

Section 4--Consumer Issues and Education

Title of Lesson/Subject: *Identity Theft 3: It Could Happen to You!*

Prepared by: Annette M. Dirks

Contact Information

E-mail address: adirks@asbt.com

Phone: (701) 774-4176

Time Allotment: 1 Hour

Target Audience: Adult

Brief Description:

Using an acrostic for IDENTITY the audience will learn about Identity Theft. The audience will learn these key concepts about Identity Theft: what it is, how it happens, how prevalent it is becoming, how identity theft can affect a person's credit rating, how to detour identity theft and the steps to take if they should fall victim to Identity Theft.

Introduction:

Identity theft is a serious crime. Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. You can't entirely control whether you will become a victim, there are things you can do to minimize your risk. Just one missing puzzle piece can dramatically change a puzzle's characteristics. The same is true with a person's identity – one bit of information is all someone needs to steal your identity.

Lesson Outline: "I D E N T I T Y"

I Information

Criminals are interested in gaining access to your personal credit information. Personal credit information includes: your name, birth date, social security number, bank account numbers, credit and debit card numbers. They can then use this information to apply for credit in your name and run up huge bills, leaving creditors unpaid and generally ruining your credit history. How do thieves obtain this information?

- your mailboxes without locks
- locked mailboxes in unsecured areas
- dumpsters
- telemarketing and computer (e-mail) scams
- computer hacking
- paying workers in retail or financial institutions to copy down information

Armed with a Social Security number thieves can go online to find a spouse's name, last three addresses and other information.

The most commonly affected age group is people between 18-29 years old. This information is misused in the following ways:

- Credit card fraud 33%
- Phone and utilities fraud involving new wireless accounts 21%
- Other including: bank accounts, employment-related fraud, government documents or benefits fraud

D Deterrence

You must detour the thieves from gaining access to your personal credit information. Here are a few simple steps to help you safeguard your personal and financial information.

- Don't give your Social Security or account numbers to anyone over the phone unless you initiated the call and are certain you are speaking to a representative of a reputable company.

- Tear your receipts, old bank statements and unused credit card offers into small pieces before throwing them away. (Invest in a personal shredder)
- Protect your PINs and computer passwords. Use a random combination of letters and numbers and change them every six months or so. **Don't** use family or pet names, or dates or addresses that a thief can deduce or discover. Never carry this information with you!

E Education

Mind the criminals who commit the serious forms of identity theft do it for a living. You're up against pros.

- Have you made a list of all your credit cards and bank accounts, along with associated numbers, possible expiration dates and telephone numbers for each issuer's customer service and fraud department? And is it in a secure location?
- Do you carry in your wallet or purse only the credit cards, bank cards and identification you actually need and use? Carrying extra cards and identification like your Social Security card can invite even more trouble if your wallet or purse is stolen.
- Have you changed your driver's license from your Social Security number to an alphanumeric number?
- Have you replaced all your PINs and passwords with random numbers and letters?
- Know your billing cycles, and watch for any missing mail.
- Have you ordered your credit card report recently to review it for any incorrect information and unauthorized accounts?

N Notify

If you suspect someone has misused your personal information to commit fraud, take action immediately. Keep a record of all conversations and correspondence.

Step 1: Contact your bank(s) and credit card issuers immediately

- Access to your account can be protected
- Stop payments can be placed on any checks that are stolen or missing
- Personal identification numbers (PINs) and passwords can be changed
- A new account can be opened, if necessary

Step 2: Ask your bank to notify the check verification service with which it does business so that company can use its database to notify retailers not to accept stolen checks. It is best to work through your bank, but Tele-check does accept report of check fraud directly from consumers. Call 1-800-710-9898

Step 3: File a police report with your local police department. This is very important. Be sure to obtain a police report number with the date, time, police department, location and police officer taking the report. Get a copy of the police report for your files.

Step 4: Contact the three major credit bureaus and request a copy of your credit report. There fraud alert numbers are:

- Equifax: 1-800-525-6285
- Experian: 1-888-397-3742
- Transunion: 1-800-680-7289

Review your reports to make sure additional fraudulent accounts have not been opened in your name. Review activity in your existing accounts, including those rarely used, for possible unauthorized changes. Check the section of your report that lists "inquiries."

T Take action

- Take your Social Security number out of circulation

- Do not have your Social Security number printed on your checks
- Do not allow merchants to write your Social Security number on your checks
- Never give your Social Security number, account numbers or personal credit information to anyone who calls you.
- Make sure your mailbox is secure.
- Do not leave bill payments envelopes clipped to your mailbox or inside with the flag up.
- When you order new checks from the bank ask to pick them up instead of having them delivered to your home.
- “Opt Out” Of receiving pre-approved financing or credit offers call 1-888-5-OPT-OUT
- Reduce the number of mail and telephone solicitations by mailing your name, home address and signature to : Mail Preference Service, Direct Marketing Association, P.O. Box 9008, Farmingdale, NY 11735-9008 or visit the DMA Web site, www.dmconsumers.org
- Reduce the amount of unsolicited commercial email you receive register at: www.e-mps.org

I Inquire

- Check your Social Security Earnings and Benefits statement once each year to make sure no one else is using your Social Security number for employment.
- Order copies of your credit reports once a year to ensure they are accurate. Call each of the three national credit – reporting agencies because each may contain different aspects of your credit history.
- Review your bank and credit card statements as soon as you receive them to check for unauthorized transactions. Review account activity on a weekly basis.

T Track

- Keep track of credit card, debit card and ATM receipts. Never throw them in a public trash container. Tear them up or shred them at home when you no longer need them.
- Track the merchant as they complete your credit transaction. Never let your credit card out of your sight.
- Use both the Customer Activity Log and Customer Account Record to assist you in tracking information if your identity is stolen.

Y You

- You can protect your personal credit **information**.
- You can **detour** the thieves from gaining access to your personal credit information.
- You can **educate** yourself to help prevent Identity Theft.
- You can **notify** the bank and credit card companies if you fall victim to identity theft.
- You can **take action** to help avoid identity theft.
- You can **inquire** about your Social Security Earnings and Benefits statement, credit reports, and bank accounts on a regular basis.
- You can **track** all account activities and identity theft victim correspondence.
- **You can protect yourself against Identity Theft.**

Materials Needed:

- ✓ Identity Theft note sheet
- ✓ Customer Account Record
- ✓ Customer Activity Log

Resources:

Get Smart about Credit: Preventing Identity Theft, North Dakota Bankers Association. Available at: www.ndba.com

IDENTITY THEFT

INFORMATION

DETERRENCE

EDUCATION

NOTIFY

TAKE ACTION

INQUIRE

TRACK

YOU

CUSTOMER ACCOUNT RECORD

Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

CREDIT BUREAUS (Report Fraud)

Bureau	Phone Number	Date Contacted	Contact person	Comments
Equifax	1-800-525-6285			
Experian	1-888-397-3742			
Trans Union	1-800-680-7289			

BANKS, CREDIT CARD ISSUERS AND OTHER CREDITORS

Creditor	Address and Phone	Date Contacted	Contact Person	Comments

LAW ENFORCEMENT AUTHORITIES

Bureau	Address and Phone	Date Contacted	Contact Person	Comments
Federal Trade Commission (FTC)	1-877-ID-THEFT			
Social Security Administration	1-800-269-0271			
Local Police Department				
Postal Service				

CUSTOMER ACTIVITY LOG

This log is designed to assist you in maintaining a written chronology of what happened, what was lost and the steps you took to report the incident to various banks and agencies.

Incident Details (date, time, location and circumstances of incident)
Methods of Discovery (how did you first discover the incident?)
Statement Review (list of any unauthorized withdrawals, transactions or charges)
Other Information