State of Connecticut

IDENTITY THEFT

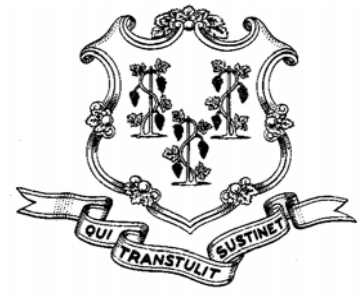
A Guide for Connecticut Citizens

What is Identity Theft?
How is it Committed?
How to Avoid Becoming a Victim
What to Do If You Become a Victim

Office of the Victim Advocate
OVA

505 Hudson Street · Hartford, Connecticut 06106
Phone: (860) 550-6632 · Toll Free 1-888-771-3126
Fax: (860) 566-3542

Visit us on the web at www.ct.gov/ova



Dear Connecticut Citizen:

This guide has been published to help raise awareness of identity theft — America's fastest growing, yet vastly underreported, crime. Within its pages, this booklet describes the nature of identity theft, how it is committed, how to avoid becoming a victim and what to do if you become a victim.

Identity theft is a very frustrating crime which often leaves unsuspecting victims with a good deal of work to clear their name and credit history. Victims can spend months or even years trying to get their life back in order.

The goal in publishing this guide is to educate citizens on how they can help protect themselves from becoming an identity theft victim. Arming citizens with information is one way to help prevent this crime from the start.

I encourage you to share this booklet with family, friends, colleagues and neighbors. Combining greater prevention, crime reporting and law enforcement efforts could eliminate identity theft as a significant threat to both personal and homeland security.

James F. Papillo, J.D., Ph.D.
State Victim Advocate, State of Connecticut

Contents

I. What is identity theft?

As it is throughout the United States, identity (ID) theft is a growing crisis in Connecticut. ID theft is also a very frustrating crime. Because ID theft is flourishing, the crime is becoming more visible, and stories about victims' experiences permeate the press. Identity theft occurs when someone invades your life, taking pieces of your personal identifying information as his or her own, and, in the process, ruins your financial reputation. Victims of identity theft face extreme difficulties attempting to clear their damaged credit—or even a criminal record—caused by the thief.

Identity theft occurs when **someone uses your name, your Social Security number, your credit card number or another piece of your personal information to commit fraud or theft**.

Your personal information can be used to open credit cards and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment or accommodations and even secure employment.

If you become the victim of ID theft, you could be left with bills, charges, bad checks and taxes you did not accrue. Victims of ID theft can spend months or even years—not to mention money—restoring their good name and credit record.

Identity theft has been called America's fastest growing crime. The Federal Bureau of Investigation estimates that hundreds of thousands of Americans become identity theft victims each year. The Federal Trade Commission (FTC) has reported that 27 million Americans have been ID theft victims since 1998, making ID theft a multi-billion dollar problem. The FTC has also reported that in the past year, businesses lost nearly $48 billion to ID theft. Consumers reported $5 billion in out-of-pocket expenses.

Stealing a person's identity is now easier than it has ever been, thanks to computers and public access to personal data. Criminals know that businesses are reluctant to prosecute individual cases and often consider losses a "cost of doing business." The very nature of the crime makes the perpetrator difficult to identify and prosecute. For these reasons, **the victim of ID theft must personally take steps to limit damage to their financial standing, credit history and peace of mind.**

There is no short-cut to eradicating ID theft; the most formidable problem is catching the criminals. You may not know your identity has been stolen until you notice that something is awry. Time may pass before you begin receiving strange bills for goods and services you did not purchase. **Experts have determined that early detection of identity theft significantly reduces total financial loss and damage to your credit record.**

Identity Theft: the Connecticut connection

The most recent statistics published by the Federal Trade Commission (FTC) show that occurrences of identity theft are on the rise in Connecticut. As you can see from the table below, identity theft comes in all shapes and sizes, and the types of identity theft and fraud reported by Connecticut residents runs the full gamut of crimes.

Identity Theft Types
Reported by Connecticut Victims
(Calendar Year 2004)

Rank	Identity Theft Type	No. of Victims	Percentage
1	Credit Card Fraud	680	34%
2	Phone or Utilities Fraud	420	21%
3	Bank Fraud	280	14%
4	Employment-Related Fraud	160	8%
5	Government Documents or Benefits Fraud	140	7%
6	Loan Fraud	100	5%
-	Other	440	22%
-	Attempted Identity Theft	140	7%

Percentages are based on the 2,000 victims reporting from Connecticut. Percentages add to more than 100 because approximately 18% of victims from Connecticut reported experiencing more than one type of identity theft. (FTC, 2005)

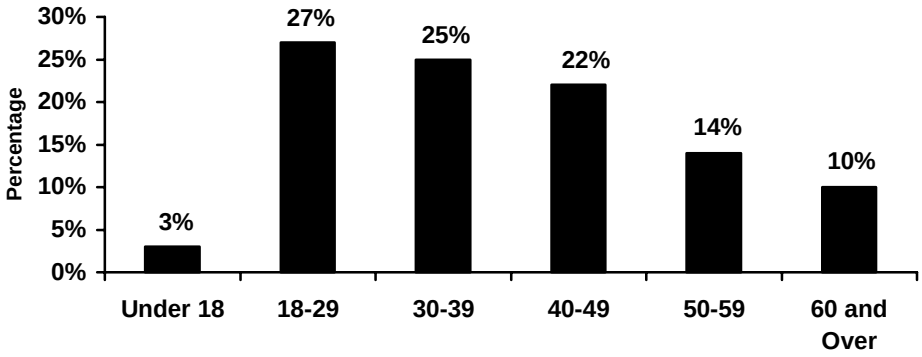
And if you thought that identity theft was only a problem in one or two of our major cities, think again. FTC statistics show that identity theft crime has touched every county of our state. The bar chart below identifies the cities in which identity theft is most often reported.

Top Connecticut Identity Theft Victim Locations
(Calendar Year 2004)

Victim City	No. of Victims
Hartford	170
Bridgeport	112
New Haven	90
Stamford	82
Waterbury	79

The statistics in Connecticut appear similar to those reported nationwide when it comes to the age of victims of identity theft. Evidence suggests that seniors are less victimized by identity theft than the rest of the population, though they can be targeted in specific financial scams that may or may not involve identity theft.

Complaints by Victim Age
(Calendar Year 2004)



Percentages are based on the 2,000 victims who provided their age. This chart represents 97% of victims reporting in Connecticut. (FTC, 2005)

How is identity theft committed?

Skilled identity thieves use a variety of methods to gain access to your personal information. According to the FTC, many thieves:

- Get information from businesses or other institutions by stealing records from their employer, bribing an employee who has access to these records or hacking into the organization's computers.
- Rummage through trash, or the trash of businesses or dumps, in a practice known as "**dumpster diving**."
- Obtain credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord, employer or someone else who may have a legal right to the information.
- Steal credit and debit card numbers as cards are processed, often by employees in retail establishments, by using a special information storage device in a practice known as "**skimming**."
- Steal wallets and purses containing identification, credit and bank cards.
- Steal mail, including bank and credit card statements, pre-approved credit offers, new checks or tax information.
- Complete a "change of address form" at the post office to divert mail to another location.
- Steal personal information from homes.

- Scam information by posing as a legitimate business person or government official.
- Use a technique commonly known as "**phishing**" to assume the identity of a corporation by relocating their logo on what looks like an official e-mail communication. These fraudulent communications often ask people to confirm passwords or personnel identification, which, if provided, are used to empty bank accounts.

Once identity thieves have your personal information, they may:

- Go on spending sprees using credit and debit card account numbers to buy "big-ticket" items, like computers, that they can easily sell.
- Open a new credit card account in your name. When thieves don't pay the bills, the delinquent account is reported on your credit report.
- Change the mailing address on a credit card account. Thieves then run up charges on the account. Because the bills are being sent to a new address, it may take some time before you realize there is a problem.
- Take out auto loans in your name.
- Establish phone or wireless service in your name.
- Create counterfeit checks or debit cards, and drain your bank account.
- Open a bank account in your name and write bad checks on that account.
- File for bankruptcy in your name to avoid paying debts they've incurred or to avoid eviction.
- Give your name to the police during an arrest. If they are released and don't appear for their court date, an arrest warrant could be issued in your name. You could be arrested for a crime or crimes you did not commit!

How can you tell if you are the victim of identity theft?

According to the Federal Trade Commission, important indications of identity theft include:

- Failing to receive bills or other mail signaling an address change by the identity thief.
- Receiving credit cards for which you did not apply.
- Receiving calls from debt collectors or companies about merchandise or services you never bought.
- Denial of credit for no apparent reason.

You may not realize you are a victim of identity theft until you try to obtain additional credit in your name, which usually requires a check of your credit report or until a few months of non-payment on accounts that thieves have opened assuming your identity.

II. How to avoid becoming a victim of identity theft

Experts tell us that to reduce or minimize the risk of becoming a victim of identity theft or fraud, you should do the following.

Be "stingy" with personal information

Become "stingy" about giving out your personal information to others unless you have a reason to trust them.

- Start by guarding your personal data and adopting a "need to know" approach to sharing such information. Your credit card company may need to know your mother's maiden name so that it can verify your identity when you call to inquire about your account. A stranger, however, doesn't need to know this information.
- Don't be a "phish." Identity thieves, assuming the identity of major corporations or on-line retail businesses, send out mass e-mails that appear to come from companies you know and respect. This technique is commonly known as "phishing." These e-mails seek personal identification – like Social Security numbers, PIN numbers, etc. **Never** click on a hot link in such an e-mail and never respond with any personal information. Reputable companies, especially financial services institutions, make it a policy never to seek personal information via the Internet.
- The more information that you have printed on your personal bank checks — such as your Social Security number or home telephone number — the more personal data you are routinely providing to people who probably don't need that information. List only your last name and first initial rather than your full name. You want a retail clerk to check your ID when you are cashing a check.
- Never throw away receipts or statements that contain personal information. The trash is the greatest repository of information for identity thieves. **Invest in an inexpensive shredder** to eliminate any personal information, like bank account numbers, Social Security numbers, etc.
- If someone you don't know calls you and offers the chance to receive a "major" credit card, a prize or other valuable item, but asks you for personal data — such as your Social Security number, credit card number and expiration date or mother's maiden name — ask them to send you a written application form. If they won't do it, tell them you're not interested and hang up. If they do send you an application, review it carefully to make sure it's from a company that's well-known and reputable. The Better Business Bureau can give you information about businesses that have been the subject of complaints.
- Don't leave your mail or newspaper out overnight. If you will be away from home for any period, have your home mail delivery stopped. If possible, secure a locked mail box at your local post office or a retail store mail box service for your home mail delivery. You may also install a mail slot in your front door so that thieves do not have access to your mail. If you go on vacation, continue to have

your yard maintained. Make sure your home looks as if it is occupied while you are gone.

- Write “Check ID” on the back of your debit or credit cards next to your signature. In that way, when a retail store checks your signature on your card, they will verify that the card is being used by the proper individual.
- Be aware of people standing too close to you and “**shoulder surfing**” for your PIN number while you conduct ATM transactions.
- If you have to call someone while you're traveling, and need to pass on personal financial information to the person you're calling, don't do it at an open telephone booth where passersby can listen to what you're saying. Use a telephone booth where you can close the door, or wait until you're at a less public location to make the call.

Check your financial information regularly

Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals.

What should be there:

- If you have bank or credit card accounts, you should be receiving monthly statements that list transactions for the most recent month or reporting period.
- If you're not receiving monthly statements for the accounts you know you have, call the financial institution or credit card company immediately to inquire why you aren’t receiving your statements.
- If you're told that your statements are being mailed to another address that you haven't authorized, tell the financial institution or credit card representative that you did not authorize the change of address and that someone may be improperly using your accounts. In that situation, you should also ask for copies of all statements and debit or credit transactions that have occurred since the last statement you received. Obtaining those copies will help you to work with the financial institution or credit card company to determine whether some or all of those debit or credit card transactions are fraudulent.

What shouldn't be there:

- Checking your monthly statements carefully for unauthorized debits or charges is the best way to safeguard your finances. Too many of us only glance at those statements, enclosed checks or credit card transactions and don't review them closely to make sure there are no unauthorized transactions.
- If someone gains access to your mail or other personal data, opens new accounts in your name or withdraws funds from your bank account, take the steps recommended in the following sections of this publication.

Get and review a copy of your credit report

Thanks to a new federal law, everyone in the United States is now entitled to one free copy of their credit report from each of the three major credit bureaus with a 12-month period. **You may obtain your free copies whether or not you have become the victim of ID theft.** You should carefully review the information contained on your credit reports. Each credit report should list all bank and financial accounts under your name, and will provide other indications of whether someone has wrongfully opened or used any accounts in your name.

Go to www.annualcreditreport.com or call (877) 322-8228 to request your report. **This is the only legitimate website consumers should use to obtain free copies of their credit reports.** Or you can obtain your copies by contacting the three major credit reporting agencies directly (see Section III for contact information).

It is not necessary for you to order all three copies of your credit reports at the same time. In fact, many experts recommend staggering your requests through the year so that a free credit report can, for example, be obtained from a different credit reporting bureau every four months. **TIP: Mark your calendar to request a free copy of your credit report from a different credit reporting bureau every fourth month.** Since each credit report provides essentially the same information, staggering your requests throughout the year in this way will allow you to better monitor the accuracy of the information contained in your credit history.

Maintain careful records

- Although financial institutions are required to maintain copies of your checks, debit transactions and similar transactions for five years, you should retain your monthly statements and checks for at least one year, if not more. If you need to dispute a particular check or transaction, your original records will be more immediately accessible and useful to the institutions you have contacted.
- You should make a list of all your credit cards, your account numbers and the telephone number you should call in case your cards are either lost or stolen. You should do the same thing for your debit and ATM cards. Alternatively, you can make a copy of the front and back of your credit and debit cards if that is easier for you. But remember to put a contact number on the photocopy because time is of the essence when your personal information is lost or stolen. Put this list in a place that is easily accessible, but not visible, in your home.

Even if you take all of these steps, however, it's still possible to become a victim of identity theft. **But forewarned is forearmed!**

III. What can you do if you become a victim?

You must act quickly once you realize you have become a victim of identity theft. **Quick action may prevent a thief from making further use of your identity and may make the process of restoring your credit rating easier and less stressful.** If you are victimized, you should take the following steps.

Document your actions

You'll soon learn that you will need documentation when reporting identity theft. The following tips will prove useful to you and should make the process of restoring your good name and credit much easier:

- Keep a log of the date, time and substance of all of your personal and telephone conversations regarding the theft. The log also should include the name, title and telephone number of each person with whom you have spoken.
- Follow up each telephone call with a letter that confirms your conversation and any agreed-upon action. You should send all correspondence by certified mail, return receipt requested, and keep a copy of each letter and each return receipt.
- Keep all documentation regarding the theft of your identity in one folder or binder, readily accessible and clearly organized. In complex identity theft cases involving credit, banking and loan fraud, an expandable file with multiple compartments may be the best choice. Consider keeping a "journal" of actions in a computer file that can be easily updated and printed when necessary.

Contact local law enforcement officials

You should immediately file a complaint with your local police or the police in the community in which the identity theft took place. Give the police as much information and documentation as possible. In Connecticut, law enforcement agencies are required by state law to take a complaint from a victim of identity theft, prepare a police report regarding the complaint, give the victim a copy of the report, investigate the allegation and any other related violations and, where necessary, coordinate investigations with other law enforcement agencies. **Make certain that you are provided the case number and a copy of the police report.** You'll find that many creditors, banks, credit reporting agencies and insurance companies require proof of the crime. In many cases, your police report will help quicken the process of documenting the crime. Request that the law enforcement agency keep you informed of any criminal prosecution that may result from your complaint.

If a victim of identity fraud files a police report, the Consumer Data Industry Association, which is the trade association for consumer information reporting agencies, notes that its national credit bureau members—Equifax, TransUnion and Experian—will immediately delete fraudulent data without a re-investigation procedure.

Contact credit bureaus

There are three major credit reporting agencies that provide banks and other lenders information about your credit history. If you believe you are a victim of identity theft, contact the fraud department of one of these credit reporting companies immediately (see contact information below). Tell the department to flag your file with a **fraud alert** and include a statement that creditors should get your permission before opening any new accounts or altering any existing accounts in your name.

At your request, the credit reporting agencies must add an initial fraud alert to any credit reports or credit rating scores they send out for at least 90 days after your request. These alerts:

- Indicate that you have been or may soon become the victim of identity theft.
- Notify the user of the credit report or credit rating score that you do not authorize granting any new credit, extensions of existing credit or additional (or replacement) credit cards for existing accounts unless the identity of the person making the request can be verified.
- *Entitle you to one free credit report, which must be provided by each credit reporting agency within three days of your request.*

Any credit reporting agency receiving such a fraud alert request must notify the other two credit reporting agencies, and these agencies must also follow the same procedures identified above.

If you file an identity theft complaint with any appropriate federal, state or local law enforcement agency, you may request that the credit reporting agencies include an **extended fraud alert** on any credit reports or credit scores they provide to users. This alert will be included for seven years from the date of your request, unless you request earlier termination.

Similar to an initial fraud alert, an extended fraud alert requires any user of the credit report or score to verify the identity of the person making a request for new credit, an extension of existing credit, or ay additional (or replacement) credit cards for *an existing account*. This verification must be accomplished *only* by contacting you in person at a telephone number you provide for this purpose.

Any credit reporting agency receiving an extended fraud alert request must share that request with the other credit reporting agencies and must follow the same procedures listed above. *If you file an extended fraud alert, you may request two free credit reports from each credit reporting agency in the 12 months that follow the date you placed an extended fraud alert on your records.*

You can request that a **security block** or **security freeze** be placed on your credit reports thereby prohibiting credit bureaus from releasing information without permission. Identity thieves often will try to open new credit accounts in a victim's name, and merely

placing an "alert" on one's account does not block *new* credit cards from being issued as a freeze would. Credit reporting agencies have 30 days from receipt of your request to place a security block on your report. Citizens may have the block temporarily or permanently removed at any time.

Should you decide to ask a consumer reporting agency to block the reporting of this information, you must identify the information to block, and provide the consumer reporting agency with proof of your identity and the police report if you did obtain one. The consumer reporting agency can refuse or cancel your request for a block if, for example, you don't provide the necessary documentation, or where the block results from an error or material misrepresentation of fact made by you. If the agency declines or rescinds the block, it must notify you. Once a debt resulting from identity theft has been blocked, a person or business with notice of the block may not sell, transfer, or place the debt for collection.

Beginning January 1, 2006, Connecticut citizens can request that a security freeze be placed on their credit reports prohibiting a credit rating agency from releasing a credit report, or any information in it, without your express authorization. The request must be made in writing by certified mail or by another secure method authorized by the agency. Upon request, the agency must freeze a credit report within 15 business days or within five business days if a police case number accompanies the request.

In addition to filing fraud alerts and blocks on your credit report, when dealing with credit reporting agencies, you should:

- Request that a victim's statement be added to your credit report.
- Check each credit report carefully when you receive it. Look for accounts that you have not opened, charges you have not made, inquiries that you have not initiated and defaults and delinquencies that you have not caused. Check that your name, address and Social Security number are correct on all reports.
- Request that the credit reporting agency remove all information that appears in your credit report as a result of the theft of your personal identification and credit information. It may take some time to have all of this erroneous information removed from each of your credit reports.
- Ask each credit reporting agency to send you a copy of your corrected credit report. Verify that the erroneous information has been removed, and that each report contains the fraud and victim's statement that you requested be placed in your file.
- Order new copies of your credit reports in a few months to verify your corrections and to make sure that no new fraudulent activity has occurred.
- Request your **credit rating score**[1] from each credit reporting agency. In addition

[1] A credit score is a value assigned to several criteria used in making lending decisions. Criteria include the amount you owe on non-mortgage-related accounts such as credit cards, your payment history and credit history. Scorers take this information from your credit report and plug it into formulas that calculate a value (ranging from 300 to 900) representing the amount of risk you pose to a lender. By looking at this value, or score, lenders are able to roughly gauge whether it's a good idea to extend you credit.

- to your score, the credit reporting agency must provide you with a summary of how that score is created and what it means. The agency may charge a fee for this service.
- Block creditors from providing information to credit reporting agencies if that information is the result of identity theft.
- Call 888-5-OPT-OUT toll-free to request that the major credit reporting companies remove your name and address from all marketing mailing lists and promotions.

For your convenience, contact information for each of the three credit reporting agencies is listed below:

TransUnion
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
Phone: (800) 680-7289
Specific requests: To order a copy of your credit report by phone or to place a fraud alert on your report, call (800) 888-4213.
To order a report online, visit www.transunion.com.

Equifax Credit Information Services Inc.
Consumer Fraud Division
P.O. Box 740250
Atlanta, GA 30374
Phone: (800) 525-6285
Specific requests: To order a copy of your credit report by phone or to place a fraud alert on your report, call (800) 685-1111
To order a report online, visit www.equifax.com.

Experian
National Consumer Assistance
P.O. Box 1017
Allen, TX 75013
Phone: (888)-397-3742
Specific requests: To order a copy of your credit report by phone or to place a fraud alert on your report: (888)-397-3742
To order a report online, visit www.experian.com

Contact relevant creditors

After contacting the credit bureaus, you should contact individual creditors to notify them of any accounts that have been tampered with or opened fraudulently. Ask to speak with someone in the security or fraud department. You need to follow up with a letter. When contacting your creditors, you should:

- Tell them that you are the victim of identity theft. Ask each credit card issuer to cancel your card and provide a replacement card with a new account number. Immediately follow up each telephone call with a letter that confirms the conversation and the action the credit card issuer has agreed to take. Send all correspondence by certified mail, return receipt requested.
- Ask each credit card issuer about the status of your account. Ask if the card issuer has received a change of address request or a request for additional or replacement credit cards. Instruct the card issuer not to honor any such requests regarding your account without your written authorization. Your liability for unauthorized use of a credit card cannot exceed $50. Some creditors will waive the $50 if you provide documentation regarding identity theft, for example, a police report.
- Call each credit card issuer or creditor that has opened a new account that you did not authorize. Explain that you are the victim of identity theft and ask each issuer and creditor to close the account immediately. Some credit card issuers and creditors may ask you to sign an affidavit or to submit a copy of a police report. Ask each issuer and creditor to inform the credit reporting agencies that the account was opened fraudulently and has been closed.

For your convenience, contact information for each of the major credit card issuers is listed below:

Visa (800) 847-2911
Mastercard (800) MC-ASSIST
American Express (800) 554-AMEX

Contact your bank

If your bank account information or checks have been stolen, or if a fraudulent bank account has been opened using your identification information, notify the bank involved immediately. Close your bank accounts and obtain new account numbers. Ask the bank to use a new unique identifier for your accounts. Do not use your mother's maiden name, since this information is available in public records.

Be aware that ATM and debit cards do not allow the same protections as credit cards. If your ATM or debit card is lost or stolen, request a new card and PIN number immediately. If you fail to report unauthorized charges within a timely manner, you could be held liable for the charges. The following rules apply to lost or stolen ATM and debit cards:

- If you report an ATM or debit card missing before it is used without your permission, your financial institution cannot hold you responsible for any unauthorized withdrawals. If you report your ATM or debit card lost or stolen within two business days of discovering the loss or theft, your liability is limited to $50.

- If you report your ATM or debit card lost or stolen after two business days, but within 60 days after a statement showing an unauthorized withdrawal, you can be liable for up to $500 of unauthorized activity.
- If you wait more than 60 days, you could be responsible for all unauthorized transactions. It cannot be said too many times: always review your financial statements upon receipt!

Contact check verification companies

Check verification companies are used by businesses and banks to authorize check cashing and checking account privileges. If your identity is stolen, a merchant may refuse to take your check on the advice of a check verification company.

If a merchant refuses your check and refers you to a check verification company, call the check verification company and explain that you are the victim of identity theft. If you cannot open a checking account because your identity has been stolen, call Chex-Systems.

For your convenience, contact information for each of the major check verification companies is listed below:

Global Payments (800) 638-4600
Chex Systems (800) 428-9623
CrossCheck (707) 586-0551
International Check Services (800) 526-5380
SCAN (800) 262-7771
TeleCheck (800) 710-9898

Contact utilities and service providers

Notify your gas, electric, telephone, water, cable and trash utilities that you are the victim of identity theft and alert them to the possibility that the thief may try to establish accounts using your identification information. Ask the utility and telephone services to use a new unique identifier for your accounts. Again, do not use your mother's maiden name, since this information is available in public records. If your long distance calling card or PIN has been stolen, cancel the card and obtain a new account number and PIN.

Contact the Social Security Administration

If your Social Security number has become associated with dishonored checks and bad credit, it is possible, in extreme cases, to obtain a new Social Security number. To obtain a new Social Security number, your situation must fit the Social Security Administration's criteria for issuing a second Social Security number. Contact the Social Security Administration for specific criteria.

If you suspect that someone else is using your Social Security number for employment purposes, request a copy of your Social Security Earnings and Benefits statement. If the statement confirms this use of your Social Security number, contact the Social Security Administration at (800) 269-0271.

Contact the Internal Revenue Service

Contact the Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations. You may contact the Internal Revenue Service by calling (800)-829-0433.

Contact the Post Office

Contact your local office of the Postal Inspection Service if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity. For your convenience, contact information for each of the Postal Inspection Service offices in Connecticut are listed below:

Postal Inspection Service, P.O. Box 8025, New Haven, CT 06530-0025
Tel. (203) 782-7018
Postal Inspection Service, P.O. Box 1700 Wallingford, CT 06492-1300
Tel. (203) 294-6760
Postal Inspection Service, P.O. Box 840, Hartford, CT, 06142
Tel. (860) 524-6454

Contact the Federal Trade Commission (FTC)

The FTC serves as the federal clearinghouse for complaints by victims of identity theft. While the FTC does not resolve individual consumer problems, your complaint helps the FTC investigate fraud and can lead to law enforcement action. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies worldwide.

You also can send an **ID Theft Affidavit** to companies where new accounts were opened in your name. Credit grantors, consumer advocates and the FTC have developed the ID Theft Affidavit to help you report information to companies using one standard form. The information you provide helps companies investigate and decide the outcome of your claim. While many companies accept this affidavit, others require that you submit additional or different forms. Before you send the affidavit, contact each company to determine if they accept the form. This affidavit is **only** for new accounts that were opened in your name without your permission.

You can get a copy of the ID Theft Affidavit from the Federal Trade Commission. For a copy of the ID Theft Affidavit, log on to www.consumer.gov/idtheft/affidavit.htm, or call (877) ID THEFT.

The FTC has also established an Identity Theft Hotline and Web site providing a central place to report identity theft and to obtain helpful information. You may contact the FTC at the address below:

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

FTC Identity Theft Hotline: (877) IDTHEFT (877)-438-4338; TDD (202)-326-2502
Web address: www.consumer.gov/idtheft

Contact an Attorney

The actions of a credit identity thief sometimes may result in civil or criminal judgments entered against you. If you are a victim of credit identity theft and have had an erroneous civil or criminal judgment entered against you, you should consult an attorney about vacating the judgment.

Consult an attorney immediately if you receive demands to pay a debt caused by an identity thief or if you receive notice of a legal action initiated against you based on fraudulent debts incurred by a thief.

Under Connecticut law, victims of identity theft have two years from the date the violation is discovered (or reasonably should have been discovered) to bring a civil action for damages against the offender in Superior Court. Courts must award prevailing plaintiffs the greater of $1,000 or treble damages, costs, and reasonable attorney's fees.

Your rights in the criminal prosecution of identity thieves

To assist victims in any criminal action the state may take against those alleged to have committed identity theft crimes, alleged offenders in Connecticut must be arraigned in the Superior Court for the geographical area *where the victim resides* rather than the area where either the crime was allegedly committed or the arrest made.

Victims of ID theft crimes, as for all crime victims in Connecticut, have important legal rights to participate in the criminal justice process. These rights include:

- the right to be treated with fairness and respect throughout the criminal justice process;
- the right to receive financial restitution;

- the right to a timely disposition of the case following arrest of the accused;
- the right to be reasonably protected from the accused throughout the criminal justice process;
- the right to receive notification of court proceedings and to attend all court proceedings;
- the right to be heard at the plea and sentencing phases of the criminal prosecution;
- the right to receive information about the arrest, conviction, sentence, imprisonment and release of the accused.

If an identity thief is arrested and criminally prosecuted in a Connecticut court, the victim has a right to obtain a written order of financial restitution from the court for monetary loss sustained as a result of the crime. The victim must request that the court issue such an order during the pendancy of the criminal prosecution. In certain cases, exercising your right to receive financial restitution in this way can be less costly, less burdensome and more efficient than hiring an attorney to bring a civil action against the identity thief.

To learn more about your rights as a crime victim in Connecticut or to learn how to assert your rights, contact:

Office of the Victim Advocate
505 Hudson Street
Hartford, Connecticut 06106

Telephone: (860)550-6632 or Toll Free (CT) 1-888-771-3126

Or visit: www.ct.gov/ova

IV. Your identity theft check list

This booklet provides you with detailed information about the nature of ID Theft, how to avoid becoming a victim of ID Theft, and what to do if you become a victim of ID Theft. We know that it may seem overwhelming, but forewarned is forearmed and, if you keep what you've read in mind, you may be able to prevent yourself from ever becoming victimized by identity thieves.

If, unfortunately, you become a victim of identity theft, we provide the checklist below which encapsulates the information you've read in this booklet, to help you clear your good name with creditors and others.

- File a complaint with your local law enforcement agency immediately. Obtain a copy of the police report—you have a right to it! Most likely your bank, credit-card company or other financial institution will require proof that a crime has been committed.

- Request or download an ID Theft Affidavit from the Federal Trade Commission to report an identity theft crime. It is accepted by all three credit bureaus and over 25 major creditors, thereby eliminating the need to file separate hand-written forms with many different companies.

- Call at least one of the "big three" credit reporting agencies. Place a fraud alert on your file. Consider placing a "block" or "freeze" on your credit information.

- Request a current credit report from each credit reporting agency. They are free if you believe you're a victim of fraud and are in addition to the free copies you are entitled to receive even if you are not the victim of identity theft. Examine each report carefully for evidence of fraudulent activity. You should also add a "victim's statement" to your credit file that describes the theft of your identity and requests that creditors contact you before opening new accounts or altering existing accounts in your name. Review your credit reports every few months to verify that the corrections were made and to look for evidence of new fraudulent activity.

- Send a registered letter to all creditors with whom fraudulent accounts have been opened. Include a copy of the police report to substantiate your claim. Request a letter from each creditor acknowledging that the fraud took place and releasing you from liability for fraudulent charges. Also request that creditors report that your previous accounts were closed "at customer request."

- Contact and notify utilities and other service providers to alert them that you have been a victim of identity theft and request that new unique identifiers be established for your accounts.

- Report the loss of an ATM card, debit card, or checkbook to your bank, as well as any other account numbers that may have been stolen. Close existing bank checking and savings accounts and open new ones with new account numbers. Get a new ATM card with a new PIN number.

- Remember that changing bank account numbers will probably also require changing paycheck direct deposit arrangements, pre-authorized account withdrawals, and other types of automated deposits or bill paying services.

- Report a lost or stolen driver's license to the state Division of Motor Vehicles and request a new license with a new number (not your Social Security number).

- Contact the Social Security Fraud Hotline at 1-800-269-0271 if your Social Security number has been misused.

- Report the theft of your mail to commit identity theft, or suspicions about falsified change-of-address forms, to your local post office inspector.

- If identity thieves have made unauthorized phone calls in your name, contact your service provider immediately to dispute the charges and establish new accounts.

- Keep copies of all correspondence with creditors and records of telephone calls (date, time, name of company, contact person, etc.) to document your efforts to correct credit problems.

- Visit www.consumer.gov/idtheft for tips on resolving identity theft problems. Download the booklet *ID Theft: When Bad Things Happen To Your Good Name* or request it by phone from the Federal Trade Commission (FTC). Also visit the Privacy Rights Clearinghouse web site: www.privacyrights.org.

Stay on top of things and be persistent! Cleaning up your credit file will take time and, at times, will feel like a full-time job. According to the Privacy Rights Clearinghouse, average identity theft victims will spend about 175 hours recovering losses and cleaning up their credit history, and about $800 for photocopying, postage, phone calls, and other expenses. But if you’re the victim of identity theft, you cannot put a price on your good name and credit.

Disclaimer

The information contained in this booklet is not provided for the purposes of rendering legal advice or authority. The Office of the Victim Advocate specifically disclaims any liability, loss or risk, personal or otherwise, which is incurred as a consequence, directly or indirectly, of the use and application of any of the contents of this publication.

Credits

The information presented in this guide was assembled from multiple sources. Sections have been reprinted with the permission of the Federal Trade Commission (FTC).

To order additional copies of this guide, please contact:

Office of the Victim Advocate
OVA

505 Hudson Street · Hartford, Connecticut 06106
Phone: (860) 550-6632 · Toll Free 1-888-771-3126
Fax: (860) 566-3542

Visit us on the web at www.ct.gov/ova