

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, CT 06106  
Phone (860)550-6632 • Toll Free 1-888-771-3126  
Fax (860)566-3542

Visit us on the web at [www.ova.state.ct.us](http://www.ova.state.ct.us)



Dear Connecticut Citizen:

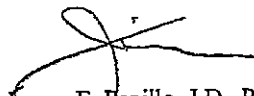
This Guide has been published to help raise awareness in Connecticut of identity (ID) theft—America's fastest growing, yet vastly underreported, crime. It describes the nature of identity theft; how it is committed; how to avoid becoming a victim of identity theft; and what to do if you become a victim of identity theft.

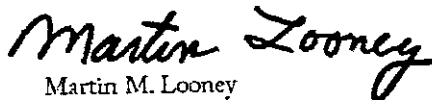
This Guide was officially released at the *Conference on Identity Theft*, sponsored by the undersigned, at the state capitol on November 9, 2004.

ID theft is one of the most frustrating crimes to deal with. ID thieves can be hard to catch. Victims of ID theft often face extreme difficulties attempting to clear damaged credit and can be left with the bills, charges, bad checks and taxes. Victims can spend months or years, and a good amount of money, restoring the damage to their good name and credit record.

There is help for Connecticut citizens! Our state lawmakers have taken steps to better catch and prosecute ID thieves and to help alleviate the frustration and financial burden victims of ID theft often experience.

We 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.  
Victim Advocate, State of Connecticut

  
Martin M. Looney  
State Senate Majority Leader

## Contents

|  |    |
|--|----|
| Letter to Connecticut Citizens   |    |
| The Nature of Identity Theft.....  | 1  |
| Identity Theft Connecticut Information.....                                  | 2  |
| How Identity Theft is Committed.....   | 3  |
| How Can You Tell if You're the Victim<br>Of Identity Theft?.....             | 4  |
| What Can You Do?.....  | 4  |
| <i>Document Your Actions</i> .....   | 4  |
| <i>Contact Credit Bureaus</i> .....  | 5  |
| <i>Contact Relevant Creditors</i> .....                                      | 7  |
| <i>Contact Your Bank</i> .....   | 8  |
| <i>Check Verification Companies</i> .....                                    | 8  |
| <i>Contact Utilities and Services</i> .....                                  | 9  |
| <i>Forms of Identification</i> .....   | 9  |
| <i>Contact the Internal Revenue Service</i> .....                            | 9  |
| <i>Contact the Post Office</i> .....   | 9  |
| <i>Other Information</i> .....   | 10 |
| <i>Potential Problems</i> .....  | 10 |
| <i>Fill Out an ID Theft Affidavit</i> .....                                  | 11 |
| <i>Contact the Federal Trade Commission</i> .....                            | 11 |
| <i>Contact Local Enforcement Officials</i> .....                             | 12 |
| <br>   |    |
| Connecticut Laws on ID Theft.....  | 12 |
| <i>Crimes</i> .....  | 13 |
| <i>ID Theft Reporting and Processing</i> .....                               | 13 |
| <i>Credit Protection for ID Theft Victims</i> .....                          | 13 |
| <i>Civil Action for Damages</i> .....  | 14 |
| <i>Prohibition Against Account Numbers on Receipts</i> .....                 | 14 |
| <i>Prohibition Against Publicly Disclosing Social Security Numbers</i> ..... | 14 |
| <br>   |    |
| Red Flag Warnings .....  | 15 |
| <br>   |    |
| Checklist.....   | 16 |
| <br>   |    |
| Credits.....   | 18 |
| <br>   |    |
| Disclaimer.....  | 18 |

## The Nature of Identity Theft



Identity (ID) theft is a growing crisis in Connecticut as it is throughout the United States. ID theft is also one of the most frustrating crimes to deal with. As the crime becomes more visible, stories of victims' complex experiences permeate the media. Identity theft occurs when someone invades your life, taking pieces of your personal identifying information as his or her own, and ruins your financial reputation. Victims of identity theft face extreme difficulties attempting to clear the damaged credit, or even criminal record, caused by the thief.

ID theft occurs when someone uses your name, your Social Security number, your credit card number or some other piece of your personal information. Someone appropriates your personal information without your knowledge to commit fraud or theft.

Your personal information can be used to open credit card 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 the bills, charges, bad checks and taxes. Victims of ID theft can spend months or years, and a lot of money, restoring the damage to their good name and credit record.

Identity theft has been called America's fastest growing crime. The FBI estimates that 500,000 to 700,000 Americans become identity theft victims each year. The results of a study conducted for the Federal Trade Commission (FTC) which concluded in the summer of 2003 suggests that almost 10 million Americans have discovered that they were the victim of some form of ID theft within the last year. The study showed that 27 million Americans have been victimized by ID theft since 1998. ID theft is a multi-billion dollar problem. The FTC study went on to show 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 easier now than at any time in the past, 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." Existing laws consider the victim to be the business defrauded -- not the person whose identity was stolen. New laws recognizing the person whose identity was stolen as a victim are being written, however, 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. In the case of ID theft, the victim is not only victimized by the criminal, but often is further victimized by lax legal protections, apathetic merchants, and uncooperative credit and banking institutions. There is no short-cut to fixing problems caused by ID theft.

The biggest problem with ID theft is catching the criminals. You may not know your identity

has been stolen until you notice that something is awry. Time can pass before you realize you haven't received a credit card statement or notice the strange bills you are receiving.

Experts have determined that:

- Early detection significantly reduces the damage.
- Only 25% of victims report theft of identity to local police.
- Only 22% of victims report identity theft to a credit bureau.
- Most ID theft starts with a stolen wallet, purse, or mail.

## Identity Theft Connecticut Information



The most recent statistics published by the Federal Trade Commission dated January 22, 2004, shows that 3,368 fraud complaints were made by Connecticut residents during 2003. Connecticut is ranked 18<sup>th</sup> in the United States.

Between 2002 and 2003, there was a 28% increase in the number of complaints filed with the FTC from Connecticut citizens.

The following table shows the most frequent types of ID theft reported by Connecticut residents during 2003.

**Identity Theft Types  
Reported by Connecticut Victims  
(Calendar Year 2003)**

| Rank | Identity Theft Type                    | No. of Victims | Percentage |
|------|--|----------------|------------|
| 1    | Credit Card Fraud                      | 713            | 37%        |
| 2    | Phone or Utilities Fraud               | 459            | 24%        |
| 3    | Bank Fraud                             | 234            | 12%        |
| 4    | Employment-Related Fraud               | 142            | 7%         |
| 5    | Loan Fraud                             | 132            | 7%         |
| 6    | Government Documents or Benefits Fraud | 116            | 6%         |
| -    | Other                                  | 367            | 19%        |
| -    | Attempted Identity Theft               | 168            | 9%         |

Percentages are based on the 1,913 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.

The following table shows the top five Connecticut cities where ID theft victims resided at the time they reported their complaints.

**Top Connecticut Identity Theft Victim Locations  
(Calendar Year 2003)**

| Victim City | No. of Victims |
|-------------|----------------|
| Hartford    | 152            |
| New Haven   | 92             |
| Bridgeport  | 86             |
| Stamford    | 54             |
| Waterbury   | 54             |

## How Identity Theft is Committed



Skilled identity thieves use a variety of methods to gain access to your personal information. According to the Federal Trade Commission (FTC):

- They 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.
- They rummage through your trash, or the trash of businesses or dumps in a practice known as "dumpster diving."
- They 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.
- They steal credit and debit card numbers as your card is processed by using a special information storage device in a practice known as "skimming."
- They steal wallets and purses containing identification and credit and bank cards.
- They steal mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.
- They complete a "change of address form" to divert your mail to another location.
- They steal personal information from your home.
- They scam information from you by posing as a legitimate business person or government official.

Once identity thieves have your personal information, they may:

- Go on spending sprees using your credit and debit card account numbers to buy "big-ticket" items like computers that they can easily sell.
- Open a new credit card account, using your name, date of birth, and SSN. When they don't pay the bills, the delinquent account is reported on your credit report.
- Change the mailing address on your credit card account. The imposter then runs up charges on the account. Because the bills are being sent to the new address, it may take

- some time before you realize there's a problem.
- Take out auto loans in your name.
- Establish phone or wireless service in your name.
- 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 under 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 show up for their court date, an arrest warrant could be issued in your name.

## **How Can You Tell if You're the Victim of Identity Theft?**



Many times the victim is unaware of the theft until they attempt to get more credit themselves, or until a few months of non-payment on the new accounts has passed.

People discover that they have become victims of identity thieves in a variety of ways. Experts suggest that you monitor the balances of your financial accounts and look for unexplained charges or withdrawals. According to the FTC, other 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.
- Denial of credit for no apparent reason.
- Receiving calls from debt collectors or companies about merchandise or services you didn't buy.

## **What can you do?**



Victims of identity theft must act quickly when they realize they have been victimized. Quick action may prevent the thief from making further use of the victim's identity, and may make the process of restoring the victim's credit rating easier and less stressful.

As soon as the victim realizes their identity has been stolen, the victim must take action:

### **Document Your Actions**

- Keep a log of the date, time and substance of all personal and telephone conversations regarding the theft. The log also should include the name, title and telephone number of each person to whom the victim speaks.
- Follow up each telephone call with a letter that confirms the conversation and any agreed-

upon action. The victim should send all correspondence by certified mail, return receipt requested, and keep a copy of each letter and each return receipt.

- Report the crime to the police immediately. Ask the police to issue a police report pursuant to the theft of your personal identification information. Give the police as much information and documentation as possible. Creditors, banks, credit reporting agencies and insurance companies may require a police report to verify the crime of identity theft.
- Call the fraud units of the three major credit reporting agencies. Inform each credit reporting agency of the identity theft. Follow the steps outlined under "Protect Your Credit History."
- Keep all documentation regarding the identity theft 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 a copy is needed.

## Contact Credit Bureaus

Contact the fraud department of one of the three major credit bureaus (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 in your name.

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

- Indicate that the consumer has been or may be about to become the victim of fraud (including identity theft).
- Notify the user of the credit report or score that the consumer does not authorize granting any new credit, extensions of existing credit, or additional (or replacement) credit cards for existing accounts unless the user verifies the identity of the person making the request.
- Entitle the consumer to one free credit report, which must be provided by the credit reporting agency within 3 days of the request.

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

If a consumer files an identity theft report with any appropriate federal, state, or local law enforcement agency, the consumer may then request the credit reporting agencies to include an extended fraud alert on any credit reports or credit scores they provide to users. This alert will be included for 7 years from the date of the request, unless the consumer requests 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 an additional (or replacement) credit card for an existing account. This verification must be accomplished by contacting the consumer in person at a telephone



number the consumer has provided for this purpose; it is not sufficient for the user to verify the identity of the person making the request by any other means.

Any credit reporting agency receiving an extended fraud alert request must share that request with the other credit reporting agencies, which must follow the same procedures. Upon request, consumers may get two free credit reports from each credit reporting agency within 12 months after filing the extended fraud alert request.

#### Additional Steps to Take:

- 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 that 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 is correct on all reports.
- Request from the credit reporting agency you contact to 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.
- You should order new copies of your reports in a few months to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.
- Upon request, each credit reporting agency must provide a consumer with his/her credit rating score (which indicates the consumer's credit risk). The credit reporting agency must also provide a summary of how the score is created and what it means. The agency may charge a fee for this service.
- Consumers victimized by identity theft may block creditors from providing information to credit reporting agencies if that information is the result of identity theft. Similarly, at the request of the consumer, credit reporting agencies must notify providers of credit information that the information provided is the result of identity theft, and those providers must take steps to ensure that such information is not resubmitted to the credit reporting agencies.

## Credit bureau contact information:

### TransUnion

Fraud Victim Assistance Department  
P.O. Box 6790  
Fullerton, CA 92834  
Phone: 1-(800) 680-7289

- » To order a copy of your credit report by phone: 1-(800) 888-4213.
- » To order a report online, visit [www.transunion.com](http://www.transunion.com).

### Equifax Credit Information Services Inc.

Consumer Fraud Division  
P.O. Box 740250  
Atlanta, GA 30374  
Phone: 1-(800) 525-6285

- » To order a copy of your credit report by phone: 1-(800) 685-1111
- » To order a report online, visit [www.equifax.com](http://www.equifax.com).

### Experian

National Consumer Assistance  
P.O. Box 1017  
Allen, TX 75013

- » To order a copy of your credit report by phone or to place a fraud alert on your report: 1-888-397-3742
- » To order a report online, visit [www.experian.com](http://www.experian.com)

Check each credit report carefully when you receive it. Look for accounts that you have not opened; charges that 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 is correct on all reports.

## Contact Relevant Creditors

- Call each of your credit card issuers to report 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.
- 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 requests regarding your card without written authorization.
- A consumer's liability for unauthorized use of a credit card cannot be more than \$50. Some creditors will waive the \$50 if the victim provides documentation regarding identity theft (i.e. police reports).
- Call each credit card issuer or creditor that has opened a new account that you did not authorize or apply for, as listed in your credit reports. 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 the

police report on the theft of your personal identification information. Ask each issuer and creditor to inform each credit reporting agency that the account was opened fraudulently and has been closed.

### **How to Contact Visa, MasterCard, and American Express:**

Visa - (800) 847-2911

Mastercard - (800) MC-ASSIST

American Express - (800) 554-AMEX

### **ATM and Debit Cards**

Be aware that ATM and debit cards do not allow the same protections as credit cards. If you fail to report unauthorized charges within a timely manner, you could be held liable for the charges.

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 the two business days, but within 60 days after a statement showing an unauthorized withdrawal, you can be liable for up to \$500 of what a thief withdraws.

If you wait more than 60 days, you could lose all the money that was taken from your account after the end of the 60 days and before you report the card missing.

### **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.
- Get a new ATM card and PIN. Do not use your old password or PIN.

### **Check Verification Companies**

Check verification companies are used by businesses and banks to authorize check cashing and checking account privileges. Due to the actions of an identity thief, a merchant may refuse to take a victim's check on the advice of a check verification company. The major check verification companies in the United States are:

|                              |                |
|------------------------------|----------------|
| 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 |

- 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 of the thief's activities, call Chex-Systems.

### **Contact Utilities and Services**

- Notify your gas, electric, 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. Provide similar notice to your local, long distance and cellular telephone services. Ask the utility and telephone services 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. If your long distance calling card or PIN has been stolen, cancel them and obtain a new account number and PIN.

### **Forms of Identification**

- 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. In order 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.

Call the Social Security Administration if you suspect that your Social Security number is being fraudulently used. The telephone number is 1-800-269-0271.

### **Contact The Internal Revenue Service**

Contact the Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations. The telephone number is 1-800-829-0433.

### **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.

### **Other Information**

- Banks, creditors and government entities may ask you to fill out fraud affidavits to be notarized or signed under penalty of perjury.
- If you suspect that an identity thief has stolen your mail or has filed a change of address request in your name, notify your local Postal Inspector.
- If you have a passport, notify your local passport office that the identity thief may apply for a new passport using your identity.
- The actions of a credit identity thief sometimes result in civil or criminal judgments being entered against the victim. 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.
- Call toll-free 888-5-OPT-OUT and request that the major credit reporting companies remove your name and address from any and all marketing mailing lists and promotions.

### **Potential Problems**

- Occasionally, a victim of credit identity theft may encounter a creditor or credit reporting agency that unreasonably refuses to cooperate with the victim as the victim seeks to restore his or her credit standing.
- The victim may notify a creditor that he or she is the victim of credit identity theft, and may provide the creditor appropriate documentation, but the creditor continues to send report of debts incurred by the thief to the credit reporting agencies.
- The victim may provide a credit reporting agency appropriate documentation and request the erroneous information be removed from the victim's credit report, but the credit reporting agency does not remove the erroneous information.
- If you are a victim of credit identity theft, and if you believe that a creditor or a credit reporting agency unreasonably or carelessly continues to report erroneous information that is the result of the theft of your personal identification and credit information, consider seeking assistance from an attorney.
- If a debt collector demands that the victim pay a debt incurred by an identity thief, the victim should explain why he or she does not owe the debt, and should send the debt collector a follow-up should consult an attorney immediately if the victim receives demands to pay a debt caused by an identity thief, or if the victim receives notice of a legal action based on debts incurred by a thief.

After contacting the credit bureaus, you should contact the creditors for 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. This step is one of the procedures outlined in the Fair Credit Billing Act for resolving errors on credit billing statements, including charges that you have not made. The Federal Trade Commission has information about the Fair Credit Billing Act.

## **Fill Out an ID Theft Affidavit**

You also can send an ID Theft Affidavit to companies where new accounts were opened in your name. This affidavit is not required, but it does help you explain your case. Credit grantors, consumer advocates and the Federal Trade Commission 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 more or different forms. Before you send the affidavit, contact each company to find out whether the form is accepted. If someone made unauthorized charges to existing accounts, deal directly with your credit card companies about those charges. The affidavit is for new accounts that were opened up in your name without your permission. You can get a copy of the ID Theft Affidavit from the Federal Trade Commission.

## **Contact the Federal Trade Commission (FTC): Be A Part of the Identity Theft Data Clearinghouse**

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.

The Identity Theft Data Clearinghouse is the federal government's database for tracking identity theft complaints. It was created as a part of the Identity Theft and Assumption Deterrence Act of 1998. The FTC established the Identity Theft hot line and Web site to give identity theft victims a central place in the government to report their problems and receive helpful information.

To contact the Clearinghouse, obtain an Identity Theft Claim form and for further information:

- Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
» FTC's Identity Theft Hotline:  
1-877 IDTHEFT (1-877 438-4338), TDD: 1-(202) 326-2502

Online: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

Complaints received from victims of identity theft by way of the hot line or an online complaint form are entered into the data clearinghouse. The clearinghouse, an integrated part of the Consumer Sentinel system, contains more than 279,000 complaints as of January 1, 2003.

## Contact Local Law Enforcement Officials

Finally, don't forget to file a complaint with your local police or the police in the community where the identity theft took place. In Connecticut, local law enforcement agencies must now accept the complaint, prepare a police report, give the complainant a copy of the report, investigate the allegation and any other related violations and, where necessary, must coordinate investigations with other law enforcement agencies.

Keep a copy of this report in case your creditors need proof of the crime. In some cases, your police report will help quicken the process when dealing with the three major credit bureaus. The Consumer Data Industry Association, which is the trade association for consumer information reporting agencies, states that if a victim of identity fraud files a police report, its national credit bureau members—Equifax, TransUnion and Experian—will immediately delete fraudulent data without the reinvestigation procedure.

## Connecticut Laws on Identity Theft



In 2003, our state legislature enacted legislation, Public Act 03-156, which imposed graduated penalties for identity theft violations; established procedures to assist victims of identity theft; and requires businesses to revise certain practices to prevent identity theft.

Effective October 1, 2003, identity theft is a class B, C, or D felony in Connecticut, depending on the value of the goods or services involved.

It is now also a crime in Connecticut to give, sell, or otherwise transfer another person's personal identifying information.

In addition, Connecticut law now allows victims of ID theft to bring civil actions for damages against their offenders.

### Crimes

Effective October 1, 2003:

A person commits **third-degree identity theft** when he intentionally obtains, without permission, another person's personal identifying information and uses it to illegally obtain or attempt to obtain money, credit, goods, services, property, or medical information. Third-degree identity theft is a class D felony, punishable by up to five years imprisonment, a \$2,000 fine, or both (CGS § 53a-129a, as amended by PA 03-156).

"Personal identifying information" includes any name, number, or other information that may be used, alone or with any other information, to identify a specific individual. Specifically, it includes a person's date of birth; employer or taxpayer identification, alien registration, government passport, health insurance identification, or debit card number; or unique biometric data, such as a fingerprint, voice print, retina or iris-image, or other unique physical

representation.

It is **second-degree identity theft**, a class C felony, to commit identity theft involving money, credit, goods, property, or services valued at over \$5,000.

It is **first-degree identity theft**, a class B felony, if the value is over \$10,000.

A class C felony is punishable by up to 10 years imprisonment, a \$10,000 fine, or both. A class B felony is punishable by up to 20 years imprisonment, a \$15,000 fine, or both.

It is a class D felony for anyone to sell, give, or otherwise transfer another person's personal identifying information to a third person knowing that the (1) information was obtained without the owner's authorization and (2) third person intends to use it for an unlawful purpose.

### **Identity Theft Reporting and Processing**

Connecticut citizens who believe that they are identity theft victims may file complaints with the law enforcement agency in the town where they live. The agency must now accept the complaint, prepare a police report, give the complainant a copy of the report, and investigate the allegation and any other related violations. Where necessary, the agency must coordinate investigations with other law enforcement agencies.

The alleged identity theft offenders must be arraigned in the Superior Court for the geographical area where the victim lives rather than the area where either the crime was allegedly committed or the arrest was made.

### **Credit Protection for Identity Theft Victims**

People who believe that they are identity theft victims can ask most credit rating agencies to block and not report information appearing on their credit reports as a result of the crime. Within 30 days after receiving the request, the agency must stop reporting any information that resulted from the crime. The agency must also promptly notify the person or business that furnished the information of the police report and the effective date of the block.

A credit rating agency may decline to block or rescind a block if it has a good faith belief that the consumer (1) misrepresented the facts in the request for a block; (2) agrees that information, or portions of it, was blocked in error; (3) knew or should have known that he received goods, services, or money as a result of blocked transactions; (4) knew of, or participated in, fraud to get the information blocked; or (5) lied about being a crime victim. The agency must give consumers prompt written notice of their decision not to block or to rescind a block on information.

Credit rating agencies that willfully violate the blocking provision or prohibition against reporting credit information resulting from identity theft are subject to the same graduated penalty that they face for (1) failing to disclose to consumers, upon request, information in



their credit report or (2) improperly charging them for the information. The penalty is up to a \$ 100 fine for a first offense, up to \$ 500 fine for a second, and up to a \$ 1,000 fine or six-month prison term for each subsequent offense.

### **Civil Action for Damages**

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 greatest of \$ 1,000 or treble damages, costs, and reasonable attorney's fees (CGS § 51-571h, as amended by PA 03-156).

### **Prohibition Against Account Numbers on Receipts**

Beginning January 1, 2005, the law prohibits individuals and businesses, other than the state or its political subdivisions, that accept credit or debit cards from printing more than the last five digits of the cards' account numbers or expiration dates on consumers' receipts. The prohibition applies only to electronic receipts and not to transactions solely recorded by handwriting or by imprinting the card.

The penalty for willful violations is up to a \$ 100 fine for the first offense, up to a \$ 500 fine for a second offense, and up to a \$ 1,000 fine or six months in prison for each subsequent offense (PA 03-156).

### **Prohibition Against Publicly Disclosing Social Security Numbers**

With certain exceptions, the law prohibits individuals and businesses from publicly disclosing Social Security numbers. The prohibition does not prevent the numbers from being (1) collected, used, or released as required by state or federal law or (2) used for internal verification or administrative purposes.

Beginning January 1, 2005, the law prohibits any person, firm, corporation, or other entity, other than the state or its political subdivisions, from:

1. intentionally communicating or otherwise making available to the general public an individual's Social Security number;
2. printing anyone's Social Security number on any card that the person must use to access the person or entity's products or services;
3. requiring anyone to transmit his Social Security number over the Internet, unless the connection is secure or the number is encrypted; or
4. requiring anyone to use his Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication is also

required to access it.

The prohibition against publicly disclosing Social Security numbers does not apply to certain individual and group health insurance policies delivered, issued for delivery, renewed, or continued on and after July 1, 2005. The affected policies cover (1) basic hospital, (2) basic medical-surgical, (3) major medical expenses, (4) accident only, (5) limited benefit, and (6) hospital and medical expenses paid by HMOs.

The penalty for willful violations is up to a \$100 fine for the first offense, up to a \$500 fine for a second offense, and up to a \$1,000 fine or six months in prison for each subsequent offense (PA 03-156).

### Red Flag Warnings

Below are some "red flag" warnings that you may be a victim of identity theft:

- Calls or letters from creditors or collection agencies demanding payment for items that you never bought or for accounts that you never opened.
- Information in your credit file about accounts that you never opened.
- Calls from creditors, or potential creditors, about suspicious new accounts, a large volume of credit card activity, wire transfers, etc.
- Unauthorized withdrawals from bank accounts.
- Your wallet, purse, or cell phone is lost or stolen. Ditto for paycheck stubs and credit card receipts.
- Credit card or telephone bills do not arrive on time as regularly scheduled (your mail may have been diverted to another address).
- Replacement credit cards have not been received prior to the expiration date on previous cards.



## Check List

The following are recommended steps to clear your good name with creditors and others:

- Visit [www.consumer.gov/idtheft](http://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: [ww.privacyrights.org](http://ww.privacyrights.org).
- Request or download a uniform affidavit form from the FTC (see above contact information), which was developed in 2002 for victims to use to report a 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: Experian, Equifax, or TransUnion. Place a fraud alert on your file (reality check: fraud alerts are not fool proof. Unfortunately, some creditors overlook them and still open new accounts for identity thieves).
- Also request a current credit report (they're free if you believe you're a victim of fraud) from each credit reporting agency. Examine each report carefully for evidence of fraudulent activity. You can also add a "victim's statement" to your credit file that describes what happened and requests that creditors contact you before opening new accounts in your name. Review your credit reports every few months to verify that corrections were made and to look for evidence of new fraudulent activity.
- File a police crime report immediately in your hometown and/or with police in the location where your wallet was stolen, or where fraudulent charges were made. Get a copy of the police report in case your bank, credit card company or other financial institution needs proof of the crime.
- Send a registered letter to all creditors where fraudulent accounts have been opened. Include a copy of the police report to back up your claim. Request a letter from each creditor that acknowledges that the fraud took place and releases you from liability for fraudulent charges. Also request that they report that your previous accounts were closed "at customer request."
- 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 (e.g., monthly car loan payments).

- 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 stealing 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 and person talked to) to document your efforts to correct credit problems.

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.



## **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) and the Office of Legislative Research (OLR), State of Connecticut.

## **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 and State Senator Martin M. Looney specifically disclaim 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.

To order more copies of this Guide, please contact the  
Office of the Victim Advocate or visit our website

November, 2004