

# Important phone numbers

**NYS Department of State  
Division of Consumer Protection**  
[www.dos.ny.gov/consumerprotection/](http://www.dos.ny.gov/consumerprotection/)  
800-697-1220  
(Consumer Guide on  
Identity Theft available)

**Federal Trade Commission  
Identity Theft Hotline**  
[www.ftc.gov](http://www.ftc.gov)  
877-IDTHEFT (438-4338)

**Federal Communications  
Commission Consumer Center**  
[www.fcc.gov](http://www.fcc.gov)  
888-CALLFCC (225-5322)

**NYS Attorney General**  
[www.ag.ny.gov](http://www.ag.ny.gov)  
Consumer Helpline  
800-771-7755

**Consumer Credit  
Reporting Companies**  
Equifax  
800-525-6285  
Experian  
888-397-3742  
TransUnion  
800-680-7289

Updated 4/13

# IDENTITY THEFT



*Information on how to protect  
your privacy and what to do if  
your identity is stolen*

*Courtesy of...*

**Assemblymember  
John T. McDonald III**



**Albany Office:**  
Room 417, LOB  
Albany, NY 12248  
518-455-4474

**Email:**  
[mcdonaldj@assembly.state.ny.us](mailto:mcdonaldj@assembly.state.ny.us)



**Assemblymember  
John T. McDonald III**

Dear Friend,

According to the Federal Trade Commission, an estimated 11.7 million Americans have their identities stolen each year. For the past several years, identity theft has been the top concern for consumers, the agency reports.

From pickpockets to highly technical computer hackers, to those who use skimmers, which is now a crime, these criminals have learned sophisticated ways to use your personal information for their personal gain. Since credit and debit card receipts and numbers, checks and computer transactions can all be used by criminals to trace and steal identities, many victims are unaware they are even at risk.

The national nonprofit Identity Theft Resource Center states that identity theft continues to be one of the fastest growing crimes in the United States, and that this crime can not only mean financial identity theft, but criminal identity theft, governmental identity theft and medical identity theft. This brochure provides guidelines about how to better protect yourself.

Feel free to contact my office if you would like more information on this or any other matter.

Sincerely,

John T. McDonald III  
Member of Assembly

## WHAT IS IDENTITY THEFT?

Identity theft starts when someone steals a credit or debit card or obtains a Social Security number, driver license number, ATM personal identification number (PIN), telephone calling card or other piece of your personal information to illegally purchase goods or services or open up new accounts in a victim's name.

Identity theft is a serious crime that can cause substantial harm to consumers. Victims are often left with damaged credit reports and are forced to spend time, effort and money to repair this damage. As a result, victims often have trouble getting credit, loans and even cashing checks due to the damage done to their credit.

**NYS Office of Victim Services (OVS)**  
www.ovs.ny.gov, 800-247-8035.

OVS may cover out-of-pocket expenses for financial counseling for eligible seniors or persons with disabilities who are victimized.



### Regulating document destruction contractors

*New York State law requires specialized contractors that shred, burn or pulverize records containing sensitive personal information, to register with the Department of State.*

## How can I prevent identity theft?

- ▶ Minimize the amount of information a thief can steal. Avoid carrying extra credit cards, your Social Security card, birth certificate or passport in your wallet or purse.
- ▶ Never keep your personal identification number (PIN) on or near your ATM or credit card. Memorize these numbers.
- ▶ Have your name removed from marketing lists of the three major consumer credit reporting companies: Equifax, Experian and TransUnion.
- ▶ Never give your credit card number or other information over the phone unless you initiated the call and trust the business.
- ▶ Beware of phishing, the practice of sending bulk email or pop-up messages that deceive consumers in disclosing personal information like passwords and Social Security numbers. Legitimate companies don't solicit information this way. Also be leery of unsolicited text messages offering too good to be true offers.
- ▶ Laptops are easily stolen. Try not to store sensitive information on them.
- ▶ Delete any personal information stored on your computer before disposing of it by using a "wipe" utility program, which overwrites the hard drive.
- ▶ Update your computer virus software and use a secure browser to guard the safety of your online

transactions. Don't download files from strangers or click on hyperlinks from strangers.

- ▶ Install a locked mailbox at your residence to help reduce mail theft.
- ▶ Keep a copy of your credit cards, their account numbers, expiration dates and the telephone numbers of customer service or fraud departments in case your cards are stolen. Make sure this information is kept in a secure location.
- ▶ Use passwords on your credit card, bank or phone accounts. Don't use easily available information like your birth date or the last four digits of your Social Security number for passwords.
- ▶ Find out who has access to your personal information at work and verify that your records are kept in a secure location. Ask how personal records are disposed.
- ▶ Tear up, cut up or, ideally, shred your credit card receipts, copies of credit and bank statements and expired applications or offers, checks and credit cards before throwing them out.

## What do I do if my identity has been stolen?

- ▶ Immediately contact the fraud department at each of the three major credit bureaus – Equifax, Experian and TransUnion. The fraud alert requires creditors to contact you before opening any new accounts or making any changes to your existing accounts.
- ▶ Order copies of your credit reports.
- ▶ Consider "freezing" your credit reports.
- ▶ Contact creditors for any accounts that have been tampered with or opened fraudulently. Speak to their security or fraud department and send a follow-up letter. Close the fraudulent account.
- ▶ File a report with your local police department. Be sure to obtain a copy of the police report to help you when dealing with creditors.
- ▶ Take steps to ensure your mail, personal information and other data are protected.

## Consumer protections "Freeze" your credit reports

Consumers in New York State can prohibit access – also known as "freezing" – to personal information in their credit reports. A security freeze can prevent identity thieves from taking out new loans and credit in a consumer's name. You must contact each of the three consumer credit reporting companies and make a request in writing with delivery confirmation or via telephone or secure electronic means.

An initial freeze request is free. Subsequent requests cost \$5, unless you provide proof that you are a victim of identity theft or domestic violence with an FTC Identity Theft Victim Affidavit or a police report, to which you are entitled. Remember, freezes will limit a consumer's ability to get "instant credit," and they may slow credit applications. You can take a freeze off your account at any time on the Internet.

### Free annual credit reports available

You are entitled to a free copy of your credit report once every 12 months. To order your free annual report from each of the nationwide consumer credit reporting companies, visit the official website: [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com); or call toll-free at 877-322-8228. ***This website is the only source authorized by the federal government for free annual credit reports.***

### Consumer notification of security breaches

New York State law requires public and private organizations to notify customers when the security of their private information has been breached. This enables consumers to take steps to prevent their identity from being stolen or to stop the theft as soon as possible.