OppenheimerFunds®
CEO Advisor Institute

Identity Theft:

How to Protect Yourself Against the Fastest Growing Crime in America

Just How Big of a Problem Is Identity Theft?

According to the Federal Trade Commission (FTC), identity theft topped its national list of consumer complaints for the 15th consecutive year in 2014. The numbers, and the damage, are staggering:

- 17 million Americans were victims of identity theft in 2014.
- $25 billion of financial losses in the U.S.
- $2,000 average loss per victim.

Identity thieves target people of all ages, from senior citizens to the youngest children—even the deceased have had their identities stolen.

This brochure will help you understand identity theft in its many forms and offer practical recommendations that will help you protect yourself and your family.

Your first line of defense against Identity Theft is you.

All statistics sourced from the Bureau of Justice Statics: Victims of Identity Theft, 2014.

What Is Identity Theft?

Identity theft occurs when criminals steal your personal information—including, but not limited to Social Security Number, credit card and bank account numbers, medical insurance card, driver's license number, even your address—with the intent of using it to assume your identity for the purpose of committing fraud. Criminals often use your identity to apply for credit cards and loans, steal your tax refund, and/or gain access to your assets and drain your bank accounts.

Identity theft is the fastest growing crime in America: Someone becomes a victim of identity theft every two seconds.[1]

The consequences of identity theft may be catastrophic. Victims may find themselves liable for purchases made with credit cards and repayments of loans obtained through the fraudulent use of their personal information. Identity thieves may run up medical bills in your name and, if they've used your personal information to obtain false identity documents, pretend to be you if they are arrested.

Repairing the damage to your credit history and reputation is often costly and always time consuming—the process may literally take years of phone calls, paperwork, and correspondence with creditors and others, not to mention potential legal fees.

While most people have a general understanding of identity theft, most also probably think it won't happen to them. This brochure explains just how easy it is to have your identity stolen, how to protect yourself using our three-pronged security cycle, and provides actionable ideas you and your family can use to protect your identity.

1. Source: CNN Money, "Identity Fraud Hits New Victim Every Two Seconds," 2014.

Who's Most at Risk for Identity Theft?

Everyone is at risk for identity theft. However, there are some shocking statistics of the higher susceptibility of identity theft within the following demographics.

Kids Under the Age of 19

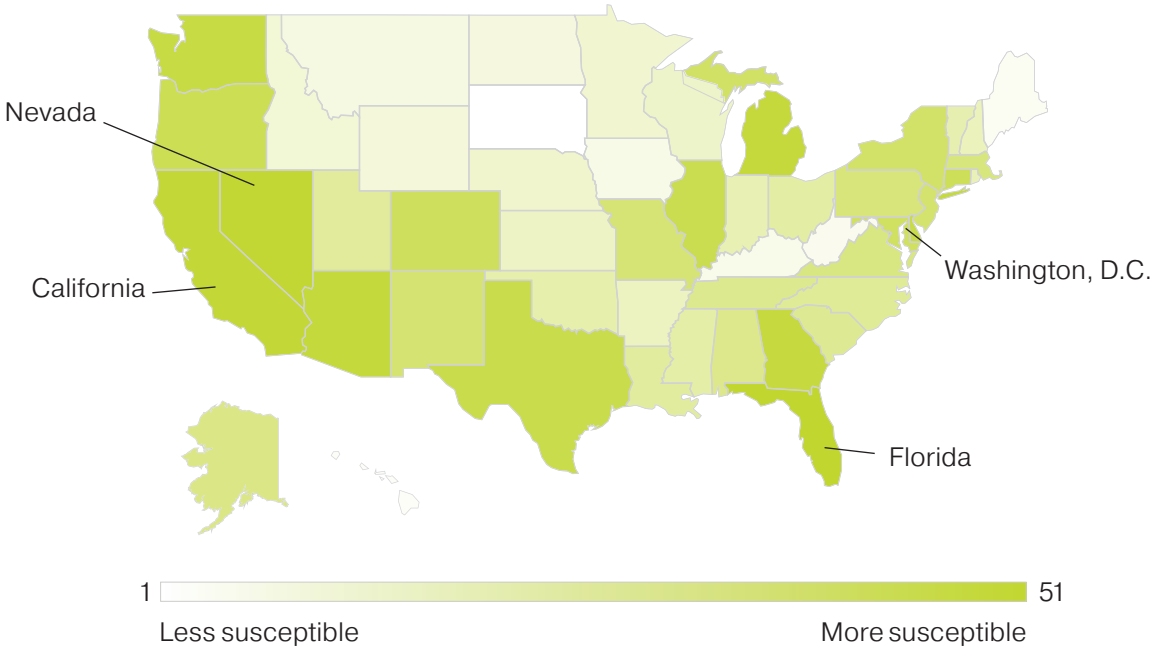
- 51 times more likely to become victims than adults.[2]
- Often doesn't build a credit history until later in life and, as a result, their credit reports are usually overlooked by parents. Thieves can have years to rack up debt without being discovered.

Senior Citizens

- Usually have large nest eggs and carry little debt.
- Don't check their credit reports generally, enabling identity thieves to use their information longer.
- Studies show they are more susceptible to digital theft and phone scams.

Residents of Florida, California, Nevada and Washington, D.C.[3]

- Residents in these locations tend to be more susceptible to identity theft.



2. Source: Carnegie Mellon University, CyLab Report, 2011.
3. Source: Money Magazine, "These States Are Most Vulnerable to Identity Theft and Fraud."

What's the Most Common Type of Identity Theft?

Identity theft may occur in a variety of ways and take many forms.

Types of Non-Financial Identity Theft

Criminal Fraud
Provides your identification when he/she is given a traffic ticket or arrested.

Medical Fraud
Steals your health insurance information and charges medical procedures to your insurance company under your name.

Children's Identity Theft
Steals a minor's identity and uses it for personal gain.

Identity Cloning
Steals multiple aspects of your identity and assumes your identity to obtain credit cards, pursue jobs, establish cable, utility and telephone services, and even get married.

Synthetic Theft
Steals your SSN and ties it to his/her name and date of birth.

Employment Theft
Uses your stolen Social Security Number (SSN) to get a job and earn wages.

Identity Theft Case Study

Tom Manning answered a call one night from someone who said he was seeking payment for a hospital bill. Thinking it was a scam to get his information, Tom hung up on the caller, who called again later in the week. It wasn't until Tom received a call from the hospital that he realized he was a victim of a fraud. An identity thief had used Tom's Social Security Number when having leg surgery at the hospital. Tom, who had never had any surgery in his life, was billed $40,000 by the hospital. It took Tom more than two years to clear up his medical records and fix his credit.

Financial fraud is what likely comes to mind most often when people think about identity theft: Someone steals your financial information, typically your debit or credit card or banking account number, and uses it to make fraudulent purchases.

However, **financial identity theft accounts for only 26% of all identity theft.**[4]

Types of Financial Identity Theft

Banking Fraud

- Steals or duplicates your debit card, credit card or checks and uses them to make purchases.
- Opens a new credit card or account using your information.

Mortgage

- Refinances your home or takes out a home equity line of credit, leaving you responsible for repayment and subject to liens on your property.
- Creates a fake title to your home and sells it to a buyer.

Tax

- Steals your Social Security Number (SSN)/Tax ID Number to file a fraudulent tax return and receives tax refunds in your name.
- Uses your SSN/Tax ID to claim you as a dependent to minimize tax liability or increase their tax return.

Identity Theft Case Study

Jane Adams owned a house that had been in her family since the 1950s. In March 2014, an identity thief falsely filed a deed that transferred title of the house from Jane Adams to her then-deceased mother, Catherine. "Catherine Adams" then sold the house to a development company. Not knowing the deed was fraudulent, the development company evicted Jane, who was prevented from returning to the house for more than six months. Jane is still trying to clear her name.

4. Source: Federal Trade Commission Survey, 2015.

Children: The Most Frequently Targeted Victims of Identity Theft[5]

By using a child's SSN, identity thieves may access a clean credit slate that will likely go unexamined until the child applies for college loans or his or her first credit card. This provides identity thieves a potentially long runway of criminal activity before any red flags are raised.

Did you know that 1 out of 10 children were victims of Identity Theft?[5]

- 10.2% of the SSNs sampled in a Carnegie Mellon University study belonged to minors with active credit files.
- 76% of the credit activity was fraudulent.
- Fraudulent activity is likely to go unnoticed until the child attends college, applies for a job or attempts to open a credit card.

Identity Theft Case Study

Amanda Scott, age 16, has already purchased a home for $600,000 and charged up to $5,000 in credit card debt…or at least that was what she discovered when she reviewed her credit report with her father while researching colleges. An identity thief had used Amanda's Social Security Number to secure mortgages on two homes and activate multiple credit cards over a period of 10 years. As with many cases of child identity theft, it goes undiscovered for so long because credit checks are rarely run on minor children. Amanda only uncovered the fraud because she searched for financial aid options for her college education. It took Amanda about six months to clean up her credit and get back on track with her college financial aid applications.

5. Source: Carnegie Mellon University, CyLab Report, 2011.

How Identity Thieves Steal Information

Just as identity theft comes in many forms, identity thieves have just as many, if not more, ways to steal the information needed to commit fraud.

Direct Theft

Direct theft occurs when identity thieves physically steal documents, data or items that contain the information they intend to use to enable their fraudulent activities.

- **Wallet, Purse, Briefcase, Luggage Theft**
  Valuable information about you, including your name, address, DOB, driver's license number, credit cards, debit cards, medical insurance cards, checkbooks, passport, work ID, contact information and access to email and social media accounts.
- **Home Invasion**
  Computers, tax and estate planning documents, mail, wallets, purses, cell phones, passports, social security cards, birth and death certificates.
- **Mail Theft**
  Monthly bills, pre-approved credit card or loan offers, tax forms/refunds, paychecks, account numbers, employee ID information and more.
- **Dumpster Diving**
  Discarded mail and personal papers that contain information about account details.

Digital Theft

Digital theft is more subtle and often more difficult to detect until after the crime is committed because your information is never physically stolen.

- **Hacking**
  Use spyware, viruses or hacking tools to gain remote access to your computer and steal your passwords, credit card numbers, bank account information and personal data.
- **Social Engineering**
  Assumes the role of a person you may tend to trust (i.e., a banker) or via social media connections and tricks you into sharing valuable personal information.
- **Wireless Theft**
  Use of RFID devices is becoming more prevalent, which has led to the introduction of chips in credit cards.
- **Skimming**
  Places objects over PIN pads or cameras on ATMs.
- **Pharming & Phishing**
  Create illegitimate websites that mirror websites of banks or other financial institutions, then send you an email that appears to be from a familiar source and directs you to the fake site, where you're prompted to enter personal information.
- **Shoulder Surfing**
  An identity thief peers over your shoulder to learn your PIN or password information.

The Security Cycle

Protecting your identity starts with you.

By taking a common-sense approach to safeguarding your most valuable information, you can make it much more difficult for identity thieves to victimize you and your family members. Our three-pronged security cycle offers simple but highly effective methods to protect your identity that focus on:

Prevention

Follow these steps to help minimize the likelihood of becoming a victim of identity theft.

1

Reduce Your Paper Trail

- **Shred** unnecessary financial and/or credit/debit card account information.
- **Store** important financial and/or credit/debit card account information.
- **Go paperless** and use automated billing.
- **Opt out** of pre-approved offers/marketing calls.

2

Protect Your Cards

- **Don't carry** your social security card, keep it in a locked safe or desk drawer.
- **Limit** the number of credit cards you use/carry.
- **Monitor** your credit card activity and statements to be aware of any suspicious charges that may indicate fraud occurred.

3

Be Less Social on Social Media

- **Don't accept** friend requests from people you don't know.
- **Be suspicious** of unsolicited calls/emails trying to verify account information or personal data.
- **Limit** the details you show on social media sites. Information such as high school mascots, birthdays, pet names, maiden names, etc., are often used as security questions and can be found easily on social sites.
- **Update** your privacy settings so that only friends can see personal details.
- **Restrict** the amount of information you share about others such as children and deceased relatives/friends.

4

Think of Others

- **Protect others** in your household, including children or elderly parents as well as any deceased relatives.
- **Request credit reports** on your children annually.
- **Confirm** that all accounts of deceased relatives are closed.

Control Your Electronics

- **Use strong passwords** (include numbers and symbols), secure browsers (https) and secure wireless networks.
- **Be careful** of disposing printers, phones and other electronic devices.
- **Turn off devices** when not using them and be especially wary of any devices that have cameras attached to them.

5

Detection

Occasionally something may seem unusual, but we ignore it. Keep the following in mind to help detect fraudulent activities.

Look Out for Red Flags

- **Investigate** all unaccounted for charges. Call your bank or credit card issuer to find out more information.
- **Take notice** of missing bills and credit card statements.
- **Don't ignore** phone calls from debt collectors or credit-card issuers. These may be indications that your account has been compromised or your identity stolen.
- **Follow up** on any communication from the Internal Revenue Service regarding improper or duplicate tax information/filings.

Check Your Credit Report Annually

- **Monitor your credit.** Everyone may receive a free annual credit report. The three national credit reporting agencies are Experian, Equifax and Transunion. In addition to monitoring your credit score, you will also see your credit usage on all accounts open. Fraudulent accounts opened in your name will appear on this report.
- **Check your children's reports** as well for any fraudulent activity on their accounts.

Stay Alert

- **File an initial fraud alert** immediately with the national credit reporting agencies if you are a victim of identity theft or suspect you are. That will place a 90-day alert on your accounts and automatically opt you out of any pre-approved credit, loan or insurance offers.
- **Monitor** the additional credit reports you will have access to and check to see if this identity theft continues or appears in new accounts. The credit bureaus will be more thorough in any scrutinizing of new accounts created or extensions of credit with this alert on your account.

Recovery

Once you confirm that you are a victim of identity theft, follow these three steps to begin the process of recovering your losses, repairing your credit and restoring your reputation.

Act Fast

- **Dispute any unauthorized transactions** and report them to your payment card issuer's fraud department. They will freeze your account and begin work on recovering the missing funds.
- **File a complaint** with the Federal Trade Commission (FTC) detailing the events of the theft.
- **Create a case folder** and store copies of all documents and communications regarding the Identity Theft.
- **Provide written notification** to all three national credit bureaus (Experian, Equifax, and Transunion) and all companies/creditors at which your stolen information may have been used for unauthorized transactions to dispute charges, purchases, loans, etc. Be sure to send all correspondence via certified mail, return receipt requested.

Clear Your Name

- **Contact local law enforcement agencies** where Identity Theft-related crimes/infractions took place.
- **File a criminal complaint** of impersonation and contact your state attorney general's office.
- **Ask law enforcement personnel** to take your fingerprints, photograph and copies of other identifying documents. Once your identity has been verified, the law enforcement agency and local district attorney's office should issue a clearance letter.

Build a Recovery Plan

- **Replace your credit/debit cards** after notifying the proper law enforcement authorities and companies so you may access accounts again.
- **Protect yourself from future identity theft** by using the steps outlined in the Prevention section on page 10. Remember, once your information is stolen, it may be stolen again.
- **Engage a credit-monitoring service** to help detect future potential occurrences of identity theft.

Your Financial Advisor Can Help

If you are a victim of identity theft or suspect you are, your financial advisor can help.

1. Verify if you are a victim.
2. Create a customized recovery plan.
3. Change account numbers and credit cards.
4. Enroll in online statements and billing for accounts.
5. Answer questions regarding your credit report.

Five Actionable Strategies for Today

Identity Theft Prevention Check List

☐ **Opt-Out of Pre-Approved Offers**
Visit the official consumer credit reporting industry website: optoutprescreen.com that processes opt-in and opt-out credit and insurance offers.

☐ **Enroll in the Do Not Call Registry**
Make sure that your home and cell phones are on the National Do Not Call Registry.

☐ **Request Your Yearly Free Credit Report**
You are entitled to receive a free annual credit report. Be sure to request it and use it to make sure you are not a victim of identity theft.

☐ **Purchase a Safe and Shredder**
A safe will help protect your most valuable documents and data that need to be stored and used in the future. A shredder helps dispose of important documents, pre-approved offers, old billing and account statements, etc., you no longer need.

☐ **Use/Request a Chip for Credit Cards**
Debit and credit card issuers are adding security chips to payment cards to help protect against identity theft. If you haven't already received new cards containing the security chip, call your credit card company or bank to request them.

Know Your Allies

IdentityTheft.gov

- Government site to help with identity theft protection, detection and recovery.
- Source of your free annual credit report from the three credit reporting agencies Experian, Equifax and Transunion.

Federal Trade Commission

- File identity theft complaints with the FTC.
- Help customize a recovery plan.
- Tips about prevention, detection and recovery.

OppenheimerFunds®
CEO Advisor Institute

Visit Us
oppenheimerfunds.com

Call Us
800 225 5677

CA5000.111.0816 April 28, 2017