FAMILY ECONOMICS & FINANCIAL EDUCATION

IDENTITY THEFT

WHAT IS IDENTITY THEFT?

Identity theft is when someone wrongfully acquires and uses a consumer's personal identification, credit, or account information.

Identity thieves use this information to do things such as open credit accounts, obtain cell phones, write fraudulent checks, or make large purchases all in the consumer's name.

Identity theft results in damage to the consumer's credit rating, denial of future credit, and job offers.

HOW IDENTITY THIEVES ACQUIRE INFORMATION

Identity theft can occur in a variety of methods. Thieves may:

- Steal wallets or purses (*most common method)*
- Steal mail
- Complete a "change of address" form for mail
- Go "Dumpster Diving" to steal information carelessly discarded in the trash.
- Obtain a credit report
- Find personal information in the home or on the internet
- Scam a person through e-mail, phone, or internet.
- "Insider Access" at the workplace.

HOW PERSONAL IDENTIFICATION INFORMATION CAN BE USED

Information identity thieves acquire can be used in numerous ways including:

- To apply for a new driver's license
- To open new bank and credit accounts
- To apply for credit cards or store credit accounts
- To obtain cash with bank cards
- To get a job
- To rent an apartment
- To make retail purchases
- To get a phone or other utilities
- To file bankruptcy
- To counterfeit checks
- To give a person's name during an arrest

People whose identities have been stolen can spend months or years and thousands of dollars cleaning up the mess thieves have made of their name and credit record.

PERSONAL IDENTIFICATION

ATM Card · Bills · Calling Cards · Bank Account Information · Checks

Credit Cards · CREDIT REPORT · Passwords · Debit Cards

Personal Records · Social Security Number · Pre-Approved Credit Cards

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

Identity Theft: How it occurs and Prevention

Credit Reports

How Theft Occurs:

A thief may use an individual's credit report to learn all of the accounts a person has, his/her social security number, and personal information about where a person works, lives, and their bank accounts.

Prevention:

- Check personal credit reports once per year and immediately dispute any wrong information from each of the three reporting agencies.
- Don't leave reports lying around. Store them in a locked file or shred.

Mail

How Theft Occurs:

Identity thieves may steal an individual's mail to learn his/her account numbers and personal information.

Prevention:

- Deposit outgoing mail in post office collection boxes or at the post office rather than unsecured mail boxes.
- Promptly remove mail from the mailbox. If an individual is going to be gone, he/she should contact the post office and request a vacation hold.

The dollar loss suffered because of identity theft from consumers was 343 million in 2002.

Federal Trade Commission

Wallets and Pocketbooks

How Theft Occurs:

Identity thieves may steal a wallet or pocketbook to have a wealth of personal and account information.

Prevention:

- Don't leave it in plain sight.
- Don't hang it from a chair at a public place.
- Use a purse which closes securely.
- Only carry what is absolutely needed. Do not carry social security cards, passports, or birth certificates unless necessary.

Bills

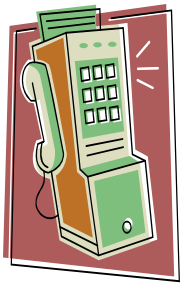
How Theft Occurs:

A thief may steal a person's bills containing his/her name, address, telephone number, bank account, credit and debit account numbers, and even a person's social security number. This information may be used to take over current accounts or open new ones.

Prevention:

- Don't leave statements lying around. Store them in a locked file and shred information not needed.
- Pay attention to the billing cycle. Follow up with creditors if bills do not arrive on time.

Calling Cards



How Theft Occurs:

If a thief has an individual's calling card and personal identification number, if required, a person may make long distance calls to anywhere.

Prevention:

- Use only calling cards which require a personal identification number.
- When at a pay phone, block the number while dialing so no one can see the numbers you are typing.

Passwords

How Theft Occurs:

With computer passwords, a thief can easily access accounts, send messages and/or viruses, purchase or sell items, or access online bank accounts.

Prevention:

- Don't give passwords to anyone.
- Don't write passwords down where others may find them.
- Create unique passwords which include a combination of numbers and letters in large and small caps. Avoid using information such as mother's maiden name, date of birth, or social security number.

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

Identity Theft: How it occurs and Prevention

ATM, Credit, and Debit

How Theft Occurs:

If an identity thief has both an individuals Automatic Teller Machine (ATM) Card and Personal Identification Number (PIN), money can be withdrawn from the individual's account.

Because most stores do not ask to compare identification with the signature on the back of the card, they are easy to use in stores, on the internet, or over the phone. Especially because merchandise may be mailed to a different address than the card's bill is sent.

Prevention:

- Don't leave the cards lying around the home or office.
- Carry only those which will be used.
- Close unused accounts cut up the card.
- Use debit cards which require a PIN number.
- Memorize the PIN number. Do not write it down in the same place the ATM or debit card is kept.
- Carry cards in a separate holder from the wallet.
- Sign the back of credit and debit cards stating "Please see I.D."
- Have a list of all cards and the account numbers.
- Don't give out the account number unless making purchases.
- Keep track of all receipts and destroy papers with the card numbers on them. Do not throw receipts in the trash.
- Check statements for unauthorized charges.

Work Records

How Theft Occurs:

A thief may fraudulently obtain work records containing a person's name, address, social security number, and bank information if pay is directly deposited.

Prevention:

- Make sure personal records at work are locked securely with limited access by employees.

The number of identity theft complaints filed in 2002 was 380,000, almost double from the 204,000 complaints in 2001.

Federal Trade Commission

Pre-Approved Credit

How Theft Occurs:

Identity thieves can apply for credit card accounts using pre-approved offers and change the address so the card will be sent to them.

Prevention:

- Shred any credit card offers received and not used.
- Cut up any pre-approved credit cards not used.
- If a person would not like to receive credit card offers, he/she can call 1-888-567-8688 to get off the marketing list.

Bank Account Information

How Theft Occurs:

With a bank account and routing number, an identity thief may be able to create fake checks and withdraw money. A thief may also access savings accounts to withdraw money.

Prevention:

- Don't leave statements lying around. Store them in a locked file and shred information not needed.
- Use passwords.
- Don't have check orders mailed home. Pick them up at the bank.

Social Security Number

How Theft Occurs:

An individual's social security number is the key to their identity. It can be used to open new accounts, apply for jobs, obtain a driver's license, file bankruptcy, etc.

Prevention:

- Don't give a social security number unless it is used for a legitimate purpose.
- Ask for an alternate number on driver's licenses, insurance cards, and other materials.
- Don't carry social security cards in a wallet or pocketbook unless necessary.

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

WHY PEOPLE SHOP ONLINE

The internet has opened a new world of products and services for consumers. It has changed the way consumers interact within the marketplace. The internet is a wealth of information. Consumers may order products from around the world. Within minutes, a consumer can easily research items or compare prices. In today's fast paced society, the internet is becoming increasingly popular because of the convenience it provides.

Shopping may be done in the comfort of one's own home at any time of the day or night.

This increase in convenience also provides a consumer with new risks. Shopping and banking online can be a goldmine for identity thieves. Consumers need to be cautious to guard personal information such as their social security numbers, credit card numbers, financial records, banking account numbers, etc. To safely shop online, consumers need to be aware of the risks and take preventative measures.

"Consumers spent 26 billion dollars online in 2002 according to the United States Department of Commerce."

SAFETY TIPS FOR SHOPPING ONLINE

1 Know the real deal

Get all the details before buying. This includes a complete description of items including the total price, delivery time, warranty information, return policies, and what to do with problems.

2 Look for clues about security

When providing payment information, the browser will show whether the information is being encrypted or scrambled when being sent. Before making an online purchase or viewing personal information, make sure the browser states "shttp" or "https" indicating it is secure.

3 Use a credit card

It is the safest way to pay because a person has the legal right to dispute charges for goods or services never ordered, received, or misrepresented.

4 Use an escrow service

If working with a company who can not accept payment by credit card, escrow services are the next safest. They will hold a person's money until confirmation the products or services has been received.

5 Keep proof handy

Print and file the information in case it is needed later.

6 Ask about "substitute" or "single-use" credit card numbers

This new technology allows a person to use his/her credit card without putting the real account number online, protecting it from abuse by "hackers" or dishonest employees of the seller. For more information, contact Orbiscom (www.orbiscom.com).

7 Get the scoop on the seller

Check complaint records at the state or local consumer protection agency and Better Business Bureau. Get the physical address and phone number to contact the seller offline. Look for sellers belonging to programs which encourage good business practices and help resolve complaints.

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona

WHAT TO DO IF IDENTITY THEFT HAPPENS

No matter how careful a person may be, identity theft can happen. If a person believes he or she may be a victim, they must follow these basic rules.

1. Act immediately.
2. Keep a detailed record of correspondence and phone records. These records should include the date, contact person, and any specific comments made or actions which will occur.
3. Contact the three major credit bureaus and request a "fraud alert" on file. Write a letter requesting no new accounts are opened without written permission. In addition, request a credit report from each bureau. Carefully review the reports to ensure they are accurate.
4. Close all accounts which have been tampered with or opened fraudulently. When opening new accounts, use different passwords and pin numbers.
5. File a police report with the local police or in the local community where the theft took place.
6. File a complaint with the Federal Trade Commission at 1.877.ID.THEFT.

PERSONAL LIABILITY

Credit Cards

The Truth in Lending Act limits a person's liability for unauthorized credit card charges to $50.00 per card. To take advantage of this law, a person must write a letter within 60 days of the first bill containing the error. The dispute must be resolved within 90 days of the creditor receiving the letter. If an individual's card has been stolen, it should be reported and canceled immediately.

ATM & Debit Cards, Electronic Funds Transfers

The Electronic Funds Transfer Act provides protection. The amount a person is liable for depends upon how quickly he/she reports the loss. Cards reported within two business days of discovering the theft or loss are liable for a maximum of $50.00. Within 60 days, a person is liable for $500.00. After 60 days, a person may be liable for all of the money. A person should always call the financial institution then follow up in writing to report any losses. When opening new accounts, use new account and personal identification numbers.

Checks

Stop payment and ask the financial institution to notify the check verification service. Most states hold the financial institution responsible for losses of a forged check if a person notifies the bank within a reasonable time.

CREDIT REPORTING BUREAUS

Equifax—www.equifax.com

P.O. Box 740241, Atlanta, GA 30374-0241

To order a report, call: 1.800.685.1111

To report fraud, call: 1.800.525.6285

Experian—www.experian.com

P.O. Box 9532, Allen, TX 75013

To order a report, call: 1.888.397.3742

To report fraud, call: 1.888.397.3742

TransUnion—www.transunion.com

P.O. Box 6790, Fullerton, CA 92834-6790

To order a report, call: 1.800.888.4213

To report fraud, call: 1.800.860.7289

Funded by a grant from Take Charge America, Inc. to the Norton School of Family and Consumer Sciences Take Charge America Institute at The University of Arizona