



STUDENT ADVOCATES FOR FINANCIAL EDUCATION

IDENTITY THEFT

Identity theft is when someone wrongfully acquires and uses a consumer's personal identification, credit, or account information. A thief can use this information to open bank accounts, apply for loans and credit cards, establish services, rent apartments, and in some cases the thief will even use the consumer's name if arrested.

INFORMATION THIEVES WANT

- Name
- Date of birth
- Address
- Telephone numbers
- Driver's license number
- Credit card account
- Bank account information
- Passwords
- Checks
- Calling cards
- Bills
- ATM cards
- Personal records
- Social security number

HOW INFORMATION IS ACQUIRED

- **Dumpster diving** - the thief goes through the victim's trash to steal personal information.
- **Shoulder surfing** - the thief watches what PIN number is entered into the ATM machine.
- **Hacking** - a hacker may be able to extract information such as income taxes or account numbers kept on a computer system.
- **Insider access** - a disgruntled employee may sell personal information to a thief.
- **Stealing** - mail, wallets, purses, etc. are the most common items stolen.
- **Changing your address** - divert your mail to steal your identity.
- **Skimming** - steal your credit or debit numbers with a copying device when processing your card.

The U.S. Federal Trade Commission estimates identity theft affects as many as 9 million Americans each year.



The most common way an identity thief steals information is by stealing a victim's purse or wallet. One's driver's license number needs to be different from his/her social security number. Social security numbers should not be pre-printed on checks, nor should a social security card be carried in a purse or wallet.



STUDENT ADVOCATES FOR FINANCIAL EDUCATION

PROTECT YOUR IDENTITY

Identity Theft Prevention

Shred/Burn All Important Documents: Purchase a paper shredder to properly dispose of papers or documents containing important personal information such as credit card solicitations and receipts.

Monitor Statements: Monitor monthly bank and credit card statements on a regular basis to ensure all of the charges and/or account activity is legitimate.

Mail Documents Wisely: Deposit outgoing mail in USPS collection boxes or at the post office rather than unsecured mailboxes. In addition, promptly remove incoming mail from the mailbox.

Review Credit Reports: Review personal credit reports from each of the three credit bureaus at least once a year to check for any inaccuracies. One free credit report can be requested annually by visiting www.AnnualCreditReport.com.

Equifax: www.equifax.com

P.O. Box 740241
Atlanta, GA 30374-0241

Order a report:
1.800.685.1111
Fraud Alert:
1.888.766.0008

TransUnion: www.transunion.com

P.O. Box 6790
Fullerton, CA 92834-6790

Order a report:
1.877.322.8228
Report fraud:
1.800.860.7289

Experian: www.experian.com

P.O. Box 9532
Allen, TX 75013

Order a report:
1.888.397.3742
Report fraud:
1.888.397.3742

Keep a record of all conversations & correspondence

IF YOU HAVE BEEN A VICTIM OF IDENTITY THEFT...

- **Contact the fraud departments** of each of the three major credit bureaus to put your file on "fraud alert."
- **Contact the security departments** of creditors and financial institutions for any accounts fraudulently opened and close the accounts.
- **File a report** in the local police station where the theft took place and get copies of the report in the event proof is needed at a later date.
- **File a complaint** with the Federal Trade Commission by contacting the Identity Theft Hotline or contacting the FTC via mail if the fraud happens in more than one state. If the fraud is in-state, contact your state's Attorney General's office.

FTC BY PHONE

Toll free: 1-877-ID-THEFT
(1-877-438-4338)
TTY: (1-866-653-4261)

FTC BY MAIL

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580