



# Deterring Identity Theft

## THE EVOLVING THREATS OF IDENTITY THEFT

**The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year.**

**Identity theft complaints increased 22 percent from 2007 to 2008 (Javelin 2009 Identity Fraud Survey Report)**

**The average consumer costs of identity fraud were \$496 per incident in 2008 (Javelin 2009 Identity Fraud Survey Report)**

**Industry estimates put the total cost of identity fraud at \$48 billion in 2008 (2009 Javelin Strategy & Research)**

You or a family member could become a victim of identity theft. This pamphlet can help protect you and members of your family against the damaging effect identity crimes can have on the victim. This pamphlet includes:

- *What* identity theft is and how it impacts all Americans
- *Ways to lessen* the likelihood you or a family member will be a victim of identity theft
- *Tools* to utilize if you or a family member becomes a victim of identity theft

Identity theft occurs when an individual's Social Security Number (SSN), credit card account number, driver's license number, bank account number or other personal identifier is captured and used to open new accounts, take over existing accounts, apply for loans, initiate services, access government benefits or commit other crimes.

Identity theft has grown along with advancements in computers, scanners, digital copiers and desktop publishing. The most common type of identity theft is credit card fraud. Other motives for identity theft include obtaining employment, access to healthcare benefits, evading law enforcement, concealing a criminal history, obtaining a driver's license and circumventing citizenship requirements.

### ► Protecting your information and good name

Many victims do not learn their identity has been stolen until they have a loan or credit application denied, or bill collectors confront them. Protect yourself by reviewing your credit reports. Credit reports are a valuable tool for identifying identity theft. By reviewing your credit report you can also identify errors that can adversely impact your credit standing. You are entitled to receive a free copy of your credit report once every 12 months from each of the three credit reporting agencies (CRAs) — Experian, TransUnion and Equifax.

deter

➤ **Free annual credit reports can be ordered in any of three ways:**

<b>BY CALLING</b>	<b>BY WRITING:</b>	<b>ON-LINE:</b>
1-877-322-8228	Annual Credit Report Services P.O. Box 105281 Atlanta, GA 30348-5281	annualcreditreport.com

- Scrutinize your credit report to verify all personal and credit information is correct
- Look for accounts you didn't open, unexplained charges on valid accounts, unfamiliar addresses and number of inquiries
- Take note of who is asking about you
- Act in writing to ensure inaccurate data is removed or corrected and send a copy to each creditor and CRA involved
- Direct the CRA to remove all inquiries generated due to the item
- Notify anyone who received a copy of the report in the past six months that the item is being disputed

**ALERT: Credit reports can be ordered online at [www.annualcreditreport.com](http://www.annualcreditreport.com). Be aware of sites that charge for this free service.**

## ► Tips for detecting, preventing and mitigating identity theft

<p><b>Guard against phishing and other online schemes by not opening or responding to suspicious e-mails</b></p>	<p>Even if an unsolicited e-mail looks authentic, it may not be. Regardless of the story or alleged urgency, exercise extreme caution when asked to reveal personal data. If data must be provided for a valid reason, confirm the site displays a closed padlock icon and that you see a secure session verified by https.</p>
<p><b>Invest in firewall/anti-virus software to protect valuable data on your computer</b></p>	<p>Ensure security patches are up to date. Use complex passwords and encryption, and do not store sensitive data on the hard drive. Always log out when you access your account online.</p>
<p><b>Remove your personal data before donating or selling a used computer either by using an erasing application or destroying the hard drive</b></p>	<p>Hitting the delete key does not make the data disappear. It remains on the hard drive and is recoverable. Erasing software must be used to sanitize the hard drive, or the hard drive must be physically removed and destroyed.</p>
<p><b>Use caution when accessing sites or downloading software</b></p>	<p>Malware, trojans and botnets are all techniques fraudsters use to infect your PC or website with the goal of collecting and misusing sensitive information. Home computers are vulnerable to malware attacks unless protection is deployed.</p>
<p><b>Protect your ATM account</b></p>	<p>Only use trusted networks, and be alert for devices used for intercepting your account information (skimmers), hidden cameras and shoulder surfers.</p> <ul style="list-style-type: none"> <li>• Don't share your PIN</li> <li>• Don't use your PIN for multiple accounts</li> <li>• Don't use easily identifiable sequences for your PIN (e.g. birthdates, last four digits of the card)</li> <li>• Don't keep your PIN with the card</li> <li>• Immediately contact the issuer if an ATM fails to return your card.</li> </ul>
<p><b>Avoid disclosing personal information to strangers who could contact you on the phone, in writing, via e-mail or in person</b></p>	<p>Even if the recipient is known to you and reputable, don't reveal financial and other sensitive information without knowing how it will be used.</p>

► **Tips for detecting, preventing and mitigating identity theft (CONT.)**

<p><b>Avoid putting payments, completed applications or any documents with personal information in your mailbox</b></p>	<p>One out of every 80 American households has mail stolen every year. Take outbound mail to the post office, give it to the mail carrier or deposit it in a postal collection box. Promptly retrieve delivered mail. Temporarily stop mail deliveries when you are away. Watch your billing cycles to monitor if statements are overdue.</p>
<p><b>Be careful when you leave your checkbook, wallet, purse or laptop in an unattended vehicle</b></p>	<p>Be extra careful at golf courses, health clubs, jogging paths and places where thieves know valuables may be left unattended in vehicles. These items should be placed in your trunk or out of sight.</p>
<p><b>Remove unnecessary credit cards and other items from your wallet or purse</b></p>	<p>Many Americans carry their SSNs in one form or another on their person. Remove Social Security cards, PINs, passwords, receipts, credit cards and items that don't need to be carried all of the time. Photocopy the front and back of credit cards and other numbered identifiers. Keep the photocopies in a safe place that can be easily accessed if the wallet or purse is lost or stolen.</p>
<p><b>Request free credit reports for minor children</b></p>	<p>The credit report will show if any fraudulent activity has occurred under the minor child's name. Report any fraudulent activity to the credit reporting agencies.</p>
<p><b>Shred documents containing personal information</b></p>	<p>An average household receives one unsolicited credit card offer, balance transfer or convenience check each week. Many of these are thrown away intact. Identity crimes can begin with items scavenged from the trash. Shred tax worksheets, credit card offers, statements and checks. A cross shredder is the most effective means of home shredding.</p>
<p><b>Protect your driver's license</b></p>	<p>Do not print your driver's license or SSN number on your checks. If your state uses your SSN for your driver's license number, request that an alternate number be assigned.</p>



► **Tips for detecting, preventing and mitigating identity theft (CONT.)**

<b>Review financial records promptly</b>	Search for unknown charges, unauthorized accounts or other flags that could indicate identity theft.
<b>Take steps after the death of a family member</b>	Notify credit card companies, financial institutions and other creditors in writing of the death of a family member and request the accounts be closed.

## Important contact information

### Credit Reporting Bureaus:

#### Equifax:

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

#### To report fraud:

1-800-525-6285

#### Experian:

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

#### To report fraud:

1-888-397-3742

#### TransUnion:

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

#### To report fraud:

1-800-680-7289

### Federal Trade Commission:

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

#### Fraud hotline:

1-877-438-4338

### Social Security Administration:

[www.ssa.gov/oig](http://www.ssa.gov/oig)

#### Fraud hotline:

1-800-269-0271

NOTE: Phone numbers for the nearest FBI and U.S. Postal Inspection Service field offices, as well as other federal, state and municipal government agencies, can be found in the blue section at the front of your local telephone directory.

## Identity Theft Contact Checklist

To mitigate damage to your credit and good name, the following entities should be notified as soon as an identity theft crime is known or suspected to have occurred:

Action	Date Completed
<b>1. Local Law Enforcement Agency</b> <ul style="list-style-type: none"> <li>• Request that a case be opened</li> <li>• Obtain a copy of the police report</li> </ul>	_____
<b>2. Credit Card Issuer(s)</b> <ul style="list-style-type: none"> <li>a. _____</li> <li>b. _____</li> <li>c. _____</li> <li>d. _____</li> <li>• Close accounts where fraud has occurred or may occur</li> <li>• Open new accounts with new passwords or PINs</li> </ul>	_____
<b>3. Financial Institution(s)</b> <ul style="list-style-type: none"> <li>a. _____</li> <li>b. _____</li> <li>• Close ATM/Debit accounts where fraud has occurred or may occur</li> <li>• Close checking, savings, and other accounts where fraud has or might occur</li> <li>• Alert recipients to the situation and arrange alternate payment for any valid checks that have been written</li> <li>• Open new accounts with new passwords or PINs</li> </ul>	_____
<b>4. Credit Reporting Bureau Fraud Units</b> <ul style="list-style-type: none"> <li>• Notify one of the three bureaus to request and review a copy of your credit report</li> <li>• Initiate a fraud alert or victim's statement as appropriate</li> </ul>	_____
<b>5. Federal Trade Commission Fraud Hotline</b> <ul style="list-style-type: none"> <li>• File a report</li> <li>• Request a copy of the FTC fraud affidavit</li> </ul>	_____
<b>6. Others (if applicable)</b> <ul style="list-style-type: none"> <li>• US Postal Inspection Service</li> <li>• Social Security Administration</li> <li>• State driver's license bureau</li> <li>• U.S. Dept of State Passport Office</li> <li>• Internal Revenue Service</li> <li>• Stock brokers and mutual fund or retirement account managers</li> <li>• Medicare/Medicaid</li> </ul>	_____

