

Identity Theft: *It Can Happen to You*

Fact #1 You are not considered a victim of identity theft or account take over if you have given permission to a family member, relative, friend or partner to use your credit or debit card and they have abused that privilege.

Fact #2 The time required by an unassisted victim to resolve an identity theft issue has increased by more than 1,000% over the past two years.

Fact#3 Among the most common and easiest ways for criminals to secure your personal information is collecting direct mail offers and account statements from your mail box or “dumpster diving” in your trash cans.

Fact #4 A 2003 survey from the Identity Theft Resource Center reported that 73% of respondents were victims of identity theft

Identity theft is one of the fastest growing crimes in America. It is estimated that about nine million people will be victims in 2006 and the total loss due to identity fraud in the United States will exceed \$56.6 billion. It can happen to anyone, and often goes unnoticed until a collection agency calls, your check is refused at the check out counter or your credit card is confiscated by the bank.

Today, your personal information – Social Security number, credit card and bank account numbers, phone card number and other important data -- are easy targets for thieves who know how to use that information for their own gain.

According to the Identity Theft Resource Center, there are four types of identity theft crime:

1. Financial ID Theft – This involves theft of your name and Social Security number. Armed with this information, someone may apply for telephone service, credit cards and loans, purchase merchandise, lease cars and even apartments.
2. Criminal ID Theft – This is when an imposter uses your personal information instead of his or her own when stopped by law enforcement. Eventually a warrant for arrest may be issued for the person whose name is listed on the original citation – yours.
3. Identity Cloning – This happens when an imposter uses your information to establish a new life. The identity thief works and lives as you.
4. Business or Commercial Identity Theft – Yes, businesses can also be victims of identity theft. In this case, the perpetrator typically steals credit card or checking account numbers in the name of the business and uses them



Whatever type of identity theft you may encounter, rest assured that the process of reclaiming your good name, credit rating and more can be a very long and arduous process. But, there are steps you can take to prevent identity theft.

What you can do

Protect Your Records & Your Good Name

1. Get a copy of your credit report. Make sure the information contained in it is accurate and there is no fraud occurring. A federal law allows you to get a free report annually from the three credit bureaus.
Go to www.annualcreditreport.com or call 877-322-8228.
2. Protect your Social Security number. Only provide it where required (tax forms, employment records, most banking, stock and property transactions.) DO NOT print it on your checks or carry it in your wallet.
3. Always take credit card receipts with you. Never toss them in a public trash container. When shopping put your receipts in your wallet, not your shopping bag.
4. When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, your mother's maiden name, your birthdate, middle name, pet's name, consecutive numbers or anything else easily discovered by thieves. Memorize these numbers. Don't carry them in your wallet.

Limit Your Exposure

5. Limit calls from telemarketers to your home or cell phone by signing up for the national "Do Not Call" registry at toll-free (888)567-8688.
6. Remove your name from mailing lists for pre-approved offers of credit by calling (888)567-8688.
7. Reduce junk mail Send your name and address to the Direct Marketing Association's Mail Preference Service (MPS). Your name will be added to a list of people who do not want to receive mail from the major nationwide catalog and marketing companies. Free opt out by mail – MPS, PO Box 643, Carmel, NY 10512. or go to www.dmaconsumers.org/cgi/offmailinglist, and opt out online, but it will cost you \$5.00
8. Don't enter national sweepstakes and other contests where you end up on mailing lists.

Watch the Mail

9. Install a locked mailbox at your residence or use a post office box or commercial mailbox service.
10. Pick up new checks at the bank; don't have them mailed to your home.
11. Do not leave envelopes containing checks at your mailbox for the postal carrier to pick up.
12. Buy a paper shredder and shred all mail, sweepstakes, credit card offers and other sensitive information.

Use the Internet

13. Use online banking for paying bills, and request that your bank NOT return copies of cancelled checks to you by mail
14. Do not send sensitive personal information – phone number, passwords, address, credit card number, Social Security number via chat lines, e-mail, instant messages, text messages, forum postings or in your online profile.
15. Opt out of sharing online cookie data with advertisers by contacting Network Advertising Initiative at www.networkadvertising.org

Banking & Shopping

16. Shield your hand when using a bank ATM machine.
17. Use a gel pen for writing checks.
18. Keep your wallet in a front pocket or zipped or closed in purse or bag and limit the number of credit and debit cards you carry. Monitor your credit card and bank statements regularly to detect fraud and report it immediately.

If you think your identity has been compromised or stolen

Many banks and financial institutions offer free identity theft resolution services where seasoned professionals know exactly what to do to determine if your identity has been compromised and lead you through the process of reclaiming your good name.

If your bank does not provide this service, take the following steps immediately:

- Contact the fraud departments of all three consumer reporting companies* to place a fraud alert on your credit report.
- Close the accounts that you know or believe have been tampered with or opened fraudulently.
- Contact all creditors and financial institutions with whom your name or identifying data have been fraudulently used.
- File a 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 least the number of the report and submit it to your creditors and others that need proof of the crime.
- File a complaint with the Federal Trade Commission. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.
- Contact your local post office if you suspect that an identity thief has submitted a change of address form at the Post Office.
- Contact the Social Security Administration if you believe your Social Security number is being used by someone else.

Identity theft is one of the most insidious crimes facing consumers today. Understanding that there are steps you can take to protect yourself, and knowing that your financial institution, as well as other businesses, organizations and even the Federal government are allies in both prevention and recovery goes a long way to easing fears. We never think something like this will happen to us, but it can and does. Be proactive. Stay alert. Act immediately whenever you believe there is cause for concern.

Resources

Credit Reporting Agencies

Equifax	(888)766-0008	www.equifax.com
Experian	(888)397-3742	www.experian.com
TransUnion	(800)680-7289	www.transunion.com

Social Security Administration

(800)269-0271 www.ssa.gov

Federal Trade Commission Identity Theft Clearing House

(877)IDTHEFT (877-438-4338)

www.consumer.gov/idtheft

Get "Take Charge", an online free identity theft guide

Other online Resources

Identity Theft Resource Center

(858)693-7935

www.idtheftcenter.org

Privacy Rights Clearinghouse

(619)298-3396

www.privacyrights.org

American Association of Retired Persons

www.aarp.org/learntech/personal_finance/identity_theft

Information in this article was compiled by the Marketing Department at First Independent Bank and came from a variety of sources including the Identity Theft Resource Center, The Federal Trade Commission, the US Department of Justice and the Privacy Rights Clearing House