

Identity Theft – What Is It?

- the use of one person's personal information by another to commit fraud or other crimes. The most common forms of identity theft occur when someone obtains another person's social security number, driver's license number, date of birth, and the like and uses it to open a fraudulent bank, credit card, cellular telephone, or other account, or to obtain false loans.

With relatively little effort, an identity thief can use this information to:

- take over existing credit accounts
- create new accounts in the victim's name or even evade law enforcement after the commission of a violent crime
- sell personal information online to the highest bidder, often resulting in the stolen information being used by a number of different perpetrators.

Identity Theft

- Identity theft can be very difficult for consumers to deal with, as they often do not know they have been defrauded until they are denied credit or receive a call from a creditor seeking payment for a debt incurred in their name.

Identity Theft

- Identity theft is on the rise, affecting almost 10 million victims in 2008 (a 22% increase from 2007)
- 71% of fraud happens within a week of stealing a victim's personal data.
- Low-tech methods for stealing personal information are still the most popular for identity thieves. Stolen wallets and physical documents accounted for 43% of all identity theft, while online methods accounted for only 11%.

Who is at Risk ?

How many victims are there ?

- E V E R Y O N E (including children and the dead)
- 27.3 million in past 5 years
- Trans Union receives over 2,000 calls a day

Indications of Identity Theft

- Charges occurring on your accounts that you did not authorize.
- If your credit is denied due to poor credit ratings, despite good credit history.
- If you are contacted by creditors regarding amounts owed for goods or services that you never obtained or authorized.
- If your credit card and bank statements are not received in the mail as expected.
- If a new or renewed credit card is not received.

Identity Theft Prevention Measures

- Never give personal information via telephone, mail or the Internet, unless you initiated the contact.
- Store personal information in a safe place.
- Shred credit card receipts and/or old statements before discarding in a garbage can--If you do not have a shredder, then use scissors.
- Protect PINs and passwords.
- Carry only the minimum amount of identifying information.

Identity Theft Prevention Measures

- Remove your name from mailing lists for pre-approved credit lines and tele-marketers.
- Order and closely review biannual copies of your credit report from each national credit reporting agency (Equifax, Experian, and Trans Union).
- Ensure that your PIN numbers cannot be observed by anyone while utilizing an ATM or public telephone.
- Close all unused credit card or bank accounts.
- Contact your creditor or service provider if expected bills do not arrive.
- Check account statements carefully.
- Guard your mail from theft.

How to minimize your risk

- Do not leave your paid bills in your mailbox for the postman to pick up
- Keep personal information secure in the workplace. Know who has access to this information.
- Shred your trash
- Cancel all lost/stolen cards as soon as possible.
- Check your credit at least once a year
- Activate computer protections; install virus software and utilize your firewall
- If you have a wireless router, enable the encryption

How to minimize your risk

- Erase your hard drive when you dispose of your old computer (consider using Eraser on your Windows computer)
- Shut off your computer
- Use “disposable” e-mail to thwart would-be spammers
- Type carefully on the web as scammers create look-alike sites utilizing common mis-typings of popular URLs.
- Run more than one anti-spyware programs.
- Opt out of credit card offers
- Don't leave mail in your mailbox too long

What is the average time a
consumer must spend to recover
from ID Theft?

600 Hours*

What cost to the individual victim?

- \$5,720 was the mean loss per victim *

Who are the culprits ?

- Common criminals
- Organized crime
- Sometimes, friends, family, roommates, household workers, disgruntled spouse
- Terrorists
- Gangs (on the rise)
- Insiders (i.e., “harvesters”)

Identity Theft - Methods to get hold of your information

- **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
- **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
- **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
- **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
- **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
- **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

ADDITIONAL TRICKS USED BY THIEVES

- Mail Theft
- Shoulder Surfing
- Social Engineering

SKIMMING

- Where a thief temporarily steals a credit card and runs it through a “skimmer” which is a credit card reader to steal information off of the card.

Phishing Defined

- **Phishing** is the term coined by hackers who imitate legitimate companies in e-mails and fake websites to trick people in to sharing personal information.
- Recent victims include AOL, Best Buy, eBay and the Federal Trade Commission. Consumers were directed to Web pages that looked nearly identical to the real websites.

» www.wordspy.com

Step 1 – “The Lure”

- The typical phishing scam usually starts with an e-mail message.
- The e-mail directs the victim to a fake web page, sometimes containing false e-mail addresses and fictitious web addresses.
- The “Lure” often contains a place for the victim to enter personal data.
- Sometimes the scam opens the real web page, but uses a fake pop-up screen.

A Recent trend: VISHING

- You are prompted by a fraudulent e-mail or fake website to contact a toll free number. If you comply, you will reach a legitimate sounding voicemail system and be prompted to enter account numbers, etc. The automaton will record your entries for ID thieves

**WATCH OUT FOR THE “FREE
CREDIT REPORT SCAM”**

Free Annual Credit Report (The genuine site)

- ***www.annualcreditreport.com***

Online Identity Theft

- In addition to reporting to local police and filing an FTC identity theft complaint at www.consumer.gov/idtheft,
- You can also report online thefts by filing complaint with www.IC3.gov (a joint effort of the FBI and the National White Collar Crime Center)

What should a victim do first ?

- 1. Place a fraud alert on your credit reports and review your credit report
- 2. Close accounts that were compromised or opened fraudulently
- 3. File a complaint with the Federal Trade Commission
- 4. File a report with local police in the community where the identity theft took place

If You are a Victim of Identity Theft

- Contact the account issuer(s) where fraudulent accounts have been opened or where your accounts have been taken over--Ask for the fraud/security department and notify them both via telephone and in writing.
- Close all tampered or fraudulent accounts.
- Ask about the existence of secondary cards.
- Contact your local police department and file a police report.
- Notify the police department in the community where the identity theft occurred, if it is different from your own.

If You are a Victim of Identity Theft

- Filing a complaint with the FTC is important for several reasons. First, the information that you enter into the [ID Theft Complaint Form](#) can be used as part of an [Identity Theft Report](#), which is an important tool in recovering from identity theft.
- Second, when you file an ID Theft Complaint with the FTC, you can help law enforcers catch identity thieves. Your complaint is entered into the FTC's Identity Theft Data Clearinghouse, which law enforcement officers can search as part of their criminal investigations. (The FTC, however, does not bring criminal cases.) Law enforcement officers who are members of the Clearinghouse may contact you if your case becomes part of their investigation. But it's also a good idea to stay in touch with your local police department about their investigation, or about any recent developments in your case.

If You are a Victim of Identity Theft

- Obtain copies of any police reports filed.
- Keep a detailed log of who you talked to and when, including their title, phone number, and other contact information.
- Contact the Federal Trade Commission's Identity Theft Clearinghouse and file an identity theft complaint as those complaints are utilized by law enforcement agencies, including the FBI, that investigate identity theft. You can also obtain additional information at that website regarding your rights as a victim.
- Online identity thefts can also be reported at www.IC3.gov.

What's a Fraud Alert?

- Legally requires that potential creditors must use “reasonable policies and procedures” to verify your identity before issuing credit in your name.
- There are 2 types of Fraud Alert:
 - Initial Alert: for 90 days
 - Extended Alert: for 7 years an alert is placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report

Things to Remember

- You have 60 days to notify your financial institution of missing funds (the institution has 10 days to put the money back)
- Notify financial institutions by telephone and follow up with certified letter w/return receipt concerning each fraudulent account and provide copies of police report
- Keep all records of what you send
- Review website www.ftc.gov/idtheft for more details and up to date information

JUNK MAIL

- To have your name removed from the Direct Marketing Association (DMA) List:

Direct Marketing Association
Mail Preference Service
P.O. Box 643
Carmel, NY 10512

Or *www.the-dma.org*

To “Opt Out” of prescreened credit
card and insurance offers

Call toll free: 1-888-567-OPTOUT (8688)

or

www.optoutprescreen.com

Credit Agencies

- Equifax: 1-800-525-6285;
www.equifax.com
- Experian: 1-888-EXPERIAN (397-3742);
www.experian.com
- TransUnion: 1-800-680-7289;
www.transunion.com

Questions ?

www.consumer.gov/idtheft

www.identitytheft.gov

1-877-ID-THEFT