## IDENTITY THEFT RED FLAGS

Mistakes on your bank, credit card or other account statements

Mistakes on the explanation of medical benefits from your health plan.

Your regular bills and account statements don't arrive on time.

Bills or collection notices for products or services you never received.

Calls, emails or notices from debt collectors about debts that don't belong to you.

A notice from the IRS that someone has used your SSN.

Mail, email or calls about accounts or jobs in your minor child's name.

## DID YOU KNOW?

People between ages 18-24 have the highest rate of ID theft.

People over 65 are less likely to experience ID theft, but spend more time resolving problems when a theft occurs.

## THREE CREDIT REPORTING AGENCIES

**EQUIFAX**
equifax.com/CreditReportAssistance; 866.349.5191

**EXPERIAN**
experian.com/fraudalert; 888.397.3742

**TRANSUNION**
transunion.com/fraud; 800.888.4213

## RESOURCES

This contact information may be helpful to you if you have questions about, or are a victim of, identity theft:

FEDERAL TRADE COMMISSION
ftc.gov/idtheft
877.438.4338

FBI INTERNET CRIME COMPLAINT CENTER (IC3)
ic3.gov
972.559.5000 Dallas Division

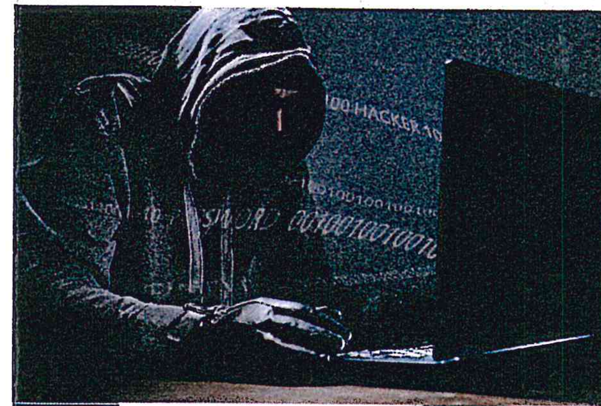
SOCIAL SECURITY ADMINISTRATION
ssa.gov/antifraudfacts
800.269.0271

OFFICE OF THE ATTORNEY GENERAL OF TEXAS
texasattorneygeneral.gov/identitytheft
800.621.0508 Consumer Protection Hotline

US POSTAL INSPECTION SERVICE
postalinspectors.uspis.gov
800.275.8777

DO NOT CALL (U.S.): donotcall.gov
TX DO NOT CALL: texasnocall.com


CDA White Collar Crimes/Public Integrity Unit
Chief: Harry E. White
401 W. Belknap
Fort Worth, TX 76196
817.884.1400

# Protecting Against Identity Theft


**Sharen Wilson**
**Criminal District Attorney**

## WHAT IS IDENTITY THEFT?

Identity theft happens when someone steals your personal information and uses it without your permission. It is a serious crime that can disrupt your finances, credit history and reputation, and requires time, money and patience to resolve. Using your information, criminals may:

- Open unauthorized charge accounts in your name
- Order goods or services billed to you
- Access your personal or business accounts
- Secure loans in your name
- Hide illegal funds or hide from law enforcement
- Gain employment by circumventing criminal background checks

## IDENTITY THIEVES WANT YOUR PERSONAL INFORMATION

- Social Security Number
- Mother's Maiden Name
- Date of birth
- PIN numbers
- Driver's license number
- Online logins/passwords
- Bank account or credit/debit card numbers

## HOW CAN THIEVES GET MY INFORMATION?

- Steal your wallet, purse, backpack, mail
- Monitor Internet transactions
- Watch you at ATM machines
- Go through trash stealing sensitive documents, bills, receipts
- Work for businesses, medical offices or government agencies and steal information on the job
- Ask for personal information "to qualify" for a phony prize
- Phony emails, notices, requests or calls claiming to be from a government entity or legitimate business

## PROTECT YOUR INFORMATION

- Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months.

- Check your bank, credit card and other account statements. Contact the business if a statement has a mistake or doesn't come on time.

- Shred old bank and credit card statements, or any other documents that show personal, financial or medical information. Shred discarded credit card applications and courtesy checks.

- Never give personal information to someone over the phone. Don't respond to emails, texts or phone messages that ask for personal information. Legitimate companies do not ask for information this way.

- Create passwords that mix letters, numbers and special characters. Don't use the same password for more than one account.

- If you shop or bank online, use only websites that protect your financial information with encryption. An encripted site has "https" at the beginning of the URL. The "s" is for secure. Always print out and save the receipt and transaction information.

- Do not pre-print your driver's license number, SSN or date of birth on your checks.

- Do NOT carry a list of PIN numbers in your purse or wallet.

- Use anti-virus and anti-spyware software, and a firewall on your computer.

- Register with the National and Texas Do Not Call Registries

## IF YOUR IDENTITY IS STOLEN

- If your wallet, checks or driver's license are stolen or lost, notify the TX Department of Public Safety, Social Security Administration, local law enforcement, credit card companies and your bank.

- If any credit card information has been stolen, contact the fraud/security department of the creditor or financial institution to close that account.

- Contact one of the three nationwide credit reporting companies to place a free fraud alert on your credit report. You will receive a letter from each bureau confirming they have placed an alert on your file. An initial fraud alert is good for 90 days (see back panel).

- Texas law also allows you to request a "Security Freeze" be placed on your consumer file, which requires the credit reporting agency to notify you of material changes to your consumer file and prevents access by some entities. You may request this by contacting each of the three credit reporting companies (see back panel).

- Create an Identity Theft Report. This can help get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name.
    (1) File a complaint with the Federal Trade Commission (FTC). Your completed complaint is called an FTC affidavit.
    (2) Take your FTC affidavit to your local law enforcement agency, or the police depart ment where the theft occurred, and FILE A POLICE REPORT. Get a copy of the police report. These two documents comprise an Identity Theft Report.