American Consumer Credit Counseling

The Credit Counseling Professionals

Identity Theft Protection

What is Identity Theft?

Identity theft occurs when someone uses your personally identifiable information, like your name, social security number, or credit card number, without your permission to commit fraud or other crimes.

12.7 Million adults were victims of identity theft in 2014, with a total amount of $16 Billion stolen

(Javelin Strategy & Research Identity Fraud Study, 2015)

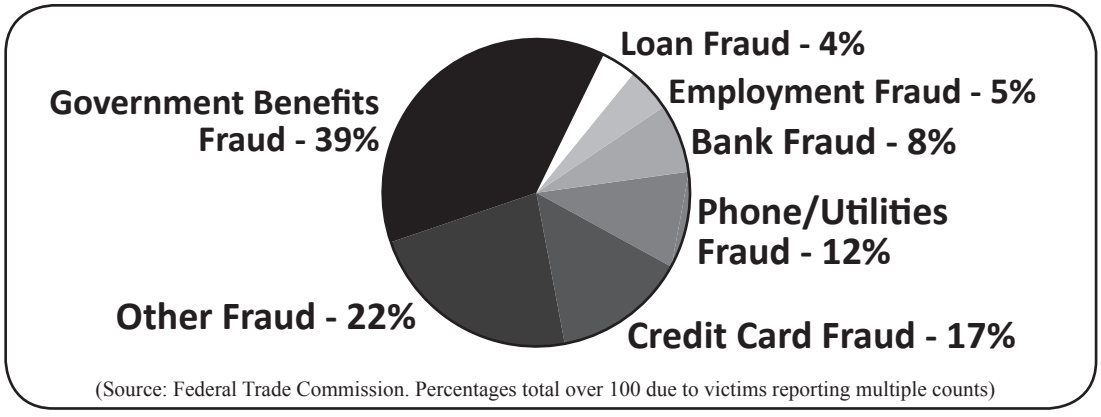
What Do Identity Thieves Look For?

- Name
- Address
- Social Security Number
- Date of Birth
- Bank Account Numbers
- Credit Card Numbers
- PIN Numbers
- Signature
- Health Insurance Number
- Any Answers to Security Questions...
  - (mother's maiden name, first pet's name, etc.)

In 95% of cases, information was used to open an account in the victim's name

How Your Information is Misused

Here are the most common ways that thieves use stolen information, and how frequently they occur among ID theft cases...



(Source: Federal Trade Commission. Percentages total over 100 due to victims reporting multiple counts)

Document #: ED REF017 r(2)
Effective Date 9/30/15

How Does Identity Theft Occur?

Identity theft can occur in a number of ways. Thieves use several methods to obtain the information they need. Some are old, some are new, but all can be effective in wreaking havoc on your finances. With simple precautionary measures you can protect yourself from theft.

Dumpster Diving

Thieves will literally dig through your garbage looking for documents that contain your personal information, such as bank and credit card statements, utility bills, etc.

Prevention:

- ***Shred personal and financial documents before disposing.***

Mail Theft

Any unlocked mailbox on the street could be susceptible to mail theft. Someone could walk by and grab an envelope containing private information, or even a check.

Prevention:

- ***Put outgoing sensitive mail in a blue USPS mailbox.***
- ***Bring outgoing mail to the post office.***
- ***Use online bill payment services.***
- ***Use a PO Box or mailbox with a lock.***

Tip: Never carry your social security card or number on your person

Stolen Wallet / Purse

Your wallet/purse probably contains your IDs, credit cards, insurance card, and maybe your check book. With these items, a thief could make purchases, empty accounts, or even open new accounts in your name.

Prevention:

- ***Keep your wallet/purse close to you.***
- ***Never leave it unattended.***
- ***Know what's inside in case of theft.***

How Do Thieves Use Technology?

Skimming

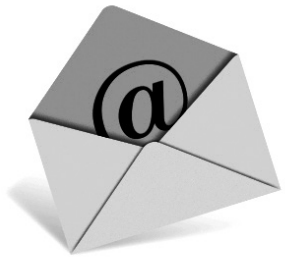
Thieves place their own "skimmers" over the card slots on ATMs, gas stations, store check out lines, etc. so that they can capture the information on your card. They will then create duplicates of your card for their own use. They may also use cameras pointed at the keypads to watch you enter your PIN.

Prevention:

- ***Anytime you swipe your card, inspect the device for loose or mismatched parts and anything out of the ordinary.***
- ***Cover the keypad with your hand whenever you enter your PIN to hide it from cameras or onlookers.***

Phishing/Email

Phishing is when you receive an email or a pop-up ad claiming to represent a financial institution or company, asking you to verify personally identifying information.



Prevention:

- ***Do not respond to such emails, or click any links.***
- ***If you wish to do any business online, visit the correct website by typing in the official URL yourself. Othewise call the institution directly.***
- ***Report phishing emails to the FTC by forwarding to spam@uce.gov.***

Malware

Malware is malicious software that can gather sensitive information or gain unauthorized access to computers. Malware can infect your computer if you click pop-up ads, unfamiliar links, or download music or videos from illegitimate sites. Some malware may even disguise itself as protective software, telling you that you're in danger, and to click a link for protection.

Prevention:

- ***Do not download illegal copies of music or videos.***
- ***Do not click on pop-up ads or run unfamiliar programs.***
- ***Install anti-virus software from a reputable company.***
- ***Do not respond to or click unfamiliar notifications.***
- ***Use creative passwords for your accounts with mixes of numbers and letters, and avoid writing them down.***

How to Monitor Your Identity

Credit Reports

- Review your credit reports at least once a year. You can check it for any incorrect information or fraudulent activity.
- You are entitled to one free credit report every year from each of the three credit reporting agencies (Experian, Equifax, TransUnion).
- You can get them all at once or stagger your requests every 4 months, so that you are monitoring your credit report as frequently as possible.

Request Your Free Credit Reports Online at AnnualCreditReport.com Or Call 1-877-322-8228

Monitor Your Accounts

- Review your bank and credit card statements every month and check for any unfamiliar activity.

Explanation of Insurance Benefits

- This document from your health insurance provider will outline any activity regarding hospital and doctor visits, procedures, etc.

What if You've Been Victimized?

1

Contact the 3 Credit Reporting Agencies

- www.Experian.com | 1-888-EXPERIAN
- www.Equifax.com | 1-800-525-6285
- www.TUC.com | 1-800-680-7289
- Contact each agency, and ask to place an identity theft alert on your reports.

2

Contact your Bank and Creditors

- You can report stolen/missing cards, and any fraudulent activity on your statements.
- You can close/freeze any accounts that have been tampered with.

3

Contact the Federal Trade Commission

- www.FTC.org | 1-877-ID-THEFT
- File a complaint with the FTC and you will receive a document verifying that you are the victim.
- Fill out the ID theft affidavit.

4

Contact the Local Police

- File a report with local police.
- Your identity should be treated like any other stolen property. Document and report the theft to begin the investigation.
- Get a copy of the report as evidence for re-securing your identity and removing the fraudulent charges.