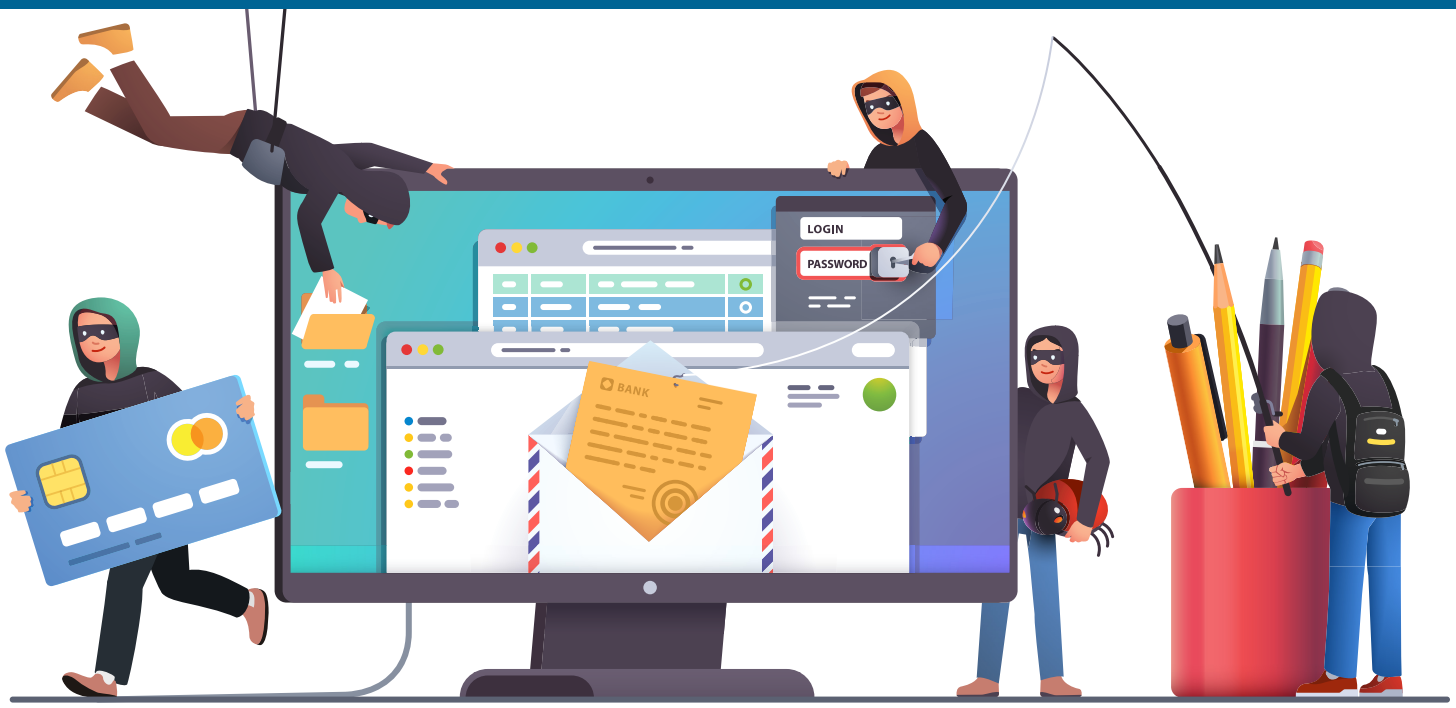
Identity Theft:

A fraudulent and illegal use of someone's personal information.



What is Identity Theft?

Identity theft is defined as a fraud committed or attempted using the identifying information (such as full name, social security number, driver's license number, passport number, and/or email address) of another person without authority.

Is Identity Theft Common Today?

Yes! Reports of identity theft continue to be reported several thousand times per year to the Federal Trade Commission. Reports are submitted from all 50 States with thieves reportedly using different techniques to fraudulently steal personal information and use it illegally.

How Does Identity Theft Happen?

Thieves can use one or more of the following techniques to steal all or just a portion of your personal and/or account information:

- **Skimming**- capturing your credit/debit card information to copy for use on a fake card
- **Phishing**- emailing or sending you pop-up alerts tempting you to enter your personal information for a reward to a false bank or other site
- **Ware Attacks**- Malware, spyware, ransomware, adware, and/or other viruses and/or worms that execute keystrokes or other reporting hidden computer activity
- **Pretext Calls**- Calls to you pretending to be from a legitimate bank or company needing your help after you provide authentication info
- **CVV Code**- Calls to you pretending to be from your bank confirming a false charge and requiring you to provide your Card Verification Value (CVV) code to authenticate who you are
- **Phone Hijacking**- Stealing/using your cell phone to gain access to a wide array of apps, including credit card apps, your email, online payment apps, etc. and changing your passwords to those apps providing thieves with access to that information and potentially removing your access
- Older techniques such as dumpster diving (gaining info from discarded documents), shoulder surfing (looking over your shoulder for info), bribing company employees that have access, analyzing your social media accounts for info (birth dates, pet names, maiden names, family member names, etc.), or simply stealing your wallet/purse and/or mail

COLLEGE Planning Center OF RHODE ISLAND

935 Jefferson Blvd, Suite 3000
Warwick, RI 02886-2225
TEL: 401-468-1700 | FAX: 401-468-1745
www.risla.com

RISLA
RHODE ISLAND STUDENT LOAN AUTHORITY

What is the Impact?

Illegal Ways Your Personal Information Might Be Used

Historically, identity thieves literally took over another person's identity for a number of reasons. However, modern identity thieves are typically stealing pieces of information predominately for economic gain. Here are a few examples of ways that modern identity thieves can use your 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 the unauthorized transactions
- Ordering and using new checks with your bank account and routing number
- Opening new credit accounts (credit cards, auto loans, and even mortgages)
- Set up new cell phone or utility services
- Change passwords for any accessible app that permits thief continued access but prevents you from easily accessing your account information

How Long Does it Take to Recover Stolen Account Info?

- Generally speaking, the longer the stolen information continues to be inappropriately used, the longer it will take to resolve.
- Using a stolen credit card as an example, an identity thief may continue to make numerous cash-equivalent purchases until using that card doesn't work. If the issue is identified after one or two purchases, it will be much easier and faster for the bank that issued the card to identify the illegal purchases and reverse the charges. However, if the thief were to make purchases for several months or years and establish a trend, it will take much longer for the bank to identify and reverse the charges.
- If the identity theft involved stealing sufficient information to obtain new credit, such as a mortgage, the process for reversing more complex transactions can take years to rectify.
- By taking precautionary steps to protect your identity and account information, you can save yourself a lot of time, effort, energy, frustration, and money to recover what was stolen and illegally used.

What Can I Do to Minimize Identity Theft Risk

Read Your Statements

Banks and creditors typically provide statements that indicate all account activity, providing you an easy way of identifying fraudulent activity. But only if you read them!

Protect Your Mail

- Request a "vacation hold" when you go out of town - pick it up when you return
- Use post office collection boxes or your local post office to drop off bills and other mail that contains your personal information

Protect Your Computer/ Review Your Social Media

- Use a firewall and/or virus protection
- Review the content of your social media and remove personal info if the public can view it
- Use a secure browser

Change Your Passwords

- The longer and more complex your passwords are, the harder they are to calculate
- Change your password to an easy to remember passphrase (My cat TuTu's breath smells like cat food every day! = Mc22bslcfed!)
- Passwords with 8 or fewer characters take identity thieves just minutes to decipher using modern technology

Review Your Credit Reports

- Request your free credit bureau report every four months from a different agency at: **www.annualcreditreport.com**
- Review the information that was reported about your payment activity to ensure accuracy
- If something is not accurate, contact the agency and/or creditor and have it corrected or explained

Consider Credit Monitoring

- Credit reporting agencies can provide (for a fee) credit monitoring services which disallow any access to new credit without your permission

Resources

Annual Credit Report Request Service
Central Source
P.O. Box 105283, Atlanta, GA 30348
877-322-8228
www.annualcreditreport.com

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

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

Equifax
P.O. Box 740241, Atlanta, GA 30374
To report fraud: 800-525-6285
www.equifax.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: **www.identitytheft.gov**

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

U.S. Social Security Administration
Report fraud: 800-269-0271
www.ssa.gov

National Do Not Call Registry
www.donotcall.gov/

If You are a Victim:
- Obtain a credit report from each of the three major credit bureaus
- Review the reports carefully for any inaccurate information
- Place fraud alerts on your credit file (even if no illegal activity is evident)
- Depending upon your situation, you may want to place 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 concerned about becoming a victim of identity theft or fraud (also programs for military)
- These alerts warn credit issuers that your personal data may have been illegally accessed and before issuing a new loan or line of credit, they must first verify your identity and gain your approval
- Gather evidence of your transactions for each creditor in question