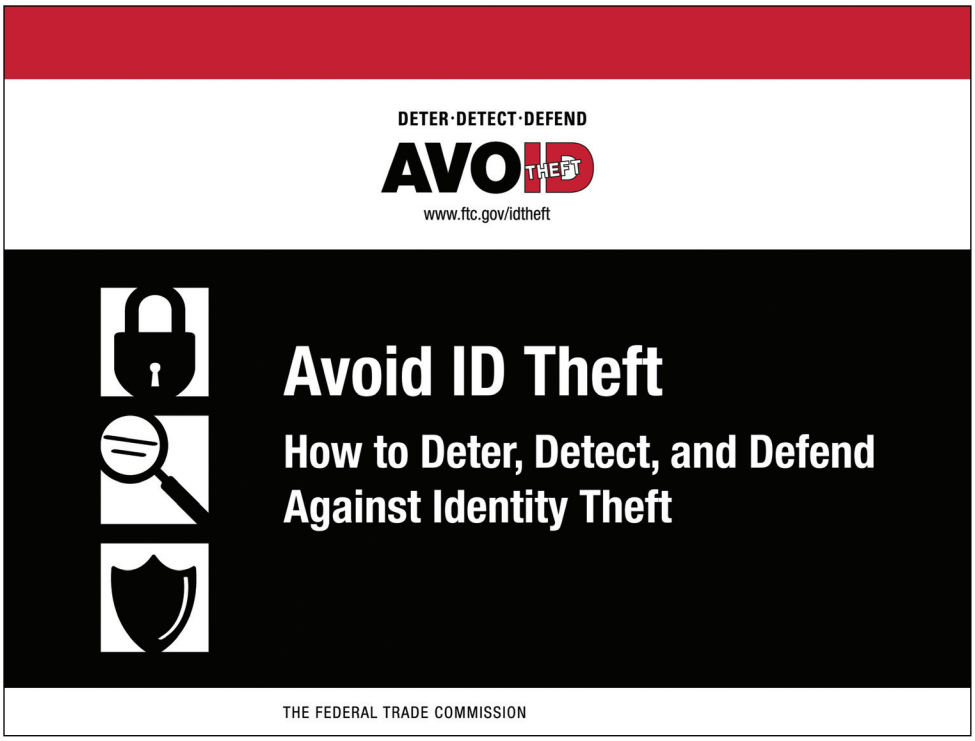
But we're paying attention now. By following the "three D's" of identity protection—*Deter, Detect, Defend*—we can all make it a lot more difficult for thieves to walk away with our identities. And a difficult crime is a less attractive crime.

Thank you for your time. I'd like to open this up for discussion or questions. My guess is there are people in this room who have an experience with identity theft, or know someone else who has. Does anyone want to share their story?

(Open up discussion.)

B. PRESENTATION SLIDES AND NOTES

Please click on the *Presentation Slides* on the CD-ROM menu to run the actual presentation.



SLIDE 1

Good morning/afternoon/evening:

Thank you for joining us today/this evening.

I want to talk to you about a problem that has affected millions of Americans, including Oprah Winfrey, Bill Gates, and Tiger Woods. Chances are it has hurt someone in this room.

The problem is identity theft.

B. PRESENTATION SLIDES AND NOTES

SLIDE 2

We'll talk about what identity theft is, how it happens, what you can do to defend against it, and where you can learn more.

[VIDEO OPTION: If the DVD will be included in the presentation:]

I want to start by showing you a brief video on identity theft.

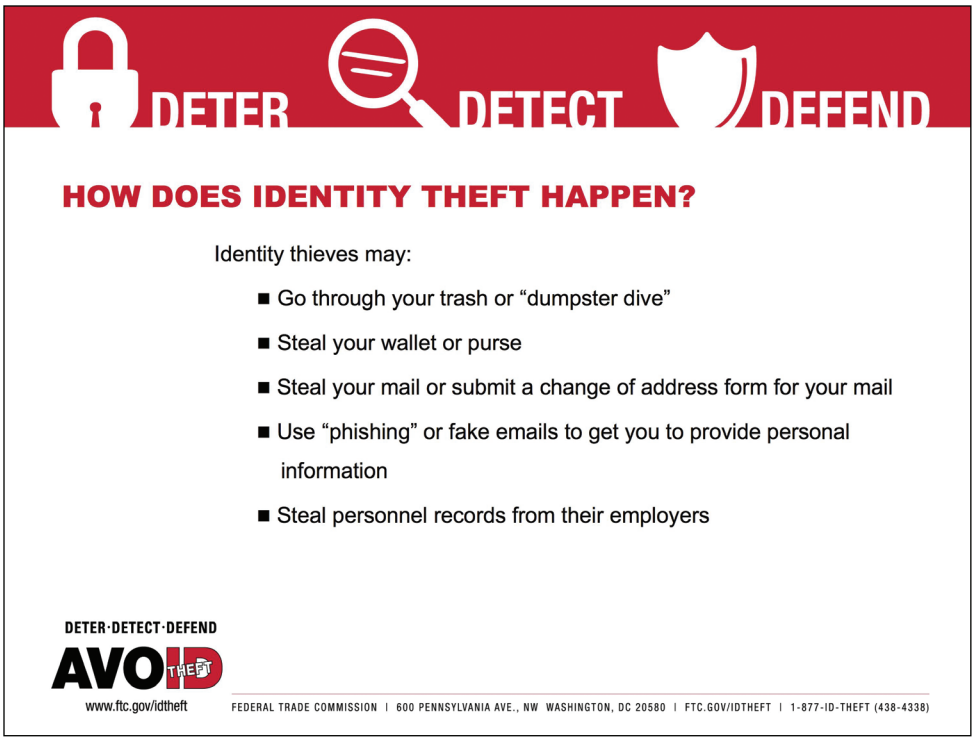
[PLAY DVD]

SLIDE 3

So, identity thieves can do a lot of damage…

- They can go on spending sprees using your credit card
- Using your name and Social Security number, they can open new credit card accounts
- They could give your name to the police if they get arrested

B. PRESENTATION SLIDES AND NOTES



SLIDE 4

Unfortunately, there are a lot of ways, from sophisticated computer hacking to low-tech "dumpster diving" into your trash, to old-fashioned stealing your wallet or purse.

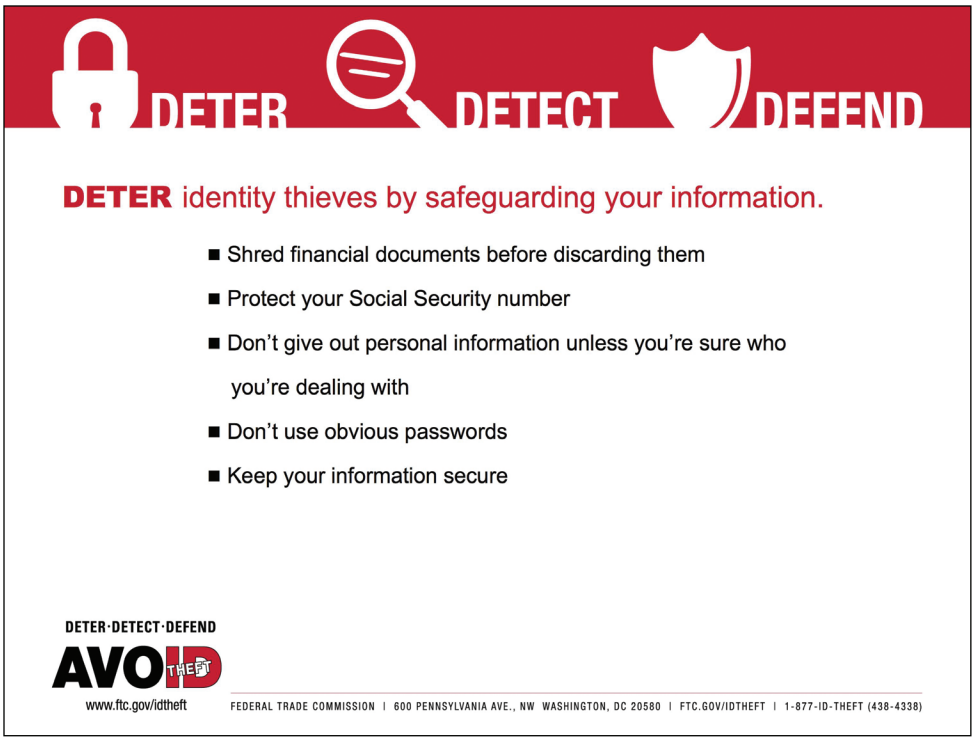
SLIDE 5

While there are no ways to absolutely guarantee you'll never be a victim of identity theft, there are ways to minimize your risk. By following the "3 D's" of identity protection, we can all make it more difficult for thieves to walk away with our identities.

The "3 D's" are Deter, Detect, and Defend; let me tell you about some specific steps you can take to minimize your risk.

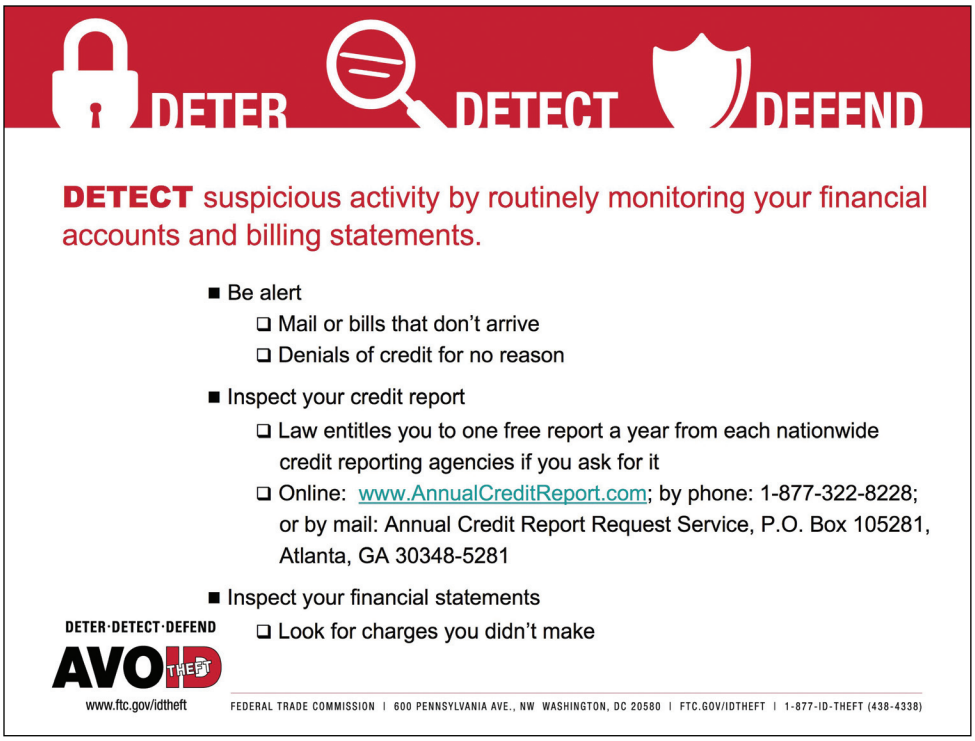
Don't worry about taking notes, I have handouts for you from the Federal Trade Commission.

B. PRESENTATION SLIDES AND NOTES



SLIDE 6

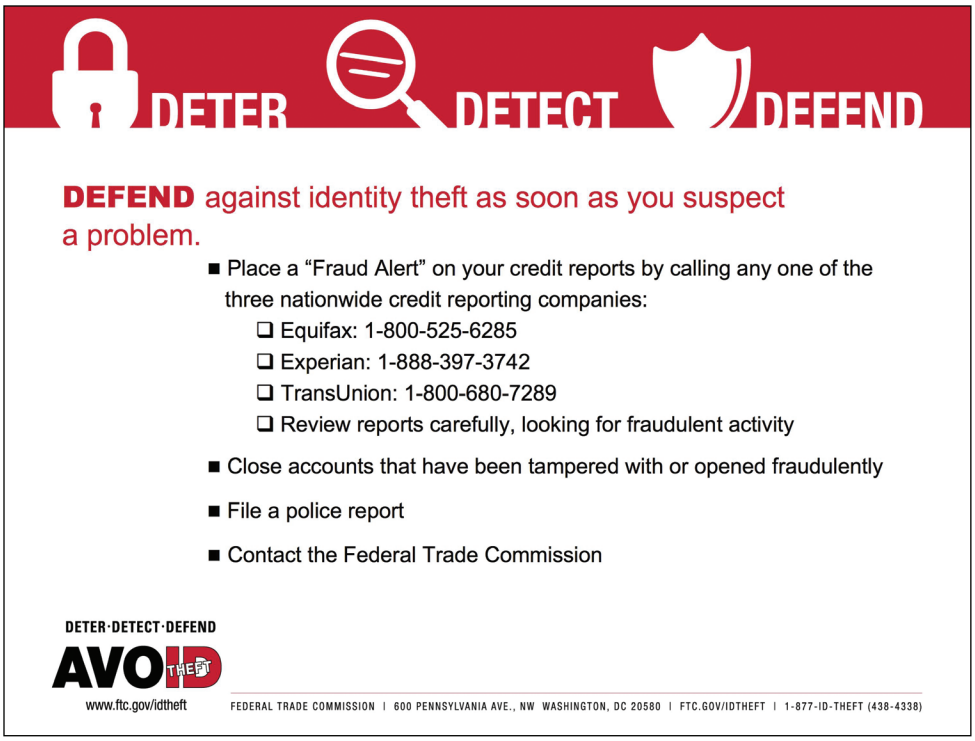
- **Shred** paperwork with personal information and financial documents before you discard them.
- **Don't carry** your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary; you can always ask to use another identifier.
- **Don't give out** personal information on the phone, through the mail, or over the Internet unless you are sure who you are dealing with.
- **Never click** on links sent in unsolicited emails; instead, type in a web address you know.
- **Don't use** obvious passwords. Your mother's maiden name, or the last four digits of your Social Security number – all are obvious passwords.
- **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.



SLIDE 7

- Credit reports contain information about you, including what accounts you have and your bill paying history.
  - There are three major nationwide consumer reporting companies—Equifax, Experian, and TransUnion—the law requires them to give you a free copy of your credit report each year if you ask for it.
  - **www.AnnualCreditReport.com** is a service created by these three companies: It is the **only** authorized site where you can order the free credit report you're entitled to each year.
  - When asking for your credit report, you may need to provide certain personal information, including your Social Security number and information about your monthly bills.

B. PRESENTATION SLIDES AND NOTES

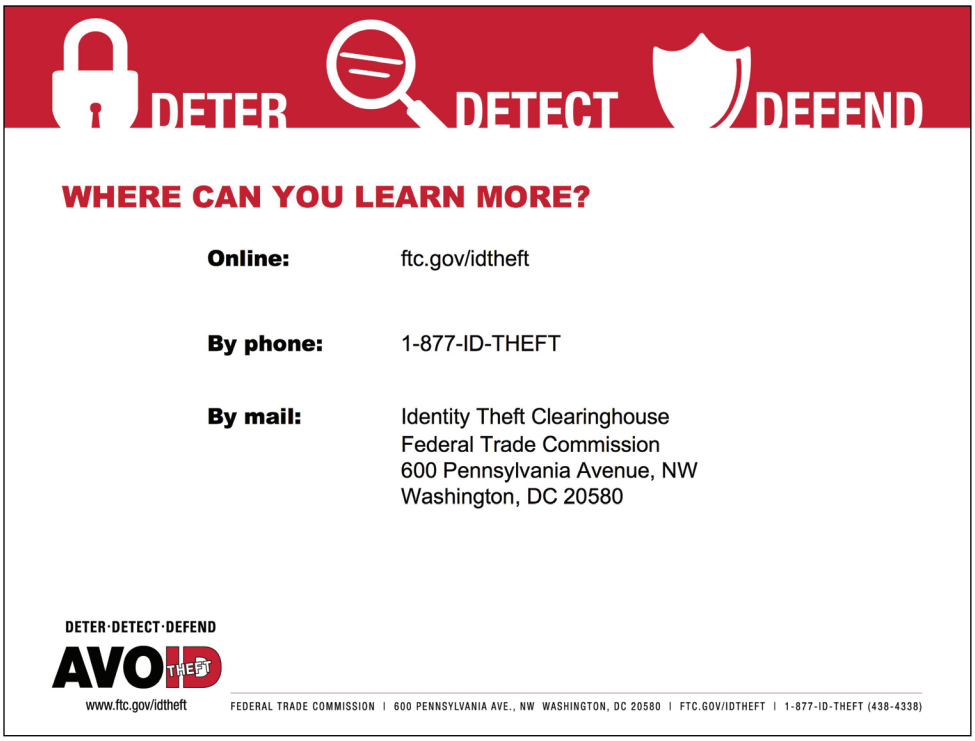


SLIDE 8

- Placing a fraud alert on your credit reports tells creditors to follow certain procedures before they open new accounts in your name or make certain changes to your existing accounts.
  - The 3 consumer reporting companies have toll-free numbers for placing an initial 90-day fraud alert; a call to one company is sufficient.
  - It 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.

- To close your accounts, call the security or fraud departments of each company where an account was opened or changed without your okay. 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 written verification that the disputed account has been closed and the fraudulent debts discharged.

- The FTC is the federal consumer protection agency that helps law enforcement officials in their investigations.



SLIDE 9

I'd like to distribute the handouts now. I hope you learned that you **can** Deter, Detect, and Defend against identity theft.

I appreciate your time and attention.

Any questions? I can try to answer them. In any case, I can direct you to people who definitely will know the answer. They're at the FTC, the nation's consumer protection agency, and they can be reached by the contact information on this slide.

C. BROCHURE TEXT

Please click on the *Deter, Detect, Defend* brochure on the CD-ROM menu to view or print the actual brochure.

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.

DETER

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 who you are dealing with.
- **Never click** on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit **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

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

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 **www.AnnualCreditReport.com** or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

DEFEND

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:
  - **Equifax:** 1-800-525-6285
  - **Experian:** 1-888-EXPERIAN (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.

- **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 okay. 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 written 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 officials 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 officials across the country in their investigations.
  - Online: **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

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

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

D. FREQUENTLY ASKED QUESTIONS

How does identity theft occur?
Identity theft occurs when someone uses your personal information, like your name and Social Security number or credit card number without your permission, to commit fraud or other crimes.

How do ID thieves get personal information?
They get information from businesses or other institutions by:

- Stealing records or personal information while they're on the job
- Bribing an employee who has access to these records
- Hacking these records
- Conning information out of employees

They also may:

- Steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.
- Rummage through trash in a practice known as "dumpster diving."
- Get your credit reports by abusing their employer's authorized access to them, or by posing as a landlord, employer, or someone else who may have a legal right to access your report.
- Swipe your card for an actual purchase, or attach a skimming device to an ATM machine where you may enter or swipe your card.
- Steal your wallet or purse.
- Complete a "change of address" form with a creditor to divert your billing statement to another location.
- Steal personal information they find in your home.
- Steal personal information from you through email or phone by posing as legitimate companies and claiming that you have a problem with your account. Done online, this practice is known as "phishing;" on the phone, it's called "pretexting."

How do ID thieves use personal information?
They may:

- Call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.
- Open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts appear on your credit report.
- Establish phone or wireless service in your name.
- Open a bank account in your name and write bad checks on that account.
- Create counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, to drain your bank account.
- Take out an auto loan or student loan in your name.
- Get identification such as a driver's license or state ID card issued in your name, with their picture.
- Get a job or file fraudulent tax returns in your name.
- Give your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

What do I do first if I learn that my identity has been misused?

1. Contact the fraud department of any one of the **three nationwide consumer reporting companies** to place an initial fraud alert on your credit report. The **fraud alert** tells creditors to follow certain procedures to protect you before opening any new accounts or making certain changes to your existing accounts. A call to any of the three companies will do: the company you call is required to contact the other two so that they place an alert on their versions of your report, too.

   A victim of identity theft also is entitled to place an extended (7 year) fraud alert. You have to follow additional procedures to place an extended fraud alert.

   Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports from each of the three nationwide consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on the reports they send you.

2. Review your credit reports closely, and **close the accounts** that have been tampered with or opened fraudulently.

3. **File a police report** with your local police or the police in the community where the identity theft took place. Get a copy of the report or at the very least, the number of the report to submit to creditors and others who may require documentation of the crime.

D. FREQUENTLY ASKED QUESTIONS

4. **File a complaint with the FTC.** The FTC maintains a database of identity theft complaints which can be accessed by law enforcement agencies for investigations. You can report identity theft at **ftc.gov/idtheft** or by calling 1-877-ID-THEFT toll-free.

For more information on recovering from identity theft and help with specific problems, read *Take Charge: Fighting Back Against Identity Theft*, a publication from the FTC. It's available online at **ftc.gov/idtheft** or you can call 1-877-ID-THEFT to order a free copy.

What do I do if my personal information has been lost or stolen?
If you've lost personal information or identification, or if it has been stolen from you, taking certain steps quickly can minimize the potential for identity theft.

Financial accounts: Close accounts, like credit cards and bank accounts, immediately. When you open new accounts, place passwords on them. Avoid using your mother's maiden name, your birth date, the last four digits of your Social Security number (SSN) or your phone number, or a series of consecutive numbers.

Social Security number: Call the toll-free fraud number of any of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. An alert can help stop someone from opening new credit accounts in your name. Consumer reporting company contact information is on page 37 of this guide.

Driver's license/other government-issued identification: Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and get a replacement. Ask the agency if it can flag your file so that no one else can get a license or any other identification document from them in your name.

Once you've taken these precautions, watch for signs that your information is being misused.

How do I prove I've been a victim of identity theft?
Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing. Be sure to ask the company representative where you should mail your request. Companies must provide these records at no charge to you within 30 days of receipt of your request and your supporting documents. You also may give permission to any law enforcement agency to get these records, or ask in your written request that a copy of these records be sent to a particular law enforcement officer.

The company can ask you for:

- Proof of your identity. This may be a photocopy of a government-issued ID card, the same type of information the identity thief used to open or access the account, or the type of information the company usually requests from applicants or customers, and

- A police report and a completed affidavit, which may be the FTC's Identity Theft Affidavit or the company's own affidavit.

E. EMAIL TO EMPLOYEES

Identity theft occurs when someone uses your personal information, like your credit card number or name and Social Security number, without your permission, to commit fraud or other crimes.

The Federal Trade Commission (FTC) estimates that as many as 10 million people have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft.

I'm writing to share some information on how you can minimize your risk of identity theft, detect a potential problem quickly, and take the right steps if you suspect a problem.

It's about the "3 D's" of identity protection—*Deter, Detect, Defend.*

DETER

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 have initiated contact and know who you are dealing with.
- **Never click** on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit **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

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

Be alert to signs that require immediate attention:

- Mail or 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

E. EMAIL TO EMPLOYEES

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 **www.AnnualCreditReport.com** or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

- **Your financial statements.** Review financial accounts and billing statements regularly, looking for charges you did not make.

DEFEND

Defend against identity theft as soon as you suspect a problem.

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

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

- **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 okay. Follow up in writing, with copies of supporting documents.
  - Use the ID Theft Affidavit at **ftc.gov/idtheft** to support your written statement.
  - Get written 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 officials to help you with creditors who may want proof of the crime.

- **Report your complaint to the Federal Trade Commission.** Your report helps law enforcement officials across the country in their investigations.
  - Online: **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

I hope you find this information useful. Identity theft is a troubling issue; being aware can have a big impact.

Thank you.

F. MEETING INVITATION FLYER

IDENTITY THEFT

You can make a difference...

Reduce your risk

Quickly detect a problem

Restore your good name

Protect your identity

To learn more about the "3 D's" of identity protection, please join us at:

Date: _____

Time: _____

Location: _____

Organized by: _____

For information, contact: _____

G. EMAIL INVITATION TO MEETING

Subject: Identity Theft—What You Can Do

Identity theft occurs when someone uses your personal information, such as your name and Social Security number or credit card number, without your permission, to commit fraud or other crimes.

The Federal Trade Commission (FTC) estimates as many as 10 million Americans have their identities stolen each year. In fact, you or someone you know may have already experienced some form of identity theft.

There are steps you can take to reduce the risk of thieves getting hold of your personal information, quickly detect a problem, and restore your good name if you have been victimized.

They are the "3 D's" of identity protection.

I invite you to attend an information session on this topic, and learn about the steps each of us can take to fight identity theft. You'll learn about how identity thieves work, and what you can do to make this crime more difficult for them.

Deter, Detect, Defend: Fighting Identity Theft
(Date/Time)
(Location)

I hope to see you there. In the meantime, should you have any questions, please be in touch.

(Your name)

H. NEWSLETTER BLURB

(Short version)

IDENTITY THEFT: You can protect your identity. Learn how to reduce your risk of identity theft, detect a problem quickly, and restore your name. Attend an information meeting on *(date, time)*, at *(location)*. For more information, contact *(your name, contact information)*.

(Longer version)

Deter, Detect, Defend: Learn More about Identity Theft

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

(Insert organization name) wants to help you learn how to protect yourself from identity theft at a free meeting that's open to the public. Please join us to learn more about how to reduce your risk of identity theft, and what to do if you suspect that your identity has been stolen.

Date: _____

Time: _____

Location: _____

For directions or more information, contact: _____

I. WEBSITE POSTING

Identity Theft
Learn how to
- Deter
- Detect
- Defend

against this serious crime.

Attend a free meeting

Hosted by: _____

When: _____

Where: _____

For more information contact: _____

J. PRESS RELEASE TEMPLATE

For Immediate Release[1]
Contact: (NAME)[2]

(Insert phone number, email address)

(Organization) Members Learn the 3 D's of Identity Theft[3]
Growing Concern Spurs Local Interest

(Your city, state), (date)[4]—(number) of (organization's) members turned out for a recent symposium on identity theft. According to the Federal Trade Commission, ID theft affects as many as 10 million Americans each year.

The meeting, titled "Deter, Detect, Defend—How to Protect Your Identity,"[5] was held on (date), at (location), at (time). It included a presentation on ID theft—and the steps people can take to reduce their risk and protect their identity.

"We received a strong response,"[6] said (organization spokesperson name). "Attendees were eager to learn more about this serious crime—and how they can better protect themselves."

#[7]

(Information on your organization here) [8]

ANATOMY OF THE PRESS RELEASE

[1] "For Immediate Release" means reporters can write a story as soon as they receive your press release.

[2] The contact is the person reporters will call to learn more about the event, to be connected with spokespeople and to schedule interviews.

[3] This is the headline, followed by a subhead. Headlines and subheads tend to be short, with no unnecessary words. If you read the headlines of the local paper, you'll see good examples. The headline should focus on the most important or newsworthy aspect of your release. The subhead provides additional, but less important, supporting information.

[4] This is the dateline, the day on which the release was sent and the location from which it originated.

[5] It helps if you name your event. This is a chance for you to catch people's interest by demonstrating the relevance of the topic.

[6] It's generally wise to include a quote in your press release. It makes the information more personal. It's also a good way to introduce your organization's leader or spokesperson. If you have information that is an opinion, put it in quotes and attribute it to the speaker. Refrain from expressing opinions outside of quotes.

[7] Triple hash marks at the bottom of a page mean "end of the story" or "end of release." This is an editing symbol that tells reporters that there is no further information. If the release is more than one page, end each page with "– more –", so the editor or reporter knows to read on.

[8] This last item isn't necessary, but it can be helpful. It's called a "boilerplate." Many organizations develop boilerplate language about themselves, which they attach at the bottom of press releases. It's in smaller italicized print so that it's not confused with the body of the story. Boilerplates generally contain basic information about organizations, such as the mission, size of the membership and some historical details.

9. ADDITIONAL RESOURCES

9. ADDITIONAL RESOURCES

You and your audience can get more information on identity theft from the following resources available online at ftc.gov/idtheft or by phone 1-877-ID-THEFT:

Avoid ID Theft: Deter, Detect, Defend video

FTC Publications:

- *Take Charge: Fighting Back Against Identity Theft*
  The FTC's comprehensive guide for victims of identity theft. Includes the ID Theft Affidavit.
- *Remedying the Effects of Identity Theft*
  Summarizes your rights as a victim of identity theft.
- *What To Do If Your Personal Information Has Been Compromised*
  How to respond if your personal information is compromised when an organization's security is breached.
- *Identity Crisis... What to Do If Your Identity Is Stolen*
  Four pages of advice on dealing with identity theft.
- *Identity Thieves Can Ruin Your Good Name: Tips for Avoiding Identity Theft*
  Basic tips on a wallet-sized card.
- *How Not to Get Hooked by a Phishing Scam*
  How to avoid online scammers who want to steal your personal information.
- *Getting Purse-onal: What To Do If Your Wallet or Purse Is Stolen*
  Basic advice on a single page.
- *Credit, ATM and Debit Cards: What To Do If They're Lost or Stolen*
  Outlines procedures for reporting loss or theft, and how to minimize your risk.
- *Your Access to Free Credit Reports*
  Educates consumers about their right to a free copy of their credit reports. The brochure outlines the nine-month roll-out period that began on December 1, 2004; explains the ordering process by Web, toll-free telephone number, and postal address; and includes a copy of the standard credit report request form.
- *How to Dispute Credit Report Errors*
  Explains how to dispute and correct inaccurate information in your credit report. Includes a sample dispute letter.
- *Fair Credit Billing*
  The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts. Includes sample dispute letter.
- *Fair Debt Collection*
  Answers commonly asked questions about your rights under the Fair Debt Collection Practices Act. It prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection.
- *Stop. Click. Think. 7 Practices for Safer Computing*
  Provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information. Available at **OnGuardOnline.gov**

NOTES

DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

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

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