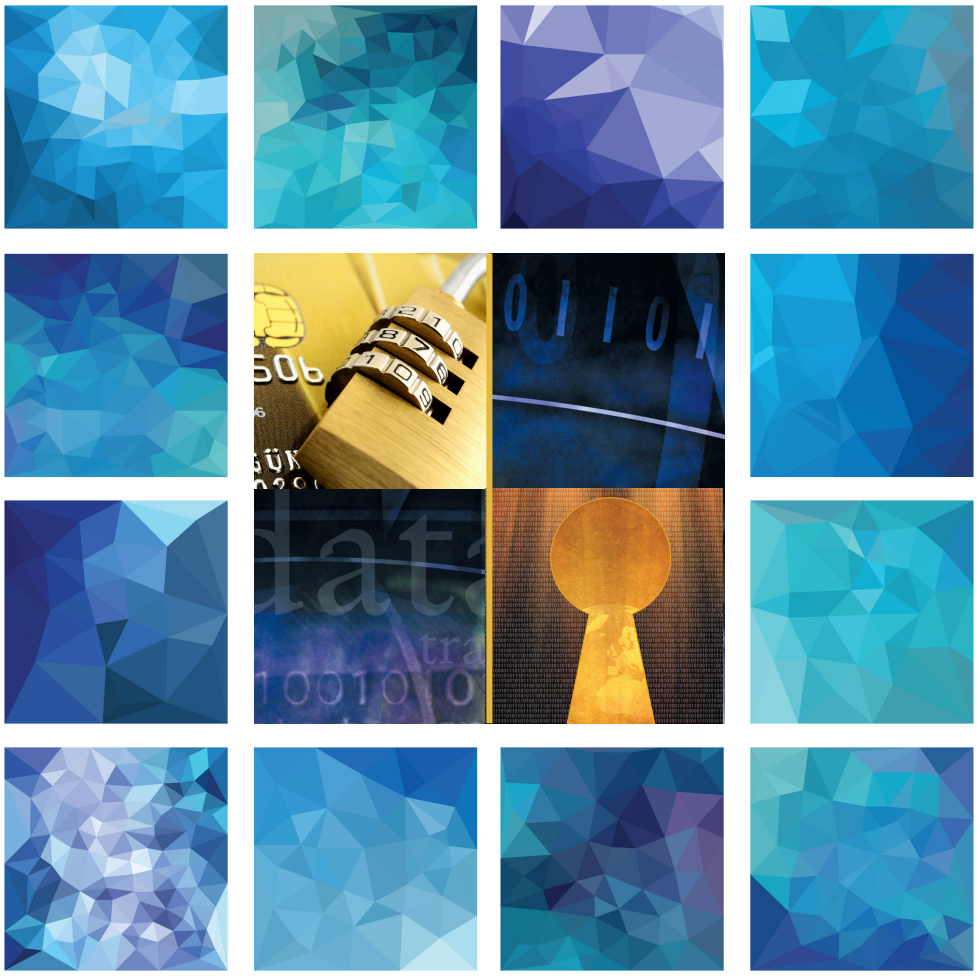
The Invisible Threat of Identity Theft and What to Do About It



Touchstone Investments®
DISTINCTIVELY ACTIVE®

How Serious is the Problem?

The threat posed by identity theft is more pervasive and the scams more sophisticated than ever, warns the Federal Bureau of Investigation.[1] Identity theft affects millions of people and costs billions of dollars in losses in the U.S. annually. No one is immune.

Identity theft occurs when a person's identification (which can include name, Social Security number, medical records, military ID or any account number) is used or transferred by another person for unlawful activities. By the time most victims learn what has happened, their credit is ruined. It usually takes months for a victim to become aware of a crime, so you could be at risk and not even know it.

Even large financial and retail businesses experience security breaches, putting their customers at risk for identity theft. While these institutions usually offer credit alert protection to those affected, one in four people who receive data breach notifications become a victim of identity fraud, underscoring the need for consumers to take all notifications seriously.[1]

Assess Your Risk

Here are some of the many actions – or inactions – that could put you at risk to become a victim of identity theft.

1. Do you throw bank statements, credit card offers, prescription bottle labels and receipts in the trash without shredding them?
2. Do you send outgoing mail from home?
3. Do you provide your Social Security or medical insurance ID number without asking questions about how the information will be safeguarded?
4. Do you carry your Social Security or military ID card in your wallet?
5. Are you required to use your Social Security or military ID number as an employee ID or at college as a student ID?
6. Do you neglect to review the privacy policy statements of your credit cards and consumer websites?
7. Do you share personal information on social networking sites?
8. Do you forget to log off when doing online banking or when on social media sites?
9. Do you use public computers for Wi-Fi internet access to your private accounts?
10. Did you forget to secure your phone with a screen lock that activates after a short period of inactivity?

If you answered "YES" to any of these questions, your risk for becoming an Identity Theft victim is increased.

How Do Thieves Get Your Information?

Thieves get information by stealing your wallet or purse, by using skimming devices, by obtaining access to billing statements or other financial and medical records. Many times, thieves will go through your trash to find credit card bills, cancelled checks and even junk mail for pre-approved credit card offers. Your personal information from loan and credit card applications is at risk, as are your files at hospitals, banks, schools and businesses.

Thieves will also listen in on your conversations in public, and look over your shoulder when you are entering your passcode at an ATM machine or using your computer in a public place. They will also use information from ATM and gas pump skimming devices, social networking internet sites, bogus emails and unsecured Wi-Fi computers.

Three other scams are Vishing – where you are tricked into giving information over the telephone; Phishing – where you are sent an email; and SMiShing – where you are sent a text message that contains a link to a fraudulent website or phone number. If your computer becomes infected with malware or spyware, thieves can steal your passwords and other personal information, and install key logging software that tracks your keystrokes.

[1] *www.fbi.gov/investigate/white-collar-crime/identity-theft, January 2019*

Five Common Types of Identity Theft

Financial ID Theft	Typically focuses on your name and Social Security Number	Thief may: • Apply for telephone service • Take out credit cards or apply for loans • Buy merchandise • Lease cars or apartments
Child ID Theft	Thief uses a minor's personal information (name, DOB, Social) to grain credit or other benefits	• Discovery can go undetected for long periods of time • Can range in severity from single fraudulent bill to foreclosed mortgages
Criminal ID Theft	Thief provides your information when stopped by law enforcement	Warrant for arrest will be written for name of the person issued the citation – you
Medical ID Theft	Thief provides your personal, financial and medical insurance information when seeking medical services and prescriptions	Services are provided and submitted to your medical insurance provider for payment
Synthetic ID Theft	Thief uses your information to establish a new life and works and lives as you	Examples: Illegal aliens, criminals avoiding warrants, people hiding from abusive situations and individuals wanting to become a "new person" to leave behind poor work/financial history

Protecting Your Assets

The information thieves could obtain is more than enough to open accounts and take out loans in your name. Take action today. Institute these important recommendations and make them part of your normal routine.

1. Social Security Number

- Guard it closely
- Before providing your Social Security number, ask if another piece of ID can be used
- Never provide your Social Security number to an unverifiable source
- Never carry your Social Security card with you

2. Checks

- Provide only your first initial and last name printed on checks
- Use work phone number and P.O. Box as address if you have one
- Use only last four digits of account on "For" line when paying bills
- Close inactive accounts

3. ATMs

- Inspect ATMs closely before using – thieves are attaching skimming devices
- Memorize your pin and never write it on the back of your card or keep it in your wallet
- Always shield keypad

4. Credit Cards

- Monitor your credit report regularly
- Match credit card receipts and statements, and report any discrepancies immediately
- Destroy old and expired credit cards
- Close inactive accounts
- Protect using an RFID-blocking wallet or purse

5. At Home

- Use a shredder for all documents containing sensitive information
- Keep copies of your driver's license and back and front of credit cards in secure place in case they are stolen
- Keep digital medical records secure using a password
- Protect your medicare card as it displays your social security number

6. Mail

- Put mail on "vacation hold" at the post office when traveling
- Do not mail bill payments and checks from home mailbox
- Check with post office if you do not receive mail for two consecutive days
- Remove your name from marketing lists: Mail: www.dmachoice.org

7. Telephone

- Respond with "speaking," never "yes," when asked to verify name on phone
- Never give personal information or credit card numbers over phone
- Instruct children what information they should not give on the phone
- Secure smartphone with screen lock

8. Computer

- Install up to date virus and firewall programs and use secure browsers; enable pop-up blockers
- Do not click unknown links or open attachments in unsolicited emails
- Never use public Wi-Fi to access personal files; log-in directly
- Avoid sharing personal information through email or on social media sites and lock down privacy settings

9. Passwords

- Do not use numbers related to birthdays, anniversaries, Social Security number, phone number, names of family members, friends, pets, etc.
- Never tell anyone your passwords or put in writing
- Change passwords at regular intervals
- Consider using two-factor authentication

What Are the Warning Signs?

Victims of identity theft may receive collection calls, or have credit denied although they believe they have a good credit score. They discover unauthorized charges on medical or credit card bills or receive bills on accounts never opened. They may miss a bill for a billing cycle. They may have their driver's license revoked.

If You Are A Victim . . . Action Plan

If you fall victim to identity theft, taking immediate action can help protect your credit and start the process of clearing your name. While this process can be frustrating and may take weeks, months, or even years, it's up to you to create a personal recovery plan and fix the damage caused by thieves.

Immediate Steps

- File a police report and keep a copy as evidence.
- File a fraud alert with national credit bureaus Equifax, Experian and TransUnion. This alert requires lenders to call you to verify your identity prior to granting credit in your name. Some states allow you to place a credit "freeze" on your credit report.
  - Equifax – Freeze Credit Report: 888-298-0045.
  - Experian – Freeze Credit Report: 888-397-3742.
  - TransUnion – Freeze Credit Report: 800-916-6800.
- Notify all financial institutions with which you do business; cancel credit cards and stop payment on outstanding checks.
- File your case with the Federal Trade Commission (FTC). The FTC enters all complaints into its database, to be is used by law enforcement.
- Send creditors a copy of your ID theft report.

Next Steps

- Keep all evidence. You are building a case to present to creditors, so don't discard anything. Keep detailed records of your conversations and people spoken to, and copies of all your correspondence.
- Do not pay any bills that are not yours. Paying appears as if you are admitting the bill is yours.
- Do not change your Social Security number, even if it was used in identity theft.
- If the Department of Motor Vehicles verifies that your driver's license number is being used by an impersonator, do get a new license and cancel the old one.

Resources to Assist You

Credit Reporting Bureaus

You may be entitled to receive free annual credit reports in some states. Check with the following resources:

- **Equifax:** To report fraud: 800-525-6285; to order credit report: 866-349-5191 or Equifax.com
- **Experian:** To report fraud or to order credit report: 888-397-3742; or Experian.com
- **TransUnion:** To report fraud: 800-680-7289; to order credit report: 800-888-4213 or TransUnion.com
- **Order a free annual credit report:** 877-322-8228 or AnnualCreditReport.com

Other Organizations

- IDTheftCenter.org or 888-400-5530 – provides support and advice to victims
- Identity Theft Survival Kit: IdentityTheft.org
- Federal Trade Commission Identity Theft – IdentityTheft.gov or 877-IDTHEFT (438-4338)
- Department of Justice ID Theft website – Justice.gov/Criminal-Fraud/Identity-Theft
- www.irs.gov/newsroom/Taxpayer-Guide-to-Identity-Theft

Contact your financial professional who can provide you with more information and valuable resources.

Touchstone Investments®
DISTINCTIVELY ACTIVE®

800.638.8194 • TouchstoneInvestments.com

Touchstone Funds are distributed by **Touchstone Securities, Inc.**
A registered broker-dealer and member FINRA and SIPC
Touchstone is a member of Western & Southern Financial Group