

NEW YORK

IDENTITY THEFT RANKING BY STATE: Rank 6, 100.1 Complaints Per 100,000
Population, 19319 Complaints (2007)
Updated January 25, 2009

Current Laws: A person is guilty of identity theft when he knowingly and with intent to defraud assumes the identity of another person by presenting himself as that other person; or by acting as that other person or by using personal identifying information of that other person, obtains goods, money, property or services or uses credit in the name of the other person or causes financial loss to that person.

If the offense causes a financial loss of over \$500, it is identity theft in the second degree, a class E felony, punishable by up to four years in jail and/or a fine of up to \$5,000 or double the amount of the defendant's gain from the commission of the crime, whichever is greater. It is also a class E felony if the person commits or attempts to commit a felony or acts as an accessory of a felony, or has been previously convicted of an identity theft crime or larceny in the last five years.

Statute: Penal Code §190.79:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.79\\$\\$@TXPEN0190.79+&LIST=LAW+&BROWSER=18966614+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.79$$@TXPEN0190.79+&LIST=LAW+&BROWSER=18966614+&TOKEN=25506506+&TARGET=VIEW)

If the defendant obtains goods, money, property or services or uses credit of another person in an amount that exceeds \$2000, or causes financial loss of that amount, it is identity theft in the first degree, a class D felony, punishable by up to seven years in jail and/or a fine of up to \$5,000 or double the amount of the defendant's gain from the commission of the crime, whichever is greater. It is also a class D felony if the defendant has previously committed the crime of identity theft in the second degree, and was previously convicted of another identity theft crime or larceny.

Statute: Penal Code §190.80:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.80\\$\\$@TXPEN0190.80+&LIST=LAW+&BROWSER=44093500+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.80$$@TXPEN0190.80+&LIST=LAW+&BROWSER=44093500+&TOKEN=25506506+&TARGET=VIEW)

A person is guilty of aggravated identity theft when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, knowing that such person is a member of the armed forces and is presently deployed outside of the continental United States and:

- Obtains goods, money, property or services or uses credit in the name of the member of the armed forces in an aggregate amount that exceeds \$500; or

- Causes financial loss to such member of the armed forces in an aggregate amount that exceeds \$500.

Aggravated identity theft is a Class D felony.

Statute: Penal Code §190.80-A:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.80-A\\$\\$@TXPEN0190.80-A+&LIST=LAW+&BROWSER=44091292+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.80-A$$@TXPEN0190.80-A+&LIST=LAW+&BROWSER=44091292+&TOKEN=25506506+&TARGET=VIEW)

All other identity theft crimes are classified as identity theft in the third degree, a class A misdemeanor, punishable by up to one year in jail and/or a fine up to \$1000.

Statute: Penal Code §190.78:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.78\\$\\$@TXPEN0190.78+&LIST=LAW+&BROWSER=17352218+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.78$$@TXPEN0190.78+&LIST=LAW+&BROWSER=17352218+&TOKEN=25506506+&TARGET=VIEW)

A person is guilty of unlawful possession of personal identification when he knowingly possesses another person's personal identifying information. If a person possesses 250 or more items of personal identification information, it is unlawful possession of personal identification information in the second degree, a class E felony, punishable by up to four years in jail and/or a fine of up to \$5,000 or double the amount of the defendant's gain from the commission of the crime, whichever is greater.

Statute: Penal Code §190.82:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.82\\$\\$@TXPEN0190.82+&LIST=LAW+&BROWSER=57837684+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.82$$@TXPEN0190.82+&LIST=LAW+&BROWSER=57837684+&TOKEN=25506506+&TARGET=VIEW)

If a person supervises more than three accomplices with the intent to commit identity theft in the second degree or has been previously convicted of identity theft crimes, unlawful possession of personal identification information, or larceny previously in the past five years, it is unlawful possession of personal identification information in the first degree, a class D felony, punishable by up to seven years in jail and/or a fine of up to \$5,000 or double the amount of the defendant's gain from the commission of the crime, whichever is greater.

It is the same crime if, with intent to further the commission of identity theft in the second degree, he or she supervises more than two accomplices, and knows that the personal whose identification information that he or she possesses is a member of the armed forces and is presently deployed overseas.

Statute: Penal Code §190.83:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.83\\$\\$@TXPEN0190.83+&LIST=LAW+&BROWSER=05654320+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.83$$@TXPEN0190.83+&LIST=LAW+&BROWSER=05654320+&TOKEN=25506506+&TARGET=VIEW)

All other violations are unlawful possession of personal identification information in the third degree, a class A misdemeanor, punishable by up to one year in jail and/or a fine up to \$1000.

Statute: Penal Code §190.81:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.81\\$\\$@TXPEN0190.81+&LIST=LAW+&BROWSER=05654320+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.81$$@TXPEN0190.81+&LIST=LAW+&BROWSER=05654320+&TOKEN=25506506+&TARGET=VIEW)

[EN190.81\\$\\$@TXPEN0190.81+&LIST=LAW+&BROWSER=35249888+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.81$$@TXPEN0190.81+&LIST=LAW+&BROWSER=35249888+&TOKEN=25506506+&TARGET=VIEW)

These crimes do not apply to people under 21 years old who used or possessed the personal identifying identification of another solely for the purpose of purchasing alcohol, to people under 18 who used the identification to purchase tobacco, or any person who uses the information of another person solely for the purpose of misrepresenting his/her age to gain access to a place in which access is restricted by age.

Statute: Penal Code §190.84:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.84\\$\\$@TXPEN0190.84+&LIST=LAW+&BROWSER=11674220+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.84$$@TXPEN0190.84+&LIST=LAW+&BROWSER=11674220+&TOKEN=25506506+&TARGET=VIEW)

“Personal identifying information” is defined as a person’s name, address, telephone number, date of birth, driver's license number, Social Security number, place of employment, mother’s maiden name, banking account numbers, credit or debit card numbers, computer system password, signature or copy of a signature, electronic signature, unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person, telephone calling card number, mobile identification number or code, electronic serial number or personal identification number, or any other name, number, code or information that may be used alone or in conjunction with other such information to assume the identity of another person.

Statute: Penal Code §190.77:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.77\\$\\$@TXPEN0190.77+&LIST=LAW+&BROWSER=45880419+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.77$$@TXPEN0190.77+&LIST=LAW+&BROWSER=45880419+&TOKEN=25506506+&TARGET=VIEW)

Jurisdiction: Identity theft crimes may be prosecuted in any county where the crime occurred, even if the defendant was never in that county, or in the county where the victim resided when the crime was committed, or the county in which the person whose identity was used for a crime resided at the time of the offense.

Statute: Criminal Procedure Law §20.40(1):

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$CPL20.40\\$\\$@TXCPL020.40+&LIST=LAW+&BROWSER=07868300+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$CPL20.40$$@TXCPL020.40+&LIST=LAW+&BROWSER=07868300+&TOKEN=25506506+&TARGET=VIEW)

Payment Cards: A person is guilty of unlawful use of credit card, debit card or public benefit card when in the course of obtaining or attempting to obtain property or a service, he uses or displays a credit card, debit card or public benefit card which he knows to be revoked or cancelled. Violations are a class A misdemeanor.

Statute: Penal Code §165.17:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN165.17\\$\\$@TXPEN0165.17+&LIST=LAW+&BROWSER=40968761+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN165.17$$@TXPEN0165.17+&LIST=LAW+&BROWSER=40968761+&TOKEN=25506506+&TARGET=VIEW)

Credit or debit card theft is grand larceny in the fourth degree, a class E felony.

Statute: Penal Code §155.30:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN155.30\\$\\$@TXPEN0155.30+&LIST=LAW+&BROWSER=26310494+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN155.30$$@TXPEN0155.30+&LIST=LAW+&BROWSER=26310494+&TOKEN=25506506+&TARGET=VIEW)

A person is guilty of criminal possession of stolen property in the fourth degree, a class E felony, when he knowingly possesses stolen property, with intent to benefit himself or a person other than an owner thereof or to impede the recovery by an owner thereof, and when the property consists of a credit card, debit card or public benefit card.

Statute: Penal Code §165.45:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN165.45\\$\\$@TXPEN0165.45+&LIST=LAW+&BROWSER=04320664+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN165.45$$@TXPEN0165.45+&LIST=LAW+&BROWSER=04320664+&TOKEN=25506506+&TARGET=VIEW)

Phishing: State law prohibits phishing scams, in which identity thieves try to trick consumers out of personal information by sending fraudulent e-mails that appear to come from banks or other trusted businesses and are used to induce recipients to verify their accounts by typing personal details, such as credit card or bank account information, into a Web site disguised to appear legitimate. The bill specifically prohibits a person from using a Web page, e-mail message, or otherwise use the Internet, to solicit, request, or take action to induce another person to provide identifying information by representing himself, either directly or by implication, to be a business, with the intent to defraud and without the consent of the business. The attorney general, Internet service providers, or a person who owns a Web site or trademark that has been adversely affected may bring an action to stop further violations, and recover the greater of actual damages or \$1,000 for each separate violation. If the court determines there is a pattern of violations, damages can be trebled.

Statute: General Business Law §390-B:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$GBS390-B\\$\\$@TXGBS0390-B+&LIST=LAW+&BROWSER=00383915+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$GBS390-B$$@TXGBS0390-B+&LIST=LAW+&BROWSER=00383915+&TOKEN=25506506+&TARGET=VIEW)

Social Security Numbers: State law places limits on the use and dissemination of Social Security numbers (SSNs). The law will prohibit the intentional communication of an individual's SSN to the general public, and restrict the ability of businesses to print SSNs on a mailing or on any card or tag required to access products, services, or benefits. It will also:

- Prohibit requiring an individual to transmit his SSN over the Internet unless the connection with the Internet is secure or the number is encrypted.
- Prohibit requiring an individual's SSN for access to an Internet website, unless a password or unique personal identification number or other authentication device is also required for access.
- Require businesses that possess SSNs to implement appropriate safeguards and limit unnecessary employee access to the information.
- Encode or embed a SSN in or on a card or document, including but not limited to a bar code, chip, magnetic strip, or other technology, in place of removing the SSN as restricted by this section.

No person may file any document available for public inspection with any state agency, political subdivision, or in any court of this state that contains a Social Security number of any other person, unless the person is a dependent child or has consented to the filing.

Statute: General Business Law §399-DD:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$\\$GBS399-DD*4\\$\\$@TXGBS0399-DD*4+&LIST=LAW+&BROWSER=05271075+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$GBS399-DD*4$$@TXGBS0399-DD*4+&LIST=LAW+&BROWSER=05271075+&TOKEN=25506506+&TARGET=VIEW)

Beginning January 1, 2010, the state and its political subdivisions may not do any of the following, unless required by law:

- Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual's Social Security number.
- Print an individual's Social Security number on any card or tag required for the individual to access products, services or benefits provided by the state and its political subdivisions.
- Require an individual to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted.
- Require an individual to use his or her Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the website.
- Include an individual's Social Security number, except the last four digits, on any materials that are mailed to the individual, or in any electronic mail that is copied to third parties, unless state or federal law requires the Social Security number to be on the document to be mailed. Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the Social Security number. A Social Security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.
- Encode or embed a Social Security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the Social Security number as required by this section.

The law does not prohibit a county clerk or clerk from making available a document publicly recorded or filed prior to the effective date of this section. However, if any individual request redaction of a Social Security number from a publicly recorded document available to the public online, the number must be promptly redacted by the county clerk.

Statute: Public Officers 96A:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$\\$PBO96-A\\$\\$@TXPBO096-A+&LIST=LAW+&BROWSER=24265377+&TOKEN=48825368+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$PBO96-A$$@TXPBO096-A+&LIST=LAW+&BROWSER=24265377+&TOKEN=48825368+&TARGET=VIEW)

Unless otherwise required by law, an employer is prohibited from:

- Publicly post or display an employee's Social Security number;
- Visibly print a Social Security number on any identification badge or card, including any time card; or
- Place a Social Security number in files with unrestricted access; or

- Communicate an employee's personal identifying information to the general public. Personal identifying information includes a Social Security number, home address or telephone number, personal e-mail address, Internet identification name or password, parent's surname prior to marriage; or driver's license number.
- Use a Social Security number for an identification number for purposes of any occupational licensing.

Violations may be punished by a civil penalty of up to \$500 on any employer for any knowing violation. It is presumptive evidence that a violation was knowing if the employer had not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions.

Statute: Labor: 203-d:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$\\$LAB203-D\\$\\$@TXLAB0203-D+&LIST=LAW+&BROWSER=26726378+&TOKEN=48825368+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$LAB203-D$$@TXLAB0203-D+&LIST=LAW+&BROWSER=26726378+&TOKEN=48825368+&TARGET=VIEW)

Disposal of Customer Records: To prevent identity theft, state law restricts how businesses can dispose of paper records with personal identifying information about individuals. The law prohibits businesses from knowingly discarding paper records or documents with sensitive personal identifying data without first redacting the data or shredding or otherwise destroying the documents. The law defines personal identifying information as any personal information in combination with any of the following data elements: Social Security number, driver's license number, mother's maiden name, financial services account number, or ATM number or code. The attorney general may seek an injunction to stop violations. It is not necessary to prove that any person has been injured by the violation. Violations may be punishable by a civil fine of up to \$5000 per violation.

Statute: General Business Law §399-H:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$\\$GBS399-H\\$\\$@TXGBS0399-H+&LIST=LAW+&BROWSER=53599996+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$GBS399-H$$@TXGBS0399-H+&LIST=LAW+&BROWSER=53599996+&TOKEN=25506506+&TARGET=VIEW)

Scanning Devices: State law prohibits the unlawful possession of a skimmer device when the violator has the intent that the device be used in furtherance of the commission of the crime of identity theft or unlawful possession of personal identification information. A skimmer device is defined as a "device designed or adapted to obtain personal identifying information from a credit card, debit card, public benefit card, access card or device, or other card or device that contains personal identifying information. Unlawful possession of a skimmer device in the second degree is a class A misdemeanor.

Statute: Penal Code: §190.85:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$\\$PEN190.85\\$\\$@TXPEN0190.85+&LIST=LAW+&BROWSER=23498203+&TOKEN=48825368+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$PEN190.85$$@TXPEN0190.85+&LIST=LAW+&BROWSER=23498203+&TOKEN=48825368+&TARGET=VIEW)

A person is guilty of unlawful possession of a skimmer device in the first degree, a class E felony, if he or she has already been convicted within the last five years of identity theft, unlawful possession of a personal identification information, or unlawful possession of a skimmer device.

Statute: Penal Code: §190.86:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN190.86\\$\\$@TXPEN0190.86+&LIST=LAW+&BROWSER=35763734+&TOKEN=48825368+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN190.86$$@TXPEN0190.86+&LIST=LAW+&BROWSER=35763734+&TOKEN=48825368+&TARGET=VIEW)

Victim Assistance:

Mandatory Police Reports: Any individual whose identity was assumed; whose personal identifying information was used fraudulently; who has suffered a financial loss as a direct result of identity theft crimes; or has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another may make a complaint to the local law enforcement agency of the county in which any part of the offense took place, regardless of whether the defendant was actually present in the county, or in the county in which victim resided. The law enforcement agency must take a police report of the matter and provide the complainant with a copy of the report at no charge.

Statute: Executive Law: §646:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$EXEC646\\$\\$@TXEXEC0646+&LIST=LAW+&BROWSER=42807557+&TOKEN=48825368+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$EXEC646$$@TXEXEC0646+&LIST=LAW+&BROWSER=42807557+&TOKEN=48825368+&TARGET=VIEW)

Restitution: State law allows for a court to order restitution to a person who has suffered out-of-pocket losses as a result of an identity theft crime, including losses that a person incurs when his credit rating is affected, and allows a consumer to bring a civil action against the perpetrator of the crime to recover for the damages done to his credit ratings. Restitution includes the actual loss incurred by the victim, including an amount equal to the value of the time reasonably spent by the victim attempting to remediate the harm incurred by the victim from the offense, and the consequential financial losses.

Statute: Penal Law §60.27:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$PEN60.27\\$\\$@TXPEN060.27+&LIST=SEA69+&BROWSER=19715252+&TOKEN=02964829+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$PEN60.27$$@TXPEN060.27+&LIST=SEA69+&BROWSER=19715252+&TOKEN=02964829+&TARGET=VIEW)

Security Freeze: State law allows all consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts 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. A consumer may request a freeze by mail with delivery confirmation, or via telephone, secure electronic means, or other methods developed by the consumer credit reporting agencies. The agencies must have a secure website and a separately dedicated toll-free number to offer information, to process requests, and deliver the services provided under this section.

The credit reporting agencies are permitted to charge a fee of \$5 for each placing, removing or temporary lifting of a security freeze. However, freezes are free for victims of identity theft who provide a valid copy of a police report or an FTC ID Theft Affidavit or victims of domestic violence who provide a valid domestic violence incident report form, an order of protection, a police report, or a signed affidavit from specific legal or medical authorities.

The reporting agency must place the freeze within three business days after receiving the request, and within five business days of placing the freeze must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time. After January 1, 2010, security freezes must be placed within one business day. Requests for a temporary unlocking of the freeze must be completed within three business days. However, after September 1, 2009, the unlocking must take place within 15 minutes if the request is received by telephone or secure electronic method.

Statute: General Business Law §380-t:

<http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=%%GBS380-T%%@TXGBS0380-T+&LIST=SEA49+&BROWSER=21450037+&TOKEN=38019186+&TARGET=VIEW>

Office of the Attorney General, “Placing a Security Freeze on Your Credit File”:

http://www.oag.state.ny.us/bureaus/consumer_frauds/pdfs/security_freeze.pdf

“How to Place A Security Freeze in New York”:

<http://www.consumersunion.org/pdf/security/securityNY.pdf>

Security Breach: State law requires state government agencies and businesses operating in the state to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. It applies to any state agency or business that owns or licenses a computerized database that includes personal information to disclose any breach of security of such a system to any resident of the state whose unencrypted personal information may have been acquired by an authorized person. A security breach is defined as an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of private information. Private information includes any personal information with any one or more of the following data elements: Social Security number, driver’s license number, account number, or credit or debit card in combination with any required security card.

The law requires notification in the most expedient time possible consistent with legitimate needs of law enforcement agencies. It can be provided to the affected persons by mail, e-mail, or telephone. If the cost of providing regular notice would exceed \$250,000, the amount of people to be notified exceeds 500,000, or the entity or business not have sufficient contact information, 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 entity’s web site, and notification to statewide media. If more than 5,000 residents are to be notified, consumer reporting agencies must also be notified. In addition, notice must be provided to the Attorney General’s office, the Consumer Protection Board, and the New York State Office of Cyber Security and Critical Infrastructure Coordination.

Statute: State Technology Law § Article 2:201-208:

<http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=@SLST0A2+&LIST=LAW+&BROWSER=39131754+&TOKEN=02964829+&TARGET=VIEW>

“NY State Security Breach Law”

http://www.consumer.state.ny.us/pdf/security_breach_tip_card.pdf

“A Security Checklist: Surviving a Data Breach”

(http://www.consumer.state.ny.us/pdf/a_data_check_list.pdf)

Prohibition Against Debt Collectors: State law requires a creditor to cease collection activities when notified that the debtor is a victim of identity theft. The victim must provide a copy of a valid police report and a written statement that the specific debt being collected is a result of the identity theft, in addition to supporting documents.

Statute: General Business Law §29-HH:

<http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=@PLGBS0A29->

[HH+&LIST=SEA2+&BROWSER=13861536+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=@PLGBS0A29-HH+&LIST=SEA2+&BROWSER=13861536+&TOKEN=25506506+&TARGET=VIEW)

Prohibition Against Discrimination in Extending Credit: State law provides that credit issuers may not deny credit, reduce the credit limit, or raise the cost of credit to someone simply because he or she has been a victim of identity theft, as long as the victim has filed a criminal complaint of the theft.

Statute: General Business Law §399-E:

[http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=\\$\\$GBS399-E*2\\$\\$@TXGBS0399-](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$GBS399-E*2$$@TXGBS0399-)

[E*2+&LIST=LAW+&BROWSER=42694599+&TOKEN=25506506+&TARGET=VIEW](http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$GBS399-E*2$$@TXGBS0399-E*2+&LIST=LAW+&BROWSER=42694599+&TOKEN=25506506+&TARGET=VIEW)

State Resources:

Office of the Attorney General, “Identity Theft Pamphlet”

(http://www.oag.state.ny.us/bureaus/consumer_frauds/pdfs/identity_theft_pamphlet.pdf)

This comprehensive document includes information on how to prevent identity theft and what to do if you become a victim of the crime. It directs victims to: “*Report any fraudulent activity to the appropriate police or sheriff’s department with jurisdiction in your area. Give them as much documented evidence as possible.*”

“Identity Theft: What to Do If You Have Been Victimized”

(http://www.oag.state.ny.us/bureaus/consumer_frauds/tips/id_theft_victim.html)

This site provides victims of identity theft with a list of actions that should be taken, including: “*Report any fraudulent activity to the appropriate police and sheriff departments with jurisdiction in your area. Be sure to keep a copy of the police report because financial institutions often require verification that there was a purported crime before they will continue an investigation.*”

New York State Consumer Protection Board, “Identity Theft, Information Privacy, and Internet Security”

(http://www.consumer.state.ny.us/internet_security.htm)

This site has numerous publications related to identity theft:

- “A Consumer Guide to Preventing and Responding to Identity Theft”
(http://www.consumer.state.ny.us/pdf/id_theft_online_version.pdf)

This pamphlet gives advice on preventing identity theft, and provides a list of things that identity theft victims should do. It directs victims to: *“File a report with the police department. Identity theft and fraud are felonies punishable by law. Keep a copy of the police report to provide to credit card companies, banks and credit reporting agencies as proof that a crime was committed. Submitting a police report can block reporting of fraudulent data on your credit report.”*

- “Tips on Preventing Identity Theft”
(http://www.consumer.state.ny.us/pdf/id_theft_tip_sheet.pdf)
- “A Security Check List: Surviving a Data Breach”
(http://www.consumer.state.ny.us/pdf/a_data_check_list.pdf)
This document provides a list of steps to take and questions to ask when personal information is lost or stolen from a company's computer system.
- “Social Security Number and Identity Theft”
(http://www.consumer.state.ny.us/pdf/ss_id_theft_brochure.pdf)
- “Back to School Basics: Keeping Your Child’s Identity Theft”
(http://www.consumer.state.ny.us/pdf/btsb_child_identity_theft.pdf)
- “Identity Theft Mitigation at a Glance”
(http://www.consumer.state.ny.us/pdf/id_theft_mitigation_at_a_glance)
- “Identity Theft and Domestic Violence”
(http://www.consumer.state.ny.us/pdf/dv_id_theft_brochure_2008.pdf)

•
Division of State Police, “Crime Prevention: Identity Theft”
(https://www.troopers.state.ny.us/Crime_Prevention/Online_Safety/Identity_Theft)

This document directs victims to: *“File a police report. Get a copy of the report to submit to your creditors and others who may require proof of the crime.”*

Banking Department, “Identity Theft: What You Need To Know”
(<http://www.banking.state.ny.us/brid.htm>)

If you are a victim of identity theft, *“File a police report at your local precinct; get your complaint number or a copy of your report.”*

Legislation:

2008:

The Legislature passed comprehensive anti-identity theft legislation (**SB 1836**). The bill:

- Allows New Yorkers to place security freezes on their credit either by phone or over the Internet with the appropriate credit agency. Previously, credit freezes could only be requested by certified mail.
- Beginning January 1, 2010, requires credit reporting agencies to place a security freeze on an individual’s credit report within 24 hours of receiving notice.
- Beginning September 1, 2009, requires credit bureaus to “thaw” or remove the credit freeze temporarily within 15 minutes of receipt of the request.
- Creates the Identity Theft Prevention and Mitigation Program to be administered by the Consumer Protection Board to assist identity theft victims in undoing the damage that the identity thief has done to their financial and credit history.

- Prohibits employers from posting or displaying an employee's Social Security number, or placing Social Security numbers in files with open access.
- Makes it illegal to possess a skimmer device, which can obtain personal identifying information from credit or debit cards.
- Allows victims of identity theft to sue for restitution equal to the amount of time spent undoing the damage.

Under **AB 8634**, credit bureaus may charge for security freezes victims of identity theft who provide a valid copy of a police report or an FTC ID Theft Affidavit or victims of domestic violence who provide either a valid domestic violence incident report form, an order of protection, a police report, or a signed affidavit from specific legal or medical authorities.

SB 7297 requires a creditor to cease collection activities when notified that the debtor is a victim of identity theft. The victim must provide a copy of a valid police report and a written statement that the specific debt being collected is a result of the identity theft, in addition to supporting documents.

SB 7892 provides that credit issuers may not deny credit, reduce the credit limit, or raise the cost of credit to someone simply because he or she has been a victim of identity theft, as long as the victim has filed a criminal complaint of the theft.

SB 1829 enhances criminal penalties for identity theft when the perpetrator knows that the victim is serving overseas in the armed forces.

2007:

Under **SB 5541**, any individual whose identity was assumed; whose personal identifying information was used fraudulently; who has suffered a financial loss as a direct result of identity theft crimes; or has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another may make a complaint to the local law enforcement agency of the county in which any part of the offense took place, regardless of whether the defendant was actually present in the county, or in the county in which victim resided. The law enforcement agency must take a police report of the matter and provide the complainant with a copy of the report at no charge.

2006:

AB 8025 targets phishing scams, in which identity thieves try to trick consumers out of personal information by sending fraudulent e-mails that appear to come from banks or other trusted businesses and are used to induce recipients to verify their accounts by typing personal details, such as credit card or bank account information, into a Web site disguised to appear legitimate. The bill specifically prohibits a person from using a Web page, e-mail message, or otherwise use the Internet, to solicit, request, or take action to induce another person to provide identifying information by representing himself, either directly or by implication, to be a business, with the intent to defraud and without the consent of the business. The attorney general, Internet service providers, or a person who owns a Web site or trademark that has been adversely affected may bring an action to stop further violations, and recover the greater of actual damages or \$1,000 for

each separate violation. If the court determines there is a pattern of violations, damages can be trebled.

AB 7349 allows all state residents to place a security freeze on their credit reports to prevent an identity thief from opening an account or obtaining credit under their name. To obtain a freeze, residents must request one in writing from the three consumer reporting agencies. Consumers who place a security freeze will be provided a password to give to credit reporting agencies each time they want to allow temporary access to their credit information.

AB 8456 requires companies to take preventative measures to combat identity theft in handling customers' personal information. The bill requires companies to properly shred or destroy any records containing customers' personal information before they throw it away. Violators will be subject to a civil penalty of up to \$5000.

SB 6909 places limits on the use and dissemination of Social Security numbers (SSNs). Specifically, the bill:

- Prohibits the intentional communication of an individual's SSN to the general public.
- Restricts businesses' ability to print an individual's SSN on mailings or on any card or tag required to access products, services, or benefits.
- Prohibits businesses from requiring an individual to transmit his or her encrypted SSN over the Internet.
- Requires businesses that possess SSNs to implement appropriate safeguards and limit unnecessary employee access to SSNs.

2005:

AB 4254 requires state government agencies and businesses operating in the state to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. It applies to any state agency or business which owns or licenses a computerized database that includes personal information to disclose any breach of security of such a system to any resident of the state whose unencrypted personal information may have been acquired by an authorized person. A security breach is defined as an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of private information. Private information includes any personal information with any one or more of the following data elements: Social Security number, driver's license number, account number, or credit or debit card in combination with any required security card.

The law requires notification in the most expedient time possible consistent with legitimate needs of law enforcement agencies. It can be provided to the affected persons by mail, e-mail, or telephone. If the cost of providing regular notice would exceed \$250,000, the amount of people to be notified exceeds 500,000, or the entity or business not have sufficient contact information, 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 entity's web site, and notification to statewide media. If more than 5,000 residents are to be notified, consumer reporting agencies must also be notified. In addition, notice must be provided to the Attorney General's office, the Consumer Protection Board, and the New York State Office of Cyber Security and Critical Infrastructure Coordination.

Under the bill, the Attorney General may seek injunctive relief against any business entity for violation of the law. The court may award damages to consumers for actual costs or losses incurred by a person entitled to notice, including consequential financial losses. If the court finds the business violated the law knowingly or recklessly, the court may also impose a civil penalty of the greater of \$5000 or up to \$10 per instance of failed notification, up to \$150,000.

2003:

AB 5150 prohibits businesses from printing charge, credit, or debit card numbers on receipts that are electronically created.

2002:

AB 4939 criminalizes identity theft, making New York the 49th state to pass such a law. The bill creates three levels of identity theft, from misdemeanors to felonies, and sets a maximum prison sentence of seven years for the most serious offense. The highest sentencing can go to criminals who use people's stolen identities to buy more than \$2,000 worth of services or goods. In addition, the bill contains provisions for restitution for victims. Judges are allowed to order convicted thieves to repay their victims, who can also sue in civil court for damages done to their credit ratings.

To prevent identity theft, **AB 5972 / SB 4697** provides enhanced security for debit card transactions by regulating these transactions in the same manner as credit card purchases. Existing law prohibits printing the last four digits of credit card numbers only. The new law will provide the same security to debit card users.