

CONNECTICUT

IDENTITY THEFT RANKING BY STATE: Rank 19, 68.8 Complaints Per 100,000
Population, 2409 Complaints (2007)
Updated November 28, 2008

Current Laws: A person commits 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. The punishment depends on the value of the money, credit, goods, property, or services stolen. If the value is over \$10,000, it is considered first degree identity theft, which is a Class B felony punishable by up to twenty years imprisonment and/or a \$15,000 fine. If the value is between \$5000 and \$10,000, it is second degree identity theft, a class C felony punishable by up to ten years imprisonment and/or a \$10,000 fine. Below a value of \$5000, it is third degree identity theft, a class D felony punishable by up to five years in prison and/or a \$2000 fine.

In addition, 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 information was obtained without the owner's authorization and the third person intends to use it for an unlawful purpose.

"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. It includes, but is not limited to, an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation.

Statute: §53a-129a: <http://www.cga.ct.gov/2007/pub/Chap952.htm#Sec53a-129a.htm>

Jurisdiction: 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.

Statute: §54-1d: <http://www.cga.ct.gov/2007/pub/Chap959.htm#Sec54-1n.htm>

Payment Card Numbers: It is a class A misdemeanor, punishable by up to one year in jail and/or a fine up to \$2000, for any person to:

- Make or cause to be made, either directly or indirectly, any false statement in writing, knowing it to be false and with intent that it be relied on, respecting his identity or that of any other person or his financial condition or that of any other person, for the purpose of procuring the issuance of a credit card.

Statute: §53a-128b: <http://www.cga.ct.gov/2007/pub/Chap952.htm#Sec53a-128b.htm>

- Take a credit card from the person, possession, custody, or control of another without the consent of the cardholder or issuer; or who, with knowledge that it has been so taken, receives the card with intent to use, sell, or transfer it to any other person.
- Receive a credit card that he knows to have been lost, mislaid, or delivered under mistake as to the identity or address of the cardholder, and who retains possession, custody or control with intent to use, sell, or transfer it to any person other than the issuer or the cardholder.
- If not the issuer, sell a credit card or purchase a credit card from someone other than the issuer.
- Sign a credit card, if not the cardholder or any person authorized by him, with intent to defraud the issuer, a participating party, or a person providing money, goods, services or anything else of value, or any other person.

It is a class D felony for a person to:

- During a twelve-month period, receive credit cards issued in the names of two or more people, which he has reason to know were taken or retained under circumstances that constitute credit card theft.

Statute: §53a-128c: <http://www.cga.ct.gov/2007/pub/Chap952.htm#Sec53a-128c.htm>

It is unlawful for any person, with intent to defraud the issuer, a participating party, or a person providing money, goods, services or anything else of value, or any other person, to:

- Use for the purpose of obtaining money, goods, services or anything else of value a credit card obtained or retained in fraudulently or a credit card that he knows is forged, expired or revoked; or
- Obtain money, goods, services, or anything else of value by representing without consent of the cardholder that he is the holder of a specified card or by representing that he is the holder of a specified card or by representing that he is the holder of a card and such card has not in fact been issued.

Violations are a class A misdemeanor if the value of all money, goods, services and other things of value obtained in violation of this subsection does not exceed \$500 in any six-month period.

If it exceeds \$500, it is a class D felony.

Statute: §53a-128d: <http://www.cga.ct.gov/2007/pub/Chap952.htm#Sec53a-128d.htm>

Scanning Devices: State law prohibits the use and possession with intent to use of a scanning device or reencoder that is used to obtain or record encoded information from the magnetic strip of a payment card without permission of the cardholder to defraud the authorized cardholder, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or computer chip of a credit card. A reencoder is an electronic device that places encoded information from the magnetic strip or computer chip of a credit card onto the magnetic strip or stripe of a different card. Violators are subject to one to ten years in prison, and a fine of up to \$10,000. Possession of a scanning device or reencoder under circumstances showing intent to violate the law is a class A misdemeanor.

Statute: §53-388a: <http://www.cga.ct.gov/2007/pub/Chap949.htm>

Social Security Numbers: With certain exceptions, state law prohibits individuals and businesses from publicly disclosing Social Security numbers (SSNs). The prohibition does not prevent the numbers from being collected, used, or released as required by state or federal law or used for internal verification or administrative purposes. However, the law prohibits any person, firm, corporation, or other entity, other than the state or its political subdivisions, from:

- Intentionally communicating or otherwise making available to the general public an individual's Social Security number;
- Printing anyone's Social Security number on any card that the person must use to access the person or entity's products or services;
- Requiring anyone to transmit his Social Security number over the Internet, unless the connection is secure or the number is encrypted; or
- 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 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.

Statute: §42-470: <http://www.cga.ct.gov/2007/pub/Chap743dd.htm>

In addition, any person who collects Social Security numbers in the course of business must create a privacy protection policy which must be published or publicly displayed. "Publicly displayed" includes, but is not limited to, posting on an Internet web page. The policy must: (1) Protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers. This does not apply to any agency or political subdivision of the state.

Violators will be subject to a civil penalty of up to \$500 for each violation, provided that the penalty may not exceed \$500,000 for any single event. It is not a violation if it was unintentional.

Text of Legislation: <http://www.cga.ct.gov/2008/ACT/PA/2008PA-00167-R00HB-05658-PA.htm>

Disposal of Customer Records: Any person in possession of personal information of another person must safeguard the data, computer file and documents containing the information from misuse by third parties. In addition, a person must destroy, erase, or make unreadable such data, files, and documents prior to disposal. "Personal information" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. Violators will be subject to a civil penalty of up to \$500 for each violation, provided that the penalty may not exceed \$500,000 for any single event. It is not a violation if it was unintentional.

Text of Legislation: <http://www.cga.ct.gov/2008/ACT/PA/2008PA-00167-R00HB-05658-PA.htm>

Victim Assistance:

Mandatory Police Reports: Any person who believes he or she is a victim of identity theft may file a complaint with the law enforcement agency for the town in which he or she resides. The agency must accept the complaint, prepare a police report, give a copy of the report to the complainant, and investigate the alleged violation, coordinating if necessary with other law enforcement agencies.

Statute: §54-1n: <http://www.cga.ct.gov/2007/pub/Chap959.htm#Sec54-1n.htm>

Civil Suits: Connecticut law allows victims of identity theft to bring civil actions for damages against their offenders. The victim will be rewarded \$1000 or treble damages, whichever is greater, in addition to costs and reasonable attorney's fees. The statute of limitations to bring such a case is two years from the date when the violation is discovered or in the exercise of reasonable care should have been discovered.

Statute: §52-571h: <http://www.cga.ct.gov/2007/pub/Chap925.htm#Sec52-571h.htm>

Security Freeze: All Connecticut consumers are allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information. To request a freeze, a consumer must request one in writing by certified mail or through any other secure method as authorized by the consumer reporting agency. The agencies may charge a fee of up to \$10 for each security freeze, removal of such freeze or temporary lift of such freeze for a period of time, and a fee of up to \$12 for a temporary lift of such freeze for a specific party.

Credit reporting agencies must place the freeze within five business days of receiving the request, and within ten days, must provide the consumer with written confirmation of the freeze and a unique personal identification number, password or similar device to be used by the consumer when providing authorization for the release of the consumer's credit report to a specific person or for a specific period of time or for permanent removal of the freeze. Requests for a temporary unlocking of the freeze must be completed within three business days.

Statute: §36a-701a: <http://www.cga.ct.gov/2007/pub/Chap669.htm#Sec36a-701.htm>

How to Place a Security Freeze: www.consumersunion.org/pdf/security/securityCT.pdf

Security Breach: State law requires a person who conducts business in the state and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, to disclose any breach of security to any resident whose personal information was, or is reasonably believed to have been, accessed by an authorized person. "Breach of security" means unauthorized access to or acquisition of electronic files, media, databases, or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Personal information is defined as an individual's first name or first initial and last name in combination with any one or more of the following data: Social Security number; driver's license

number or state identification card number; or an account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

The disclosure shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, and completion of an investigation to determine the nature or scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the data system. Notification is not required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Notification can be provided by mail, telephone, or e-mail. If the cost of providing regular notice would exceed \$250,000, the amount of people to be notified exceeds 500,000, or the agency does not have sufficient contact information to provide written or electronic notice, substitute notice may be provided. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the person's web site, and notification to major statewide media, including newspapers, radio and television.

Statute: §36a-701b: <http://www.cga.ct.gov/2007/pub/Chap669.htm#Sec36a-701b.htm>

Credit Blocking: 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.

Statute: §36a-699f: <http://www.cga.ct.gov/2007/pub/Chap669.htm#Sec36a-701b.htm>

State Resources:

Office of the Victim Advocate, "Identity Theft: A Guide for Connecticut Citizens"

(www.ct.gov/ova/lib/ova/Identity_Theft_Guide_2005_For_PDF.pdf)

This comprehensive 22-page document includes a detailed list of steps identity theft victims should take, including directing victims to: "*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.*"

"Protect Yourself Against Identity Theft"

(http://www.ct.gov/dcp/lib/dcp/pdf/factsheets/identity_theft0107_final_for_web.pdf)

Office of the Attorney General, "Identity Theft Alert"

(<http://www.ct.gov/ag/cwp/view.asp?A=2066&Q=292644>)

This document directs identity theft victims to: "*Contact your local police. In Connecticut, identity theft is a Class D Felony, under CGS53a-129, punishable by one to five years in prison and a fine.*"

Connecticut State Police, "Prevent Identity Theft"

(http://www.ct.gov/dps/lib/dps/public_information_files/brochures/identity_theft.pdf)

Department of Consumer Protection, "Identity Theft Information and Resources"

(<http://www.ct.gov/dcp/cwp/view.asp?a=1629&q=289474>)

- "How You Can Safeguard Your Identity"
(<http://www.ct.gov/dcp/cwp/view.asp?a=1629&Q=289476&PM=1>)
- "How Do Find Out If You Are an ID Theft Victim"
(<http://www.ct.gov/dcp/cwp/view.asp?a=1629&Q=289484&PM=1>)
- "What To Do If ID Theft Happens To You"
(<http://www.ct.gov/dcp/cwp/view.asp?a=1629&Q=289488&PM=1>)

This document instructs victims to: "*First, report the crime to your local police **immediately** and ask them to issue a police report about the theft. In Connecticut, local law enforcement must accept the complaint, prepare a police report, 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. Keep a copy of your police report to share with your creditors. It may help quicken the process when dealing with the credit bureaus.*"

Division of Motor Vehicles, "Identity Theft"

(<http://www.ct.gov/dmv/cwp/view.asp?A=805&Q=305616>)

This document contains prevention tips and instructions for victims of identity theft. It directs victims that, "*If you believe you have been a victim of identity theft your first step is to contact your local law enforcement agency and file a complaint.*"

Department of Banking, "Identity Theft"

(<http://www.ct.gov/dob/cwp/view.asp?a=2235&q=297930>)

This site contains prevention tips and instructions for victims of identity theft. It instructs victims to: "*Report the crime to the police immediately. Ask the police to issue a police report. Creditors, banks, credit reporting agencies and insurance companies may require a police report to verify the crime of identity theft.*"

Legislation:

2008:

HB 5658 seeks to prevent identity theft by limiting the collection of Social Security numbers and other personal identifying information. Any person in possession of personal information of another person is required to safeguard the data, computer files and documents containing the information from misuse by third parties, and must destroy, erase or make unreadable such data, computer files and documents prior to disposal. Any person, other than the state, who collects Social Security numbers in the course of business must create a privacy protection policy which must be published or publicly displayed. The policy must: protect the confidentiality of Social Security numbers; prohibit unlawful disclosure of Social Security numbers; and limit access to Social Security numbers. Violators are subject to a civil penalty of \$500 per violation, with a

maximum of \$500,000 for any single event.

2006:

HB 5694 prohibits using a scanning device to access, read, obtain, memorize, or temporarily or permanently store information encoded on a computer chip or a payment card's magnetic strip without the authorized user's permission and with the intent to defraud the authorized user, issuer, or a merchant. It also prohibits using a reencoder to take information encoded on a computer chip or a magnetic strip and putting it onto a computer chip or the strip of a different card without the authorized user's permission and with the intent to defraud the authorized user, the card issuer, or a merchant. Violators are subject to one to ten years in prison, and a fine of up to \$10,000. Possession of a scanning device or reencoders under circumstances showing intent to violate the law is a class A misdemeanor.

2005:

Under **SB 650**, consumers in Connecticut will have the right to put a security freeze on their credit files to prevent identity thieves from opening new credit accounts in their names. A security freeze enables a consumer to prevent anyone from looking at his or her own credit reporting file for purposes of granting credit unless the consumer chooses to let that particular business look at the information. This gives consumers control over who has access to their information needed to process a credit application and effectively prevents crooks from opening new accounts in their name. When the consumer is applying for credit, the security freeze can be lifted temporarily so the application can be processed.

In addition, the bill requires businesses operating in Connecticut to notify consumers whose sensitive information has been compromised as a result of a breach in data security. This applies to all unencrypted files, media or computerized data

2003:

SB 688 increases penalties for identity theft and gives victims of the crime greater power to press charges and fix their damaged credit records. Under the bill, the new maximum penalties would be increased to 10 years in prison if more than \$5,000 is stolen and up to 20 years in prison if more than \$10,000 is stolen. Previously, a person committing identity theft could be charged with a Class D felony with a maximum penalty of five years in prison. The bill also creates a new Class D felony offense of trafficking in personal identifying information.

In addition, local police and prosecutors may take jurisdiction in reports of identity thefts, allowing prosecution in the jurisdiction of the victim. Prosecution in identity theft cases has been difficult because thieves often bounce from state to state with the stolen information. The bill also gives courts the power to order credit agencies to block poor credit reports by letting victims file police reports and affidavits with the agencies. The credit agencies would also face penalties if they do not comply.

The law also prohibits businesses who accept credit cards or debit cards from printing on a receipt provided to the cardholder more than the last five digits of the credit card or debit card account number or the expiration date of the credit card or debit card. This provision applies only to receipts that are electronically generated. Violators will be charged \$100 for the first offense,

up to \$500 for a second offense, and up to \$1000 or six months in jail for each subsequent offense. The law also prohibits the public posting or display of an individual's Social Security number, and the printing of the number on any card required for the individual to access products or services.