

# IDENTITY THEFT

STOP THIEVES FROM STEALING YOUR IDENTITY

## If You are a Victim:

- Report the crime to the police and get a report.
- Contact the Queens District Attorney Economic Crimes Bureau (718) 286-6673.
- File a complaint with the Federal Trade Commission (FTC) at 877-ID-THEFT. The FTC investigates interstate and internet fraud. Download and complete ID theft affidavit. Their website is [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)
- For fraud involving stolen mail, file a complaint with postal officials at: [www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm](http://www.usps.com/postalinspectors/fraud/MailFraudComplaint.htm)
- Alert credit reporting agencies and request to have your accounts flagged with a fraud alert. Flagging your accounts will not let merchants grant new credit without your explicit approval.
- Close all accounts that have been used by thieves.
- Select new passwords and PINs for accounts.
- Order a new credit report every year.
- Maintain record of expenses.
- Contact financial institutions.

## Credit Bureaus

### Contact:

**Queens District Attorney Economic Crimes Bureau (718) 286-6673**

### Equifax

[www.equifax.com](http://www.equifax.com)

To order your report:

Call 800-685-1111 or

Write to P.O. Box 740241,  
Atlanta, GA 30374-6285

To report fraud, call 800-525-6285

### Experian

[www.experian.com](http://www.experian.com)

To order your report:

Call 800-397-3742 or

Write to P.O. Box 2104,  
Allen, TX 75013

To report fraud, call 888-397-3742

### Trans Union

[www.tuc.com](http://www.tuc.com)

To order your report:

Call 800-916-8800 or

Write to P.O. Box 1000,  
Chester, PA 01902

To report fraud, call 800-680-7289

**Office of the Queens District Attorney  
Crime Victims Advocate Program  
125-01 Queens Boulevard  
Kew Gardens, NY 11415  
718-286-6847**



**Funded by CVB**

Designed by: Pedro A. Quezada, Jr.

08/06



**Richard A. Brown  
Queens District Attorney**

# IDENTITY THEFT

Stop Thieves From Stealing  
Your Identity



## What is Identity Theft?

Identity theft is the fraudulent use of your name and identifying data by someone else to obtain credit, merchandise, services, money, or medical information.

## Personal Identifying Information

Is any information that identifies a specific individual. These personal identifiers include the following:

- Date of birth
- Employer or taxpayer identification
- Alien registration
- Government passport
- Health insurance identification
- Credit card number
- Debit card number
- Driver's license
- Social security number
- Savings account number
- Mother's maiden name

## Seven Ways To Lose Your Identity

A thief only needs three pieces of information: your name, social security number & date of birth to open accounts.

1. **Stealing company data** occurs when hackers or insiders break into company databases or websites where personal identifying information is stored.
2. **False pretense** is when e-mail spammers, telemarketers, and sales people lure you into revealing personal information.
3. **Dumpster diving** is when criminals dig through trash for medical statements, bills, or other personal papers to obtain credit or bank account information.
4. **Mail theft** occurs when individuals remove mail containing personal information, pre-approved credit offers, and checks from unlocked mailboxes.
5. **Account takeover** is when thieves use stolen or fake ID's to take over or drain existing bank or credit accounts. Thieves escape detection by forwarding mail to a private mailbox or new address.
6. **Skimming** is a technique used by thieves when a magnetic card reader is used to read the magnetic strip on credit or debit cards. The information obtained by swiping a credit or debit card can be transferred to a counterfeit credit card. Some private automatic teller machines have also been rigged to skim account numbers and PINs. The culprits include waiters, gas station attendants, and store clerks.
7. **Old computers** can be raided to access sensitive files from the hard drives.

## Minimize Your Risk

Shred Papers that contain personal information and pre-approved credit card offers.



1. Do not use e-mail to send your social security number or other personal data.
2. Do not give personal information based on unsolicited e-mails and phone calls.
3. When discarding an old computer, use hard drive shredding software or remove and destroy hard drives.
4. Watch your credit by requesting a credit report once a year from three major credit reporting agencies: Equifax, Experian, and Trans Union. Report all errors promptly in writing.
5. Install firewalls and virus detection software on your home computer.
6. Deal with reputable websites.
7. Password protect all your banks/brokerage accounts by creating a password at least eight characters long.
8. Get your checks delivered to your bank, not your home address.