WHAT is IDENTITY THEFT?

Identity theft occurs when someone uses your personal identifying information like your name, Social Security number, or credit card number without your permission to commit fraud or other crimes. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector. Some consumers victimized by identity theft may lose out on job opportunities or be denied loans for education, housing, or cars because of negative information on their credit reports. They may even be arrested for crimes they did not commit.

HOW do thieves steal an identity?

Skilled identity thieves may use a variety of methods to get your information. Be cautious of these types of common scams:

PHISHING

They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.

SOCIAL MEDIA

They can gather a significant amount of personal information from social media accounts which can be used to authenticate your identity.

HACKING

Tech savvy thieves hack into online databases to obtain stored personal information.

IRS SCAMS

Fake IRS contacts are informing victims that in order to receive additional tax-stimulus rebates, they need to verify bank account information.

TELEPHONE SOLICITATIONS

Fast-talking thieves can convince you to provide financial information over the phone.

DUMPSTER DIVING

They rummage through trash looking for bills or other paper with your personal information on it.

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.

DATA BREACH

Thieves steal secure information from trusted sources. Malicious data security breaches are a steadily growing threat.

HOW do they use a stolen identity?

Identity theft is a broad crime, encompassing several things a person can do if they get access to your personal information.

CREDIT CARD FRAUD

- They may open new credit card accounts in your name.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account.

BANK/FINANCE FRAUD

- They may create counterfeit checks using your name or account number.
- They may take out a loan or open a bank account in your name and write bad checks.

GOVERNMENT DOCUMENTS FRAUD

- They may get a driver's license or official ID card issued in your name but use their photo.
- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.

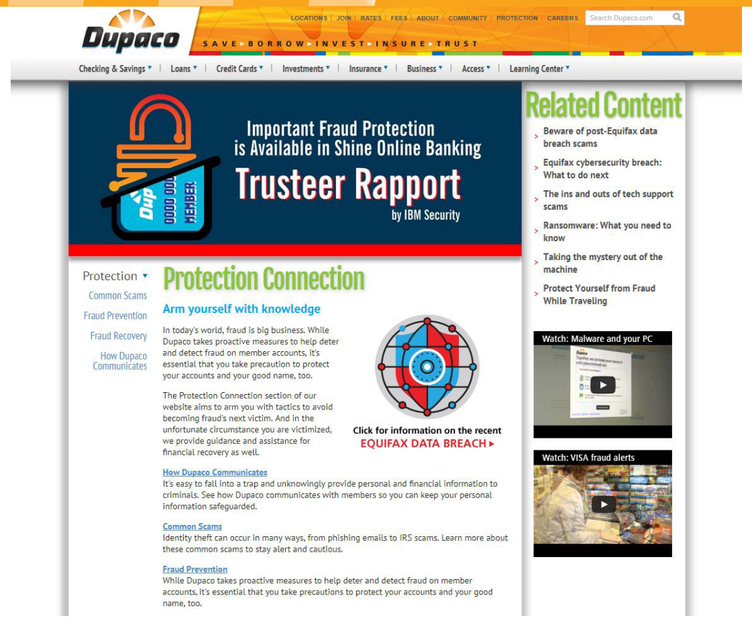
OTHER FRAUD

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

One of the most common way to become victimized is through data breach.

FRAUD ALERT

dupaco.com/fraud



Protect your credit and your good name with help from Dupaco

Through Shine Online and Mobile Banking, as a no-cost benefit of your credit union membership, Dupaco offers tools to keep you in the know about your accounts and credit.

- Regularly log in and view Dupaco account activity through Shine – through Dupaco.com or Dupaco's mobile app.
- Within Shine, enable eNotifers to receive automatic text or e-mail alerts about transaction activity and online banking sign-ins.
- Use Bright Track, also within Shine, to access your full credit report and validate that all credit accounts reporting to the credit bureau are accounts you opened.
- Use Bright Track to monitor changes in your credit score and see new credit inquiries.

With Family ID Restoration coverage from Dupaco, should you become the victim of identity theft, the protection will help you restore your credit.* For $1.95 per month, the coverage provides you a Certified Resolution Specialist who will work on your behalf to repair the damage done by identity theft, including working with credit bureaus, the Social Security Administration, the U.S. Postal Service, the police department, the Department of Motor Vehicles, the Internal Revenue Service and your financial institution(s).

To enroll in this protection service, or for help with Shine, Bright Track, or eNotifiers, call Dupaco at 800-373-7600.

**Family ID Restoration coverage must be in place at the time of the covered event. Coverage is not retroactive.*

Dupaco

Protecting YOUR IDENTITY

Every two seconds another American becomes a victim of identity fraud. Understanding the seriousness of this crime is one of the ways you can fight back.

Dupaco

HOW should you keep your personal information secure?

Protecting your personal information can help reduce your risk of identity theft. There are four main ways to do it: know who you share information with; store and dispose of your personal information securely, especially your Social Security number; ask questions before deciding to share your personal information; and maintain appropriate security on your computers and other electronic devices.

Keeping Your Personal Information Secure Offline

- **Lock your financial documents and records in a safe place** at home, and lock your wallet or purse in a safe place at work. Keep your information secure from anyone who comes into your home.
- **Limit what you carry.** When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you—unless you are going to use your card at the doctor's office.
- **Ask before you share** information at your workplace, a business, your child's school, or a doctor's office why they need it, how they will safeguard it, and the consequences of not sharing.
- **Shred** receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you no longer need them.
- **Destroy the labels on prescription bottles** before you throw them out.
- **Promptly remove mail that arrives in your mailbox.** If you won't be home for several days, request a vacation hold on your mail.
- **Consider opting out** of prescreened offers of credit and insurance by mail. You can opt out for five years or permanently. To opt out, call 1-888-567-8688 or go to optoutprescreen.com.
- **Check your credit report annually** for any unfamiliar accounts or charges.

Keeping Your Personal Information Secure Online

- **Know who you share your information with.** Store your personal information securely.
- **Be alert to impersonators.** Don't give out personal information on the phone, through the mail, or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement.
- **Safely dispose of personal information.** Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. Before you dispose of a mobile device, check your owner's manual or the service provider's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.
- **Encrypt your data.** To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted.
- **Secure your browser.** Always use a secure browser. Look for "https" at the beginning of the web address. Access your accounts from a secure location using computers and networks that you know are safe and secure.
- **Keep passwords private.** Use strong passwords with your laptop, credit, bank, and other accounts. Be creative. Think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters.
- **Don't overshare on social networking sites.** If you post too much information about yourself, an identity thief can find information about your life, use it to answer "challenge" questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.
- **Securing your Social Security number.** Keep a close hold on your Social Security number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your Social Security number or your child's, ask:

  a. Why they need it
  b. How it will be used
  c. How they will protect it
  d. What happens if you don't share the number

  The decision to share is yours. Sometimes you will have to share your number. Your employer and financial institutions need your Social Security number for wage and tax reporting purposes. A business may ask for your Social Security number so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

Keeping Your Devices Secure

- **Use security software.** Install anti-virus software, anti-spyware software, and a firewall. Update these protections often. Protect against intrusions and viruses that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.
- **Avoid phishing emails.** Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

Be Wise About Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Clues That Someone Has Stolen Your Information:

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

THE CHANCES OF BEING A VICTIM OF:

Violent Crime: 1 in 5,000
Heart Disease: 1 in 2,600
Auto Accident: 1 in 130
Identity Theft: 1 in 27

WHAT should you do if your identity is stolen?

Filing a police report, checking your credit reports, notifying creditors, and disputing unauthorized transactions are some of the steps you must take immediately to restore your good name.

- Place a "Fraud Alert" on your credit reports and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. Placing a fraud alert entitles you to free copies of your credit reports.
- Close any accounts that have been tampered with or established fraudulently. Call the security or fraud departments of each company where an account was opened or changed without approval. Ask for verification that the disputed account has been closed and the fraudulent debts discharged.
- File a report with law enforcement officials to help you with creditors who may want proof of the crime. You should also report the theft to the Federal Trade Commission. Your report helps law enforcement officials across the country in their investigations.

ITEM	HOW TO TRACK	TIPS
Telephone Calls	Create a log of all telephone calls.	Record the date of each call and the names and telephone numbers of everyone you contact.
Postal Mail	Send letters by certified mail. Ask for a return receipt.	Keep all originals. • Send copies of your documents and reports, not originals. Make copies of your identification to include.
Documents	Create a filing system.	Sample letters can be found here: www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft
Deadlines	Make a timeline.	List important dates, including when: • You must file requests • A company must respond to you • You must send follow-up

WHAT about child IDENTITY THEFT?

A child's Social Security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, or apply for a loan. Check for a credit report to see if your child's information is being misused. Take immediate action if it is.

Many school forms require personal and sensitive information. Find out how your child's information is collected, used, stored, and thrown away. Asking schools and other organizations to safeguard your child's information can help minimize your child's risk of identity theft.

As a parent, you have control over the personal information companies collect online from your kids under 13. The Children's Online Privacy Protection Act (COPPA) gives you tools to do that. If a site or service is covered by COPPA, it has to get your consent before collecting personal information from your child.

MORE information?

Federal Resources

National Do Not Call Registry
www.donotcall.gov

Credit Card Solicitation Opt-Out
www.optoutprescreen.com

National Credit Reporting Agencies

Annual Credit Report Request Service
A service created by these three companies to order your free credit reports each year.

www.AnnualCreditReport.com
(877) 322-8228

Federal Trade Commission

www.ftc.gov
www.identitytheft.gov