IS

ShareThis

OUR IDENTITY SAFE?



# called new account fraud. This happens when a criminal steals your personal information, opens credit or other accounts in your name and goes on a spending spree.

**Enroll By Phone** 

PROTECT YOURSELF NOW

# **Useful Tips To Protect Your Identity**

To minimize your risk of becoming a victim of identity theft, be very careful with your personal information.

Here are a few important suggestions regarding common circumstances faced throughout the day

#### Your Bank Statement

- → Review your bank and credit card statements monthly for signs of suspicious activity. Immediately contact the company if an item looks suspicious.
- If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

#### Your Car

- → Do not leave any personal information in your car
- → If your car is broken into, report it to the police immediately
- When buying a new car from a private individual, make sure the title an registration match the name and address of the person selling the car Be cautious of a seller with no fixed address, place of employment, or phone
- number

# **Your Computer**

- → Do not keep computers online when not in use. Either shut them off or physically disconnect them from Internet connection Use anti-virus software and a firewall, and keep them up to date. Some
- phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge
- → Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security. If you get an email or pop-up message that asks for personal or financial
- information, do not reply. And don't click on the link in the message, either.

## **Your Credit Cards**

- → Do not hand over your ATM/Debit Cards or Credit Cards to anyone.
- Cancel all unused credit card accounts. Even though you do not use them, their account numbers are recorded on your credit report. Avoid paying by credit card if you think the business does not use adequate
- safeguards to protect your personal information.

### Your Credit Report

- → Check your credit reports from the three major credit bureaus, Equifax Experian and TransUnion, at least twice a year and correct any inaccuracies.
- Experian and Transchion, at least twice a year and correct any maccuracies. Order a copy of your credit report. An amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit reports, at your request, once every 12 months. To order your free annual report from one or all the national consumer reporting companies, visit <a href="https://www.annualcreditreport.com">www.annualcreditreport.com</a>, call foll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it for Annual Credit Report Request Form and mail it for Annual Credit Report Recognition from <a href="https://doi.org/10.1007/j.com/credit.">fc.gov/credit.</a> Do not contact the three nationwide consumer reporting companies individually they provide free annual credit reports only reporting companies individually; they provide free annual credit reports only through www.annualcreditreport.com
- Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports.

#### Your Financial Accounts When you open new accounts, place passwords on them.

- Add passwords to your credit card, bank and telephone accounts that are not the typical passwords, such as the last four digits of your Social Security number, your birth date, your mother's maiden name, your phone number, or a series of consecutive numbers. If you are opening a new account that requests your mother's maiden name, use a password instead.

# Your Home

- → Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done. → If your house or car was broken into, report it to the police immediately

# Your Mail

- Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox.
- If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it. When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.
- Remove your name from mailing lists by contacting the Direct Marketing Association at: Mail Preference Service Attention: Dept.9301235
- Direct Marketing Association P.O. Box 643 Carmel, NY 10512 Opt out of receiving offers of credit in the mail by calling: 1-888-5-OPTOUT (1-888-567-8688) or through the following website: www.o The three nationwide consumer reporting companies use the same toll-free number to let consumers choose not to receive credit offers based on their
- consumer reporting companies need to match you with your file

# Your Phone Offers Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.

- Be wary of anyone calling you to "confirm" personal or financial information Often, these are criminals trying to obtain those facts under the guise of
- "confirmation" Stop receiving unsolicited calls. You may do so by contacting the National Do Not Call Registry either by phone at 1-888-382-1222 or online at <a href="https://www.donotcall.gov/">https://www.donotcall.gov/</a>. The registration is free of charge and is effective
- Never give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or you are sure you know who you're dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information.
- Before you share any personal information, confirm that you are dealing with a legitimate organization. Call the company back using a phone number from a statement or from the telephone book (not a phone number the person who is calling gives you). You may check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. For more information, see

How Not to Get Hooked by a 'Phishing' Scam.

### Your Social Security Number → Before providing identifying information, especially your Social Security number, ask if the information is required. Give your Social Security number only when absolutely necessary and ask to use other types of identifiers.

- → Remove your Social Security number from any identification you carry, such as checks, a driver license or your health insurance card. Both your health insurance company and the Department of Motor Vehicles will give you a new
- number if you request it. → If you ask, only the last four digits of your Social Security number will appear on your credit reports.
- Your Trash → Treat your trash carefully.

# To thwart an identity thief who may pick through your trash or recycling bins to

- capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. Preferably use a crosscut shredder, which cuts paper into confetti like pieces instead of strips → Carry only one or two credit cards in your wallet.

# Your Wallet

- → Carry only the identification information that you'll actually need when you go → Do not carry your Social Security card in your wallet; leave it in a secure place.
- → If your purse or wallet is stolen, report it to the police immediately. Your Workplace
  - Secure personal information in your workplace. Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information such as your paycheck

- → Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personally identifying information.
- Find out who has access to your personal information and verify that records are kept in a secure location. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential. → Ask about the disposal procedures for those records as well
- Chances are, you insure your home or car from theft or damage. Wouldn't you agree that protecting your identity is just as important?

Protect your most valuable asset - Your Identity! ENROLL NOW

Identity Protection. Life Protection.

800.640.0468

SEARCH

# Member Login/Signup Already a member? <u>Login</u> Become a member now: <u>Signup</u>

Not a member yet? Learn more

# Stay Informed

right to your Inbox





