15

Identity Theft!! Is Someone Else Claiming to be You?
Leader Guide

Items for Preparation:
1. **Make copies as needed of participant handouts.**
2. **Find ID theft scenarios**

Lesson:

1. Begin with one or two scenarios on ID theft. (find in newspapers or magazines)
2. Participants take quiz found on page 8 of participant handouts. Correct at end of lesson.

ASK: What is Identity Theft?

The 1990's spawned a new variety of crooks called identity thieves. How do they do it? With little bits of information about you found in everyday transactions: bank and credit card account numbers; your income; your Social Security number; or just your name address and phone numbers. An Identity thief obtains little bits of information about you and uses it without your knowledge to commit fraud or theft.

ID theft is a serious crime. People who are victims can spend months or even years and their hard earned money clearing their good name and credit record. Many victims have lost job opportunities, refused loans, and some have even been arrested for crimes they didn't commit.

Can you prevent it from occurring? Just like any other crime, you cannot control whether you will be a victim, but you can do minimize your risk by managing your personal information, and being more careful in some areas of your life.

ASK: How can I tell if I'm a victim?

There are some indications of identity theft that you should be aware of:

- Failing to receive bills or other mail signaling an address change by the identity thief
- Receiving credit cards that you did not apply for
- Denial of credit for no apparent reason
- Receiving calls from debt collectors or companies about merchandise or services you didn't purchase.

DISCUSS: Top 10 sources of Identity Theft:

- Mail theft
- Dumpster diving
- Unscrupulous employees
- Stolen or lost wallets
- Internet fraud
- Burglary (home, vehicle, documents, computer files, etc.)
- Friends or relatives
- Phone scams
- Unethical use of public documents
- Shoulder surfing for passwords at ATMs, computers, etc.

Identity theft is an epidemic, affecting over 900,000 people a year. It can cost the average victim more than $1,000 to rectify the damage done by an ID thief. Thieves steal identities for financial gain, to get a job, to avoid prosecution or exact revenge. **It is crucial to control your personal information to prevent ID theft.**

DISCUSS: The following is covered in your handouts, but I will cover the main steps now.

- Review your credit report from each of the credit agencies twice a year, see if there are accounts or addresses you do not recognize. Is your SSN correct? Have there been more inquires than normal? Any of these may be early signs of ID theft. You may want to add consumer alert, which asks creditors to call you each time a new account is opened in your name.

- Shred or burn important papers, even those pre-approved credit card applications we all get, also, mail order receipts, use a cross cut shredder, thieves have a lot of free time, they can piece together strips from regular shredders.

- Do not use your Mothers maiden name as a password on accounts; ask if you may use another word or numbers instead.

- Deposit outgoing mail in secure Post Office collection boxes or at your local Post Office, never leave it in your curbside mailbox. If you will be gone on vacation for an extended time, arrange with the Post Office for a Vacation Hold.

- Pay attention to your billing cycles, follow up with creditors if your bills do not arrive on time, a missing bill may indicate and ID thief has taken over your account and changed your address.

- At ATMs, either shoulder block your pass code or try to cover the keypad with your whole hand, I personally use my whole hand as if I am typing instead of the one finger number punch method.

- Secure your purse or your wallet; limit the amount of credit cards you carry.

DISCUSS: Protect your Social Security Information

Do not carry your Social Security card in your wallet. Limit the use of your SSN; ask if you may use another form of I D. Never give the number to any one on the phone unless you initiated the call.

The only ones who need your SSN are:

- Employers
- Financial Institutions, for tax reporting purposes.
- IRS and State Income Tax

Other private businesses may ask for your SSN to do a credit check, such as when you apply for a house or car loan, if someone asks for your SSN, ask the following questions:

- Why do you want it?
- How will it be used?
- How do you protect it from being stolen?
- What will happen if I don't give it to you?

Be aware, if you don't provide your SSN, some businesses may not provide you with the service or benefits you want. You will have to decide from their answers if you wish to share your SSN with them.

Insurance Companies routinely use our SSN for our ID number. A new law has passed that Insurance Companies have until 2006 to issue new numbers, if you do not want to wait, you may request, in writing, to have yours done now.

Stores have until December 4th 2006 to stop printing the whole credit card account number and expiration date on our receipts. Any business still using the mechanical imprinters, or, hand written receipts, is exempt.

DISCUSS: **Should you be concerned about your computer?**

Your computer can be a goldmine of personal information to an ID thief.
If you are storing personal information such as SSN, financial records, tax returns, birth dates or bank account numbers in your computer, the following tips can help keep your computer and personal information safe.

- Update your virus protection software regularly; computer viruses can have a variety of damaging effects, including introducing program codes that cause your computer to send out files or other stored data to an ID thief.

- Do not open or download files sent from someone you don't know.

- Use a firewall program, especially if you have a high speed or "always on" program which leaves your computer connected to the internet 24 hours a day, without a firewall, hackers can take over your computer and access sensitive material for ID theft or other crimes.

- Try not to store financial information in your laptop unless absolutely necessary, don't use automatic log in feature and always log off each time you are finished, that way, if your laptop gets stolen or lost, it will make it harder for thieves to access your personal information.

- Before you dispose of your old computer, delete personal information. Use a Wipe Utility Program to overwrite the entire hard drive, it makes the files unrecoverable.

EMPHASISE: **Managing your personal information and preventing identity theft requires everyday diligence.**

(✓ Items are on page 6 of handouts so audience can follow your explanations)

READ: "I applied for a loan in November 2000 and was told I had bad credit. I requested a credit report in November 2000 and found all sorts of crazy information on it. I'm single but was listed as married. When I renewed my driver's license by mail, I was surprised to find someone else's face on my license. This is a nightmare and requires a large amount of my time."

READ: **Proving You're a Victim, Not a Deadbeat**

Unlike victims of other crimes, who generally are treated with respect and sympathy, identify theft victims often find themselves having to prove that they're victims, too – not deadbeats trying to get out of paying bad debts. So how do you go about proving something you didn't do? Getting the right documentations and getting them to the right people is the key.

DISCUSS: **What to do if you become a victim:**

- ✓ **Set up a folder to keep a detailed history of this crime.**
  "Accurate and complete records will greatly improve your chances of resolving your identity theft case. Set up a filing system for easy access to your paperwork. Keep old files even if you believe your case is closed. One of the most difficult and annoying aspects of identity theft is that errors can reappear on your credit reports or your information can be re-circulated. Should this happen, you'll be glad you kept your files"

- ✓ **Keep a log of all your contacts and make copies of all documents.**
  "Keep copies of all correspondence or forms you send. Write down the name of anyone you talk to, what he or she told you, and the date the conversation occurred. Use Chart Your Course of Action form to help you. Copy of Chart is in your handout. Keep the originals of supporting documentation, like police reports, and letters to and from creditors; send copies only."

- ✓ **Contact all creditors, by phone and in writing to inform them of the problem**
  "Follow up in writing with all contact you've made on the phone or in person. Use certified mail, return receipt requested. A "Sample Letter" is in handout.

- ✓ **File a police report**
  "Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number."

DISCUSS: **Tips on Filing a Police Report**

Provide documentation – Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, your notarized ID Theft Affidavit (available at FTC website), and other evidence of fraudulent activity can help the police file a complete report.

Be persistent – Local authorities may tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Also, remind them that under their voluntary "Police Report Initiative," credit bureaus will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but **only if** you can give them a copy of the police report. If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police. If you're told that identity theft is not a crème under your state law, ask to file a Miscellaneous Incident Report instead.
Be a motivating force – Ask your police department to search the FTC's Consumer Sentinel database for other complaints in your community. You may not be the first or only victim of this identity thief. If there is a pattern of cases, local authorities may give your case more consideration.

That's why it's also important to file a complaint with the FTC. Law enforcement agencies use complaints filed with the FTC to aggregate cases, spot patterns, and track growth in identity theft. This information can then be used to improve investigations and victim assistance.

✓ **Contact the fraud department of each of the three major credit bureaus to report the identity theft and request the bureaus place a fraud alert status in your file:**

	Order credit report	Report fraud	Web site
Equifax:	800/685-1111	800/525-6285	www.equifax.com
Experian	888/397-3742	888/397-3742	www.experian.com
Trans Union	800/916-8800	800/680-7289	www.tuc.com

"Call the toll-free fraud number of any one of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charges."

✓ **Contact the Federal Trade Commission's toll free Identity Theft Hotline at 877/ID-THEFT (438-4338).**
"By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials' track down identity thieves and stop them. The FTC also can refer victim's complaints to other appropriate government agencies and companies for further action. The FTC enters the information you provide into our secure database."

✓ **Contact your bank. Close your accounts, change all of your account passwords, and obtain new credit, debit and ATM cards.**
"Thieves may have opened a bank account with a line of credit in your name and write bad checks on that account."

✓ **Contact the US Postal Inspection Service. Call your local post office or write to:**
Inspection Service Operations Support Group
Attn: Mail Fraud, Ste. 1250, 222 S.
Riverside Plaza, Chicago, IL 60606-6100
The Direct Marketing Association's (DMA) Mail Preference Service lets you "opt-out" of receiving direct mail marketing from many national companies for five years. When you register with this service, your name will be put on a "delete" file and made available to direct-mail marketers.

✓ **Contact the Social Security Administration 800/772-1213.**
"Under certain circumstances, SSA may issue a new SSN – at your request – if, after trying to resolve the problems brought on by ID theft, you continue to experience problems. Consider this option carefully. A new SSN may not resolve your ID theft problems, and my actually create new problems."

✓ **Contact your local Depart of Motor Vehicles.**
The Drivers Privacy Protection Act forbids states from distributing personal information to direct marketers. It does allow for the sharing of personal information with law enforcement officials, courts, government agencies, private investigators, insurance underwriters and similar businesses. Check with your state DMV to learn more, or visit:
www.ftc.gov/privact/protect.htm#Motor.

Resources:
ID Theft - "When Bad Things Happen To Your Good Name" by Federal Trade Commission (Nov 2003)
FTC Consumer Alert – www.consumer.gov/idtheft

IDENTITY THEFT QUIZ
Leader guide
Answers **[xx]**

Circle One:

1. I receive credit card solicitations in the mail every week. **[Yes]** No
2. I do not shred credit card solicitations before throwing them away. Yes **[No]**
3. I do not review my credit reports regularly. Yes **[No]**
4. I carry my Social Security card with me at all times. Yes **[No]**
5. I will give my Social Security number to anyone who asks for it. Yes **[No]**
6. I carry my children's Social Security card with me at all times. Yes **[No]**
7. I trust people. When I type in my passwords at ATMs, work, etc., I don't think about anyone watching to learn the password. Yes **[No]**

8. Identity fraud is:
   A. Nothing to worry about.
   B. A small crime in America affecting a few people.
   C. Not much of a financial risk.
   [D] The fastest growing crime in America, affecting 900,000 new victims each year.

9. Do I know what to do if my identity is stolen?
   A. Don't pay the bills—after all I didn't make the purchases.
   B. Make more purchases and blame it on the "thief."
   C. Contact my Mother.
   [D] Contact credit reporting agencies, credit card accounts, and my bank.

10. If my identity was used fraudulently, the cost to correct my credit will be, on average:
    A. $100
    B. $500
    [C] $1,000
    D. $2,000

SAFEGUARD YOUR IDENTITY
PARTICIPANTS HANDOUT

Top 10 sources of Identity Theft:

- Mail theft
- Dumpster diving
- Unscrupulous employees
- Stolen or lost wallets
- Internet fraud
- Burglary (home, vehicle, documents, computer files, etc.)
- Friends or relatives
- Phone scams
- Unethical use of public documents
- Shoulder surfing for passwords at ATMs, computer, etc.

How Can I prevent identity theft from happening to me?
As with any crime, you can't guarantee that you will never be a victim, but you can minimize your risk. By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft.

Order a copy of your credit report from the three credit reporting agencies twice a year, see if there are any accounts or addresses, you do not recognize. Is your SSN correct? Have there been more inquires than normal? Any of these may be early signs of ID theft. You may want to add consumer alert, which asks creditors to call you each time a new account is opened in your name.

Don't give out personal information on the phone, through the mail or over the Internet unless you initiated the contact or are sure whom you are dealing with. Identity thieves can pose as representatives of banks, Internet providers (ISP's) and even government agencies to get you to reveal your SSN, Mother maiden name, account numbers, and any other identifying information. Before you share any information, confirm that you are dealing with a legitimate organization. You can check the organizations web site as many companies post scam alerts or you can call customer service using the numbers listed on your account statement or in the telephone book.

Secure personal information in your home, especially if your have roommates, employ outside help or are having service work done in your home.

Secure your purse or wallet, carry only the identification information and number of credit cards that you actually need.

Place passwords on all of your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number or a series of consecutive numbers.

Pay attention to billing cycles, follow up with creditors if your bills do not arrive on time, a missing bill may mean an identity thief has taken over your account and changed your billing address.

When ordering new checks, pick them up at the bank rather than having them sent to your home.

Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gas pumps, keep track of all your paperwork, when it is no longer needed, destroy it.

Sign all new credit cards upon receipt, and report all lost or stolen cards immediately.

Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.

According to the Federal Trade Commission, there are three scams that specifically target a person's credit and identity information.

1. Internet- If you have an online account and receive e-mail from your ISP (Internet Service Provider) stating that your account information needs to be updated or that the credit card you signed up with is invalid and the information needs to be reentered to keep your account active, beware. Call your ISP rather than responding to the E-Mail.

2. Slave Reparation Act – This targets elderly African Americans in the South and Midwest attempting to obtain their personal identifying information. These are usually on flyers placed on windshields or senior center bulletin boards claiming that African American born before 1928 might be eligible for slave reparations of $5000. THERE IS NO SUCH ACT.

3. A third scam claims that those born between 1917-1928 can apply for Social Security funds they are due because of a "fix" in the Social Security System. THERE IS NO SUCH PROGRAM AT THE SOCIAL SECURITY ADMINISTRATION.

Guard your mail and trash from theft.
Deposit outgoing mail in secure Post Office collection boxes or at your local post office, rather than in an unsecured curbside mailbox.

Promptly remove your mail from your mailbox, if you are planning to be away for an extended period of time, call your local Post Office and request a vacation hold.

To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, burn or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards and credit offers you get in the mail. Use a cross cut shredder, thieves can piece together strips.

Protect your Social Security information:
Do not carry your SS card in your wallet. Limit the use of your SSN; ask if you may use another form of ID. Never give the number to any one on the phone unless you initiated the call.
The only ones who need your SSN are:

- Employers
- Financial Institutions, for tax reporting purposes.
- IRS and State Income Tax

Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect personal information from you. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if the information will be shared with anyone else, if so; ask if they can keep your information confidential

Be wary of promotional scams, Identity thieves may use phony offers to get you to give them your personal information.

Other private businesses may ask for your SSN to do a credit check, such as when you apply for a house or car loan, if someone asks for your SSN, ask the following questions:
Why do you want it?
How will it be used?
How do you protect it from being stolen?
What will happen if I don't give it to you?

Be aware, if you don't provide your SSN, some businesses may not provide you with the service or benefits you want. You will have to decide from their answers if you wish to share your SSN with them.

Insurance Companies routinely use our SSN for our ID number. A new law has passed that Insurance Companies have until 2006 to issue new numbers, if you do not want to wait, you may request, in writing, to have yours done now.

Stores have until December 4th, 2006 to stop printing the whole credit card account number and expiration date on our receipts. Any business still using the mechanical imprinters, or, hand written receipts, is exempt.

Should you be concerned about your computer?
Your computer can be a goldmine of personal information to an ID thief. If you are storing personal information such as SSN, financial records, tax returns, birth dates or bank account numbers in your computer, the following tips can help keep your computer and personal information safe.

1. Update your virus protection software regularly; computer viruses can have a variety of damaging effects, including introducing program codes that cause your computer to send out files or other stored data to an ID thief.

2. Do not open or download files sent from someone you don't know.

3. Use a firewall program, especially if you have a high speed or "always on" program which leaves your computer connected to the internet 24 hours a day, without a firewall, hackers can take over your computer and access sensitive material for ID theft or other crimes.

4. Try not to store financial information in your laptop unless absolutely necessary, don't use automatic log in feature and always log off each time you are finished, that way, if your laptop gets stolen or lost, it will make it harder for thieves to access your personal information.

5. Before you dispose of your old computer, delete personal information. Use a Wipe Utility Program to overwrite the entire hard drive, it makes the files unrecoverable.

Our economy generates an enormous amount of data. Most users of that information are from honest businesses, getting and giving legitimate information. Despite the benefits of the information age, some consumers may want to limit the amount of personal information they share. And they can, more organizations are offering people choices about how their personal information is used.

Managing your personal information and preventing Identity theft requires everyday diligence.

Learn more about the options you have for protecting your personal information by contacting the following organizations:

Department of Motor Vehicles
The drivers Privacy Protection Act forbids states from distributing personal information to direct marketers, it allows sharing of personal information with law enforcement officials, courts, government agencies, private investigators, insurance underwriters and similar businesses. Check with your local DMV to learn more.

Direct Marketers
The Federal Government has created the National Do Not Call Registry- the free, easy way to reduce the telemarketing calls you get at home. To get more information or to register, visit www.donotcall.gov, or call 1-888-382-1222.

Mail:
The Direct Marketing Assoc. Mail Preference Service (DMA) lets you opt out of receiving direct marketing from many national companies for five years. When you register with this service, your name will be put on a "delete" file and made available to direct-marketers. However, your registration will not stop mailings from organizations that are not registered with the DMA service. To register send your letter to:
Direct Marketing Assoc.
Mail Preference Service
P.O .Box 643
Carmel, NY 10512
Or register online at: www.the-dma.org/consumers/offmaillist.html

Email:
The DMA has an Email Preference Service to help reduce unsolicited commercial emails. To "opt- out", you can use their website, your request will be effective for one year.
Register online at: www.dmaconsumers.org/offmaillist.html

Credit Bureaus:
Trans Union
P.O. Box 390 Springfield, Pennsylvania 19064-0390
To order your report, 1-800-916-8800
To report fraud 1-800-680-7289

Equifax
P.O. Box 74021 Atlanta, Georgia 30374-0241
To order your report, 1-800-685-1111
To report fraud, 1-800525-6285

Experian
P.O. Box 949 Allen, Texas 75013-0949
To order your report, 1-888-397-3742
To report fraud 1-888-397-3742

ID Theft
What to Do

What to do if you become a victim:

- ✓ Set up a folder to keep a detailed history of this crime.
- ✓ Keep a log of all your contacts and make copies of all documents.
- ✓ Contact all creditors, by phone and in writing to inform them of the problem
- ✓ File a police report
- ✓ Contact the fraud department of each of the three major credit bureaus to report the identity theft and request the bureaus place a fraud alert status in your file:

	Order credit report	Report fraud	Web site
Equifax:	800/685-1111	800/525-6285	www.equifax.com
Experian	888/397-3742	888/397-3742	www.experian.com
Trans Union	800/916-8800	800/680-7289	www.tuc.com

- ✓ Contact the Federal Trade Commission's toll free Identity Theft Hotline at 877/ID-THEFT.
- ✓ Contact you bank. Close your accounts, change all of your account passwords, and obtain new credit, debit and ATM cards.
- ✓ Contact the US Postal Inspection Service. Call your local post office or write to:
  Inspection Service Operations Support Group
  Attn: Mail Fraud, Ste. 1250, 222 S.
  Riverside Plaza, Chicago, IL 60606-6100
- ✓ Contact the Social Security Administration 800/772-1213.
- ✓ Contact your local Depart of Motor Vehicles.

The FTC's Privacy Policy

To file a complaint or to learn more about the FTC's Privacy Policy, visit www.consumer.gov/idtheft. If you don't have access to the Internet, you can call the FTC's Identity Theft Hotline: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

SAMPLE DISPUTE LETTER CREDIT BUREAU

Date

Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Credit Bureau
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute also are circled on the attached copy of the report I received. (Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

I am a victim of identity theft, and did not make the charge(s). I am requesting that the item be blocked to correct my credit report.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation) supporting my position. Please investigate the (these) matter(s) and block the disputed item(s) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing)

SAMPLE DISPUTE LETTER FOR EXISTING CREDIT ACCOUNTS

Date

Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Credit Bureau
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) attributed to my account in the amount of $_____.
I am a victim of identity theft, and did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as police report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing)

IDENTITY THEFT QUIZ

Circle One:

1. I receive credit card solicitations in the mail every week. Yes No
2. I do not shred credit card solicitations before throwing them away. Yes No
3. I do not review my credit reports regularly. Yes No
4. I carry my Social Security card with me at all times. Yes No
5. I will give my Social Security number to anyone who asks for it. Yes No
6. I carry my children's Social Security card with me at all times. Yes No
7. I trust people. When I type in my passwords at ATMs, work, etc., I don't think about anyone watching to learn the password. Yes No

8. Identity fraud is:
   A. Nothing to worry about.
   B. A small crime in America affecting a few people.
   C. Not much of a financial risk.
   D. The fastest growing crime in America, affecting 900,000 new victims each year.

9. Do I know what to do if my identity is stolen?
   A. Don't pay the bills—after all, I didn't make the purchases.
   B. Make more purchases and blame it on the "thief."
   C. Contact my Mother.
   D. Contact credit reporting agencies, credit card accounts, and my bank.

10. If my identity was used fraudulently, the cost to correct my credit will be, on average:
    A. $100
    B. $500
    C. $1,000
    D. $2,000