RISLA

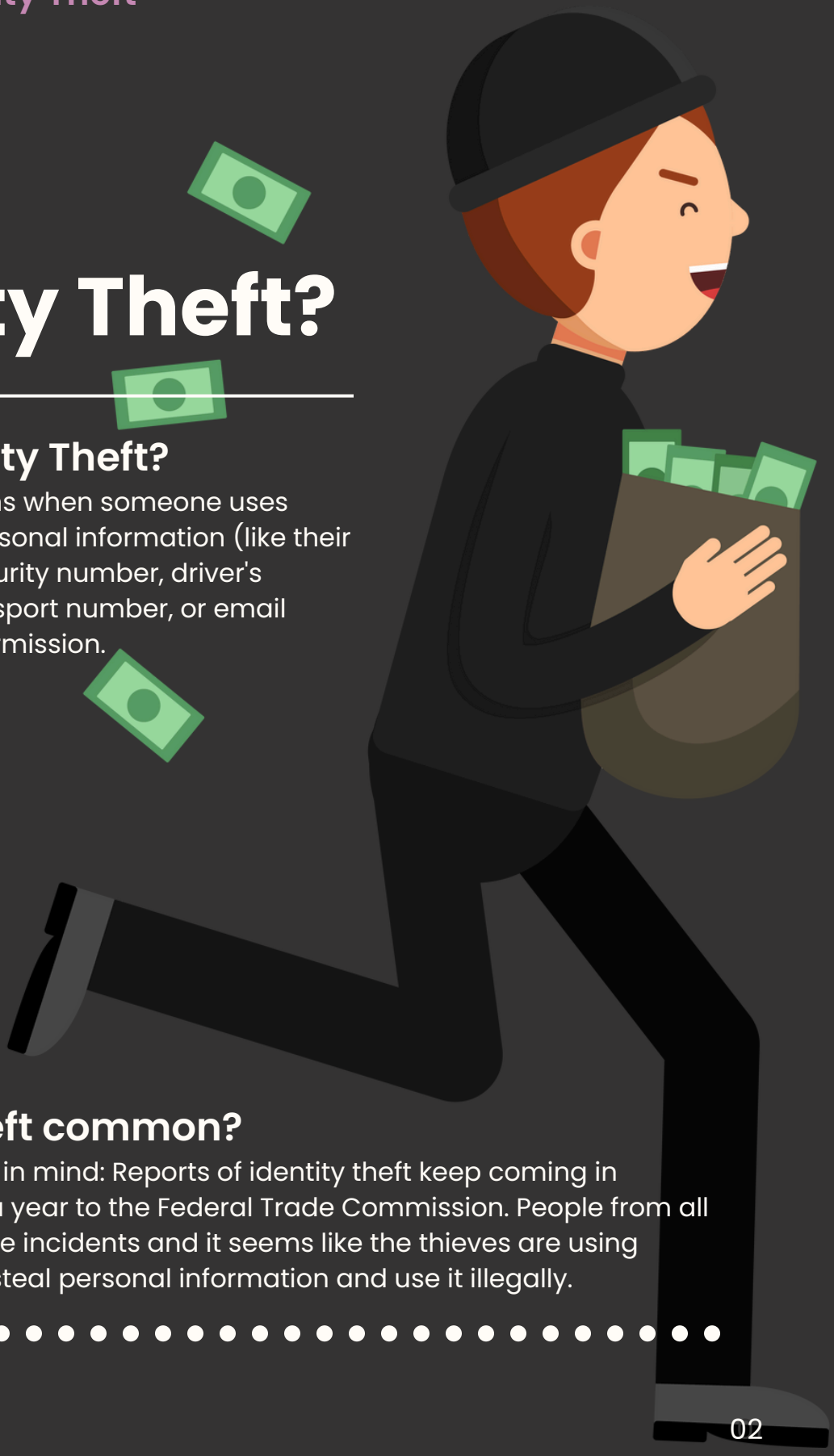
@ristudentloans

Identity Theft

Safeguarding your personal information.

risla.com

What is **Identity Theft?**



What is Identity Theft?

Identity theft happens when someone uses another person's personal information (like their full name, social security number, driver's license number, passport number, or email address) without permission.

Is Identity Theft common?

You should keep this in mind: Reports of identity theft keep coming in thousands of times a year to the Federal Trade Commission. People from all 50 States report these incidents and it seems like the thieves are using various methods to steal personal information and use it illegally.

Identity Theft

How does it happen?

Thieves can use one or more of these tricks to swipe all or just some of your personal and account info!

Skimming

- Refers to capturing your credit/debit card information to duplicate for use on a counterfeit card.

Phishing

- Involves sending falsified emails or pop-up alerts to tempt you into entering your personal information in exchange for a reward on a fake banking or other fraudulent website.

Cyber Attacks

- Ware Attacks: Malware, spyware, ransomware, adware, or other viruses and worms that execute keystrokes or report hidden computer activity.

Pretext Calls

- Are scammers pretending to be from an actual bank to steal your info.

CVV Code Scams

- Are fraudulent calls pretending to be from your bank, requesting your Card Verification Value (CVV) code to verify false charges.

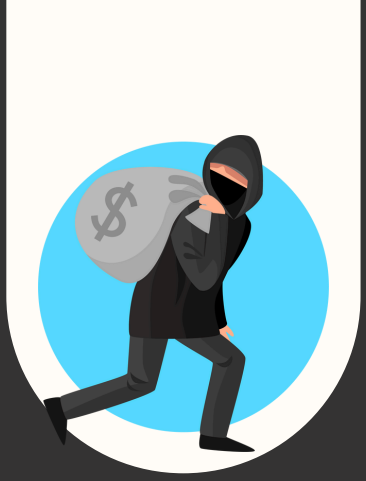
Phone Hijacking

- Is when someone steals or uses your cell phone to access a bunch of apps like credit card apps, email, online payment apps, etc. They can change your passwords for those apps, which gives them access to your information and might lock you out.

Don’t Forget

- About these techniques: dumpster diving (getting info from thrown-out documents), shoulder surfing (sneakily looking over your shoulder for info), bribing company employees with access, checking your social media for details like birth dates, pet names, maiden names, and family members' names, or just swiping your wallet, purse, or mail.

What's the Impact?



Misuse of personal information.

Identity theft has been a severe issue with far-reaching consequences. In today's world, identity thieves often target specific information to exploit for financial gain. It's imperative to understand the various ways in which modern identity thieves can misuse your personal information.

- Making unauthorized charges on existing credit accounts.
- Making unauthorized withdrawals on existing debit cards.
- Changing the credit/debit card billing address to prevent you from seeing unauthorized transactions.
- Ordering and using new checks with your bank account and routing number.
- Opening new credit accounts (credit cards, auto loans, and mortgages).
- Setting up new cell phone or utility services.
- Changing passwords for accessible apps that permit thieves continued access but prevent you from quickly accessing your account information.

Recovering stolen account info?

- Generally, the longer the stolen information is used inappropriately, the longer it will take to resolve the situation.
- An identity thief might use a stolen credit card to make cash-equivalent purchases until the card is declined. If the theft is noticed after a few purchases, the bank can more easily identify and reverse the fraudulent charges. However, if the thief continues making purchases over several months or years, it will take the bank longer to detect and reverse the charges.
- If the identity theft involved stealing enough information to obtain new credit, such as a mortgage, reversing more complex transactions can take years to rectify.
- By taking precautionary steps to protect your identity and account information, you can save a lot of time, effort, and money required to recover stolen and misused information.

Privacy Data.

→ Read your statements.

- Banks and creditors usually provide statements that detail all account activity, making it easy to identify fraudulent transactions, but only if you read them.

→ Protect your mail.

- Request a “hold mail” service when you're away and resume when you're back.
- Use post office collection boxes or your local post office to drop off bills and other mail that contains your personal information.

→ Protect your technology and digital footprint.

- Make sure to use a firewall and virus protection.
- Review your social media content and remove personal information if it is visible to the public.
- Remember to use a secure browser.

→ Change your paswwords.

- The longer and more complex your passwords are, the harder they are to crack.
- Change your password to an easy-to-remember passphrase: "My smelly cat TuTu’s breath smells like cat food every day of the year!" becomes "Msc22bslcfedoty!"
- Passwords with 8 or fewer characters can be easily decrypted by identity thieves using modern technology.

→ Review your credit reports.

- Request your free credit report every four months from a different agency at: annualcreditreport.com.
- Review the information reported about your payment activity to ensure accuracy.
- If something is inaccurate, contact the agency or creditor to have it corrected or explained.

→ Consider credit freezing/monitoring.

- Credit reporting agencies offer credit freezing and monitoring services, which prevents unauthorized access to new credit. Not all monitoring services are free.

Resources.

→ Annual Credit Report Request Service

- Central Source
- P.O. Box 105283, Atlanta, GA 30348
- 877-322-8228
- annualcreditreport.com

→ U.S. Postal Service

- For mail fraud issues, call the U.S. Post Office to obtain the phone number of the nearest Postal Inspector: 877-876-2455
- postalinspectors.uspis.gov

→ Experian

- P.O. Box 2104, Allen, TX 75013
- To report fraud: 888-397-3742
- experian.com

→ U.S. Social Security Administration

Administration Report fraud: 800-269-0271

- ssa.gov

→ TransUnion

- P.O. Box 1000, Chester, PA 19022
- To report fraud: 800-680-7289
- transunion.com

→ National Do Not Call Registry

- donotcall.gov

→ Equifax

- P.O. Box 740241, Atlanta, GA 30374
- To report fraud: 800-525-6285
- equifax.com

→ OptOutPrescreen.com

- Consumers may request to Opt-In or Opt-Out of firm offers of credit or insurance
- optoutprescreen.com

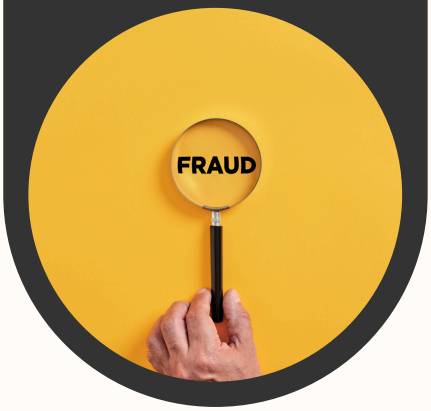
→ U.S. Federal Trade Commission (FTC)

- (Oversees the operation of credit bureaus and provides assistance for identity theft victims)
- FTC Consumer Response Center
- 877-438-4338
- FTC Identity Theft Reporting: identitytheft.gov

If you are a Victim

What you can do?

- Make sure to get a credit report from each of the three main credit bureaus.
- Carefully review the reports for any inaccurate information.
- Remember to place fraud alerts on your credit file, even if you don't see any signs of illegal activity.



- Depending on your situation, you may want to set a 7-year or 1-year alert on your file.
- 7-year alert: If you are a victim of identity theft.
- 1-year alert: If you are worried about becoming a victim of identity theft or fraud. TT
- There are also programs available for military personnel.
- These alerts notify credit issuers that your personal information may have been unlawfully accessed. Before providing a new loan or line of credit, they must verify your identity and obtain your approval.
- Gather evidence of your transactions for each creditor in question.

RISLA

@ristudentloans

Contact Information

RISLA

Student Loans & Refinancing

risla.com

College Planning Center

Free Resource to prepare, plan, and pay for college

collegeplanningcenter.org

Scholarship Hub

Scholarship opportunities to help parents and students

rislascholarshiphub.org