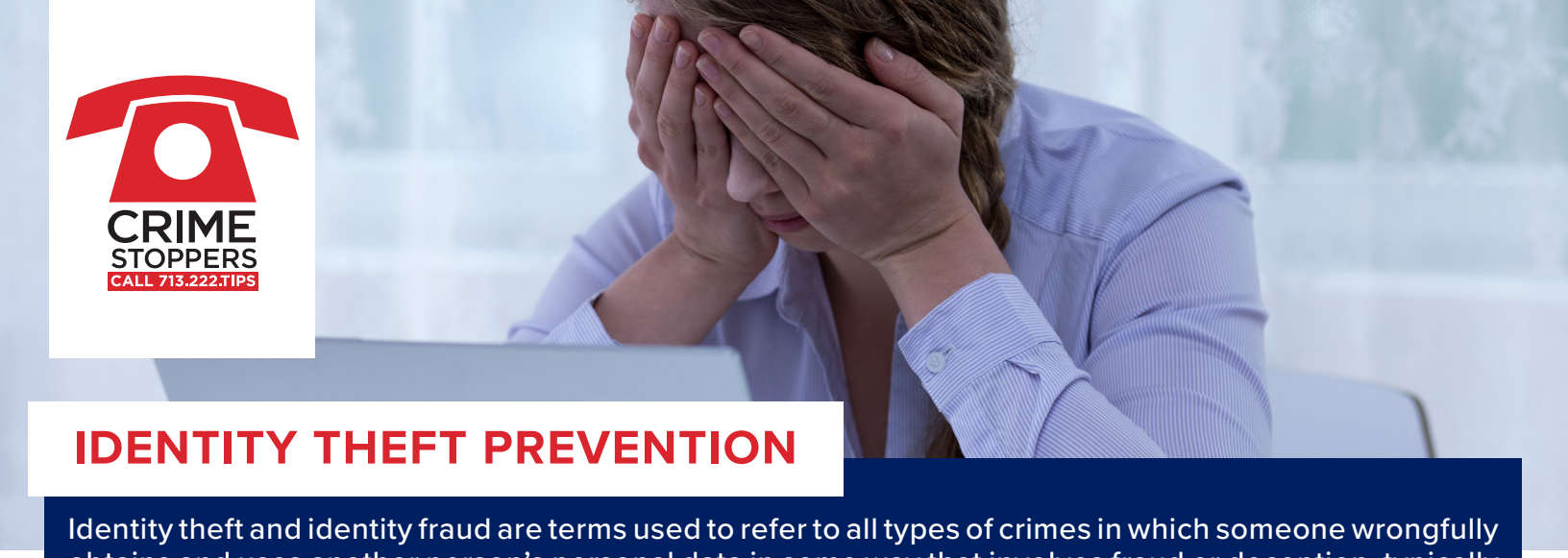
CRIME STOPPERS
CALL 713.222.TIPS



IDENTITY THEFT PREVENTION

Identity theft and identity fraud are terms used to refer to all types of crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain

Did you know?

- Financial crimes include forgery, credit/debit card abuse, identity theft, and mail theft
- Identity theft can occur through the following
  - Dumpster diving-- rummaging through your trash
  - Shoulder surfing-- watching you from a nearby location as you provide personal information
- In 2018 there were 14.4 million cases of identity fraud which is actually down since 2017. This is suspected to be because of the rise of microchips
- In 2015 many credit card companies introduced the microchip (EMV) making them difficult to counterfeit
- With the introduction of microchips, online preditors now focus on opening credit cards and accounts using a victim's name and other stolen personal information
- Even though the pure number of victims has fallen since 2016, the financial burded of those experencing financial fraud rose to nearly three times the reported burden in 2016
- Texas ranks 6th in the nation for the number of cybercrime victims
- Every year more than 25,000 Texans report being victims of identity theft
- Identity theft is one of the nation's fastest growing and most expensive criminal enterprises
- Identity thieves use the following electronic means:
  - Phishing--relies on pop-ups, spam, and website that look authentic to obtain personal information such as log in informatioin and credit card numbers
  - Pharming--uses malicious codes to redirect users to fraudulent sites where hackers can access their personal information
  - Pretexting-acquires personal information through false and illegal means, for example obtaining financial information by pretending to call from a bank

SIGNS THAT YOUR IDENTITY MIGHT HAVE BEEN STOLEN

- You stop receiving account statements at home in the U.S. mail
- You receive an account statement from an unrecognized company or from one that you do not recall opening
- You notice unfamiliar entries on your credit report
- You recieve phone calls from collection agencies or financial institutions informing you of delinquent accounts or suspicious activity

Credit agencies:

- Trans Union (1-800-680-7289 / www.tuc.com)
- CSC Credit Services (1-800-272-9281 / www.csccredit.com)
- Equifax (1-800-525-6285 / www.equifax.com)
- Experian (1-888-397-3742 / www.experian.com)

If You Are a Victim:

- Contact the fraud department of the credit company or bank.
- Request a copy of your credit report to look for further infractions.
- File a report with law enforcement and notify creditors if there is an incident or a suspicion of identity theft.
- Close your compromised account and open a new one.
- Change pin numbers and passwords.
- Keep records of phone calls, people you spoke to, dates, amounts, amounts lost, and anything pertaining to your case.
- If you report an ATM or debit card missing before someone uses it, the EFTA says you are not responsible for any unauthorized transactions. If someone uses your ATM or debit card before you report it lost or stolen, your liability depends on how quickly you report it:

  Before any unauthorized charges are made: max loss of $0.

  Within 2 business days after you learn about the loss or theft: max loss of $50.

  More than 2 business days after you learn about the loss or theft, but less than 60 calendar days after your statement is sent to you: max loss of $500.

  More than 60 calendar days after your statement is sent to you: max loss is all the money taken from your ATM/debit card account, and possibly more; for example, money in accounts linked to your debit account.

Protect Your Family's Identity:

- Never share your passwords.
- Do not carry your Social Security card with you unless you need it.
- Put yourself on the Federal No Call List (888-382-1222 or www.donotcall.gov).
- Lock your phones and computers with a strong password.
- Do not follow links from emails when conducting financial transactions – enter the URL yourself.
- Look for a lock symbol or "https" before purchasing from a website or entering personal information.
- Be cautious of pop-ups, websites, and emails asking for personal information.
- Minors can be victims of identity theft as well – talk to your children about how to react to pop-ups and being asked for personal information.
- Ensure your anti-virus software is up-to-date on your home computer and mobile devices.
- Review your account statements and credit reports frequently.
- Reduce the number of credit cards you have and only carry the cards that you intend to use, preferably ones with your photo on them.
- Shield your hand when entering your PIN at a bank ATM or when making long distance calls with a calling card.
- Shred any documents containing your personal information.
- Use a U.S. Post Office for sending and receiving mail - it is more secure than home delivery.

For more information:

www.ftc.gov
www.bjs.gov
www.statisticbrain.com/identity-theft-fraud-statistics

How to Report a Tip

Call 713.222.TIPS (8477)

Use our **Mobile App**
Download app name: Crime Stoppers Houston

Go to **crime-stoppers.org**

What are the most common types of identity theft?

> Employment or tax-related fraud (34%)
> Credit card fraud (33%)
> Phone or utility fraud (13%)
> Bank fraud (13%)
> Loan or lease fraud (7%)
> Government documents or benefits fraud (7%)