# Identity Theft

**Identity Theft: the fraudulent acquisition and illegal use of someone's personal, private, identifying information (such as Social Security Number), to commit fraud or other crimes usually for financial gain.**

## How Identity Theft Happens

**Thieves May:**

- Steal – a wallet or purse from your car or office
- Divert mail to another location by filling out a change of address form
- Sift though your trash to find documents (dumpster diving)
- Access credit reports by posing as an employer or landlord
- Hack into personal computers
- Pose as legitimate companies or government agencies to request personal information via email (phishing)
- Use an electronic device to capture information from credit/ATM/debit cards (skimming)
- Bribe an employee who has access to your records


## Illegal Ways Your Information May Be Used

**Common Practices Include:**

- Charging on existing credit accounts and/or changing the billing address to delay you from seeing the bill
- Opening new credit accounts
- Writing checks (with a forged signature) using an existing or a newly opened checking account
- Using a debit card to withdraw money from your bank account
- Establishing phone, wireless or utility service
- Securing loans to buy cars and other expensive items
- Using information & SSN to get a driver's license, medical services, rent an apartment, or secure other fraudulent benefits
- Draining your bank account using electronic transfers

## How Long Can the Effect Last?

- The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem
- Make the initial contacts by phone as soon as possible, even though you will need to follow up in writing
- Victims of identity theft should monitor financial records for several months after they discover the crime and should review their credit reports once every three months, particularly in the first year after the theft

## Legal and Government Agencies

- File a report with your local police office and keep a copy of the report
- Report the crime to the Federal Trade Commission at: **www.ftccomplaintassistant.gov**
- For "mail" fraud – notify your local postal inspector at **http://postalinspectoors.uspis.gov**
- For SSN fraud – notify the Social Security Administration at: **www.ssa.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 90-day or seven year alert on your file:
- 90-day alert: if you suspect your identity information has been compromised
- Seven-year alert: if you have been a victim of identity theft
- These alerts warn credit issuers that your personal data has been illegally accessed, and before issuing a new loan or line of credit, they must first verify your identity and gain your approval
- You may call any of the three credit bureaus (you only need to contact one, that bureau will notify the others)

COLLEGE Planning Center OF RHODE ISLAND

560 Jefferson Blvd, Suite 200
Warwick, RI 02886-1371
TEL: 401-468-1700 | FAX: 401-468-1745
www.risla.com

RISLA
RHODE ISLAND STUDENT LOAN AUTHORITY

# Tips & Strategies

## Ways to Prevent Identity Theft

### Review Your Credit Report Regularly

- Request a free copy of your credit report annually through the Annual Credit Report service **www.annualcreditreport.com**
- Dispute inaccurate information with the bureaus immediately
- Check your report for fraudulent activity
- Select one agency for review every four months, from each of the three major credit bureaus: TransUnion, Experian, and Equifax
- Dispute inaccurate information with the bureaus immediately
- You are also entitled to free reports from the bureaus if you detect inaccuracies due to fraud

### Protect Your Mail

- Request a "vacation hold" when you go out of town – pick it up when you return
- Use a secure mailbox
- Empty your home mailbox as soon after daily delivery as possible
- Use post office collection boxes or your local post office to drop off bills and other mail that contains your personal and financial information

### Protect Your Computer

- Use a firewall program to prevent accessibility to hackers
- Use a complex combination password - don't use an automatic login
- Don't download files or open hyper-links and emails from people you don't know
- Use a secure browser

### Creditors and Financial Institutions

- Contact your creditors immediately if accounts have been used or opened illegally
- Request fraudulent transaction documentation
- Use certified mail, return receipt requested
- If a collection agency attempts to collect on a fraudulent account, explain (in writing) that you are a victim of identity theft and not responsible for the debt
- Ask that they confirm in writing that you do not owe the balance and that the account has been closed
- For checking account fraud:
  - Close current checking and saving accounts
  - Place stop payments on any outstanding checks that you did not write

### Protect Your Credit / Debit Cards

- Carry only the cards you really need and record all card info and store in a secure location
- Establish e-billing to prevent mail theft – know your billing cycles
- Review your checking account and credit card statements carefully
- Shred statements and pre-approved credit card offers (use a cross cut shredder)

### Credit Monitoring & Credit Protection

- Consider extra protection carefully
- Evaluate the benefit vs. cost

## Identity Theft Recovery

- To minimize damage use an informed and systematic approach
- Immediate actions: place a fraud alert on your credit report, request a copy of your credit report and review it for suspicious activity, file a report with your local police
- Have a plan and don't assume the first person you speak with will give you all the information or help you need
- Stay organized – set up a file system
- Record the name, title, time, date and a summary of all communication – written, phone & e-mail
- Keep copies of all communication, file paperwork promptly, and store everything in a safe and accessible place
- Communicate with: all creditors and financial institutions, government agencies, credit bureaus
- Ask to speak with a supervisor if you need more help, make sure you understand everything said to you
- For a step by step guide: **http://www.consumer.ftc.gov/topics/repairing-identity-theft**

# Consumer Rights

## The Fair Credit Report Act (FCRA) ensures that the data contained in your credit report is accurate and private.

- Only those with a legitimate business need recognized by the FCRA may access your credit report – usually a creditor, insurer, landlord, or other business
- You must grant current and prospective employers written permission to access your credit report
- It is the agency's responsibility to report only accurate information, so if you discover a false item, file a dispute
- The credit reporting agency has 30 days to investigate your claim, during which time a notice of dispute will appear on your report
- Both the reporting agency and the company that sent the information are responsible for making corrections

## The Fair and Accurate Transaction Act amends the FCRA and ensures that:

- You may receive a free copy of your credit report, from each agency, once a year
- You may receive additional free reports if identity theft is suspected
- Identity theft victims who file police reports may block fraudulent information from appearing on their credit reports and have access to business records that list the fraudulent transactions
- After a credit report has been flagged for suspected identity theft, credit reporting agencies must ensure that all credit requests are legitimate
- Active military personnel may place special alerts on their files while they are deployed overseas
- Only the last five credit card number digits may be listed on store receipts

## The Fair Credit Billing Act establishes procedures for resolving billing errors.

- It provides a legal dispute process that can help with fraud committed on open-end credit accounts
- The FCBA settlement procedures apply only to disputes about billing errors
- It stipulates that you won't be charged for goods and services you didn't accept or weren't delivered

## The Fair Debt Collection Practices Act prohibits collectors from using unfair or deceptive practices to collect overdue bills (If you have been a victim of identity theft, and a debt that you did not accrue has gone to a collection agency, you have rights).

- You may write to the collector within 30 days of receiving notice of the fraudulent debt. The collection agency will conduct an investigation, during which time the collector must cease communication
- If the debt is determined to be fraudulent, collection activity will remain suspended
- If the debt is determined to be accurate, collection activity will resume

## The Electronic Fund Transfer Act protects your ATM, debit card, or other electronic debit transactions. It also limits your liability for unauthorized electronic fund transfers.

- Report lost or stolen ATM and debit cards immediately, since the amount you can be held responsible for is time sensitive (you have 60 days from your statement to report in writing a fraud upon your account)
- If you report loss or theft within two business days, your liability is limited to $50
- If you report loss or theft after two business days, but within 60 days after a statement showing an unauthorized electronic fund transfer, you can be liable for up to $500
- If you wait more than 60 days, you could lose all of the stolen money
- You may have additional protection if your ATM/debit card has the VISA or Master Card logo on it. In most instances your liability for unauthorized use is $50 per card

# Resources

## Annual Credit Report Request Service

P.O. Box 105281, Atlanta, GA 30348-5281
877-322-8228
www.annualcreditreport.com

## Experian

P.O Box 9554, Allen, TX 75013-2104
To report fraud: 888-397-3742
www.experian.com

## TransUnion

P.O. Box 2000, Chester, PA 19022-2000
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
1-877-438-4338
www.ftc.gov/idtheft
FTC Identity Theft Reporting: www.ftccomplaintassistant.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/register/reg.aspx