

ILLINOIS

IDENTITY THEFT RANKING BY STATE: Rank 11, 80.2 Complaints Per 100,000
Population, 10304 Complaints (2007)
Updated November 30, 2008

Current Laws: A person commits the offense of identity theft when he or she knowingly uses any personal identifying information or personal identification document of another person to fraudulently obtain credit, money, goods, services, or other property. Penalties for identity theft depend on the value of the theft.

If the value of the credit, money, goods, services, or other property is less than \$300, the crime is a Class 4 felony, punishable by one to three years in prison and a fine up to \$25,000. Subsequent offenses are upgraded to a Class 3 felony, punishable by two to five years in prison, as is the penalty for people who have previously been convicted of certain crimes, including burglary, theft, or fraud. If the amount is between \$300 and \$2000, it is a Class 3 felony; between \$2000 and \$10,000 is a Class 2 felony (punishable by two to seven years in prison); between \$10,000 and \$100,000 is a Class 1 felony (punishable by four to fifteen years in prison); and over \$100,000 is a Class X felony (punishable by six to thirty years in prison).

Penalties are increased one step (with the exception of a Class X felony) if the victim of the offense is an active duty member of the Armed Services or Reserve Forces of the United States or of the Illinois National Guard serving in a foreign country.

It is also identity theft if a person:

- Uses any personal identification information or document of another with intent to commit any felony theft or other felony violation of state law;
- Obtains, records, possesses, sells, transfers, purchases, or manufactures any personal identification information or document of another with intent to commit or to aid or abet another in committing any felony theft or other felony violation of state law;
- Uses, obtains, records, possesses, sells, transfers, purchases, or manufactures any personal identification information or document of another knowing that it was stolen or produced without lawful authority;
- Uses, transfers, or possesses document-making implements to produce false identification or false documents with knowledge that they will be used by the person or another to commit any felony theft or other felony violation of state law;
- Uses any personal identification information or document to portray himself as that person to gain access to information or documents of that person, without consent; or
- Uses personal identifying information or document of another in order to gain access to the record of the actions taken, communications made or received, or other activities or transactions of that person, without consent.

“Personal identifying information” means any of the following information: a person’s name; address; date of birth; telephone number; driver’s license or state identification card number; Social Security number; employer or employment number; maiden name of a person’s mother; number assigned to a person’s depository account, savings account, or brokerage account; number assigned to a person’s credit or debit card; personal identification numbers (PIN); electronic identification numbers; digital signals; user names, passwords, or other words or characters used to access information relating to an individual, or to actions taken, communications received or made, or other activities; any other numbers or information that could be used to access a person’s financial resources, to identify a specific individual.

“Personal identifying document” means a birth certificate, driver’s license, state identification card, employment identification card, Social Security card, firearm owner’s identification card, credit or debit card, or a passport. It also includes any document made or issued, or falsely purported to have been made or issued, by the federal, state, or any local government body that is intended for the purpose of identification of an individual.

Violations are a Class 3 felony, with a repeat or subsequent offense upgraded to a Class 2 felony. It is also a Class 2 felony if the offense includes the identifiers of or other information relating to three or more separate individuals.

In addition, if the person used any personal identification information or document of another person to purchase methamphetamine manufacturing material, it will be a Class 2 felony, and a Class 1 felony for a second or subsequent offense.

Statute: §720 ILCS 5/16G-15:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-15>

Aggravated identity theft occurs when a person commits the offense of identity theft against a person 60 years or older; against a disabled person; or in furtherance of the activities of an organized gang. Violations are a Class 3 felony if the identity theft of credit, money, goods, services or other property is under \$300; a Class 2 felony if between \$300 and \$10,000; a Class 1 felony if between \$10,000 and \$100,000; and a Class X felony if it exceeds \$100,000.

Subsequent convictions for aggravated identity theft regardless of the value of the property involved is a Class X felony.

Statute: §720 ILCS 5/16G-20:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-20>

A person commits the offense of facilitating identity theft when he or she, in the course of his or her employment or official duties, has access to the personal information of another person in the possession of the State of Illinois, whether written, recorded, or on computer disk and knowingly, with the intent of committing identity theft, aggravated identity theft, or any violation of the Illinois Financial Crime Law, disposes of that written, recorded, or computerized information in any receptacle, trash can, or other container that the public could gain access to, without shredding that information, destroying the recording, or wiping the computer disk so that the information is either unintelligible or destroyed. Violations are a Class A misdemeanor, punishable by up to one year in prison, for a first offense and a Class 4 felony for a second or subsequent offense.

Statute: § 720 ILCS 5/16G-13:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-13>

Jurisdiction: State law allows for an identity theft prosecution to occur in either the county where the theft occurred, the county where the information was illegally used, or where the victim resides.

Statute: 720 ILCS 5/16G-35:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-35>

Identification Cards: It is a Class 4 felony for any person to knowingly possess, display, or cause to be displayed any fraudulent or unlawfully altered identification card. The penalty increases to a Class 3 felony and a Class 2 felony for subsequent offense if the person does so to:

- Obtain any account, credit, credit or debit card from a bank, financial institution, or retailer;
- With the intent to commit a theft, deception, or credit or debit card fraud; or
- With the intent to commit any other violation of any law for which a sentence of one year imprisonment is imposed;
- Do so with the unauthorized possession of any document, instrument or device capable of defrauding another; or
- Do so with the intent to use the identification card to acquire any other identification document.

State law also prohibits knowingly possessing without authority any identification card making implement; the duplication, manufacture, sale, or transfer of any fraudulent identification card; or the advertisement or distribution of any information or materials that promote the selling, giving, or furnishing of a fraudulent identification card.

Statute: §15 ILCS 335/14B:

<http://www.ilga.gov/legislation/ilcs/documents/001503350K14B.htm>

<http://www.ilga.gov/legislation/ilcs/documents/001503350K14D.htm> **Payment Cards:** It is a Class 4 felony 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, address, or employment for the purpose of procuring the issuance of a credit or debit card.

Statute: §720 ILCS 250/3: <http://www.ilga.gov/legislation/ilcs/documents/072002500K3.htm>

A person who receives a credit card or debit card from the person, possession, custody or control of another without the cardholder's consent; or who with knowledge that it has been so acquired, receives the credit or debit card with intent to use, sell, or transfer it to another person other than the issuer or cardholder is guilty of a Class 4 felony. A person with two or more such credit or debit cards each issued to different cardholders other than himself is presumed to have committed this offense. If a person, in any 12-month period, commits this offense with respect to three or more credit or debit cards issued to different cardholders is guilty of a Class 3 felony.

Statute: §720 ILCS 250/4: <http://www.ilga.gov/legislation/ilcs/documents/072002500K4.htm>

It is a Class 4 felony for a person to receive a credit or debit card that he knows to have been lost or mislaid and who retains possession with intent to use, sell, or transfer it to a person other than the issuer or cardholder. The penalty increases to a Class 3 felony if, in a single transaction, a

person violates this law with three or more credit or debit cards issued to cardholders other than himself.

Statute: §720 ILCS 250/5: <http://www.ilga.gov/legislation/ilcs/documents/072002500K5.htm>

It is a Class 4 felony for a person other than the issuer to sell a credit or debit card, without the consent of the issuer; or for a person to purchase a credit or debit card from a person other than the issuer, without consent. It is a Class 3 felony if, in a single transaction, a person violates this law with three or more credit or debit cards issued to cardholders other than himself.

Statute: §720 ILCS 250/6: <http://www.ilga.gov/legislation/ilcs/documents/072002500K6.htm>

It is unlawful for a person, who with intent to defraud either the issuer, a person providing money, goods, property, services, or anything else of value, or any person, uses for the purpose of obtaining money, goods, property, services, or anything else of value, a credit or debit card obtained or retained fraudulently or without the cardholder's consent, or a card that he knows is counterfeit, forged, expired, or revoked. It is a Class 4 felony if the value of all money, goods, property, services, or other things of value obtained or sought does not exceed \$300 in a six-month period, and a Class 3 felony if it exceeds that amount.

Statute: §720 ILCS 250/8: <http://www.ilga.gov/legislation/ilcs/documents/072002500K8.htm>

A person who receives money, goods, property, services or anything else of value obtained fraudulently, knowing that it was so obtained, is guilty of a Class A misdemeanor if the value does not exceed \$150 in any six-month period, and a Class 4 felony if it exceeds that amount.

Statute: §720 ILCS 250/13: <http://www.ilga.gov/legislation/ilcs/documents/072002500K13.htm>

It is a Class A misdemeanor for any person, other than the cardholder or a person authorized by him, who with intent to defraud, signs a credit or debit card.

Statute: §720 ILCS 250/14: <http://www.ilga.gov/legislation/ilcs/documents/072002500K14.htm>

A person who is not party to a transaction that involves the use of a financial transaction device, such as a credit or debit card, may not secretly or surreptitiously photograph or otherwise capture or record, either electronically or by any other means, or distribute, disseminate, or transmit personal identifying information from the transaction without the consent of the person whose information is photographed or otherwise captured, recorded, distributed, disseminated, or transmitted. Violations are a Class A misdemeanor.

Statute: §720 ILCS 5/16G-14:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-14>

Phishing: State law prohibits phishing, the act of posing as a legitimate company or government agency in an email, Web page, or other Internet communication in order to trick a recipient into revealing his or her personal information. It will be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing himself, herself, or itself to be a business without the authority or approval of the business. A person who is engaged in the business or providing Internet access service to the public, owns a Web page, or owns a trademark and is adversely affected by a phishing violation will be allowed to bring an action against the violator to recover the greater of actual damages or \$500,000. Individual

victims may bring an action to seek greater of three times the amount of actual damages or \$5,000 per violation.

Statute: §740 ILCS / 7:

<http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2921&ChapAct=740%26nbsp%3BILCS%26nbsp%3B7%2F&ChapterID=57&ChapterName=CIVIL+LIABILITIES&ActName=Anti%2DPhishing+Act%2E>

Biometric Information: State law provides for guidelines for the collection and storage of biometric data and the rights of those whose data is collected. Under state law, public agencies and private entities must inform a person in writing and to receive that person’s consent before collecting biometric information.

“Biometric identifier” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. “Biometric information” means any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

State law requires private entities in the possession of biometric identifiers or information to:

- Develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for the collecting or obtaining such identifiers or information has been satisfied or within three years of the individual’s last interaction with the private entity, whichever occurs first.
- Before collecting or otherwise obtain a person’s biometric identifier or information, the entity must first inform the subject in writing that the information is being collected or stored; the length of term for which the information will be stored and used; and obtain written release from the subject.
- Store, transmit, and protect from disclosure all biometric identifiers using the reasonable standard of care within the entity’s industry, and in a manner that is the same as or more protective than the manner in which the private entity stores and protects other confidential and sensitive information.

The law also:

- Prohibits the selling, leasing, trading, or otherwise profiting from a person’s biometric information.
- Prohibits the disclosure of biometric information unless the customer consents; the disclosure completes a financial transaction requested or authorized by the customer; the disclosure is required by state or federal law; or is required pursuant to a valid warrant or subpoena.

In addition, the new law requires all public agencies and private entities collecting biometric identifiers or information to establish a retention and destruction schedule. Under this schedule biometric identifiers or information must be destroyed after the initial purpose of collecting or

obtaining the information has been fulfilled or within 3 years of the individual's last interaction with the agency or entity. It provides certain exemptions for public agencies, especially law enforcement and prosecuting agencies and entities issuing driver's licenses and permits.

Text of Legislation: <http://www.ilga.gov/legislation/publicacts/95/095-0994.htm>

Victim Assistance:

Mandatory Police Reports: Law enforcement agencies are required to accept and provide police reports to identity theft victims. After being contacted by a victim of identity theft, law enforcement agencies must take a police report of the matter, provide the victim with a copy of the report, and begin an investigation of the facts. If the suspected crime was committed in a different jurisdiction, the agency may refer the matter to the agency where the suspected crime was committed for an investigation of the facts.

Statute: §720 ILCS 5/16G-30:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-30>

Civil Suits: A person who is convicted of facilitating identity theft, identity theft, or aggravated identity theft is liable in a civil action to the person who suffered damages as a result of the violation. The person suffering damages may recover court costs, attorney's fees, lost wages and actual damages.

Statute: §720 ILCS 5/16G-20:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-21>

Criminal Identity Theft: State law allows a person who reasonably believes he is the victim of identity theft to petition a court for a factual declaration of innocence. It seeks to assist victims of criminal identity theft, in which the perpetrator of the theft was arrested for, cited for, or convicted of a crime under the victim's identity; where a criminal complaint has been filed against the perpetrator in the victim's name; or where the victim's identity has been mistakenly associated with a record of criminal conviction. After a court has issued a declaration of factual innocence, the court may order the name and associated personal identifying information contained in court records, files and indexes accessible by the public be deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity

Statute: §720 ILCS 5/16G-30:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072000050K16G-30>

Prohibition Against Debt Collectors: State law requires debt collectors to cease collection activities of a debt when an alleged debtor provides a police report of identity theft and other proof of his status as an identity theft victim. The debt collector must review and consider the information provided by the alleged victim and may only recommence debt collection activities only after making a good faith determination that the information does not establish that the information does not establish that the debtor is not responsible for the specific debt in question. The debtor must be notified of this determination. Debt collectors who cease collection activities are required to notify the creditors and consumer credit reporting agencies to which the collector previously provided adverse information.

Statute: § 225 ILCS 425/1:

<http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=1355&ChapAct=225%26nbsp%3BILCS%>

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. To request a freeze, a consumer must request one in writing to the credit reporting agencies. The credit reporting agency may charge up to \$10 to place, remove, or temporarily lift a security freeze. Senior citizens 65 years or older will not be charged to place or permanently lift the security freeze, but may be charged up to \$10 for each temporary lifting of a security freeze. Victims of identity theft will not be charged any fees in connection with the placing, removing, or temporary lifting of a security freeze.

The reporting agency must place the freeze within five business days after receiving the request, and within ten 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. Requests for a temporary unlocking of the freeze must be completed within three business days.

Statute: §815 ILCS 505/2MM:

<http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=081505050K2MM>

“Placing a Security Freeze on Your Credit Report (includes sample letters)”:

http://www.illinoisattorneygeneral.gov/consumers/security_freeze.pdf

Security Breaches: State law requires all data collectors operating in the state that own or license personal information concerning an Illinois resident to notify the resident when there has been a breach of the security of the system, putting them at risk of identity theft. A “data collector” may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that for any purpose handles, collects, disseminates, or otherwise deals with nonpublic personal information. A security breach occurs upon “unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity” of personal information.

Personal information means an individual’s first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social Security number; driver’s license or state identification card number; account number, or 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; or medical information. Publicly available information is not included.

The disclosure notification must be made in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and

confidentiality of the data system. Notification can be provided to the affected persons by mail 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 data collector does 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 data collector's web site, and notification to major statewide media.

Statute: §815 ILCS 530:

<http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapAct=815%26nbsp%3BILCS%26nbsp%3B530%2F&ChapterID=67&ChapterName=BUSINESS+TRANSACTIONS&ActName=Personal+Information+Protection+Act%2E>

“Security Breach Notification Fact Sheet”:

http://www.ag.state.il.us/consumers/breach_notification.pdf

State Resources:

Office of the Attorney General: “Identity Theft”

(<http://www.illinoisattorneygeneral.gov/consumers/hotline.html>)

“Identity Theft Resource Guide”

(http://www.illinoisattorneygeneral.gov/consumers/Identity_Theft_Resource_Guide.pdf)

This comprehensive 32-page document includes a checklist for victims, prevention tips, the ID theft affidavit, and sample letters to credit agencies. It also explains how victims of identity theft can clear their names of crimes they did not commit. It directs victims to: *“FILE A REPORT WITH YOUR LOCAL POLICE DEPARTMENT. You should initiate a law enforcement investigation by contacting the local law enforcement agency, which will take a police report of the matter, provide you with a copy of that report, and begin an investigation of the facts or, if the suspected crime was committed in a different jurisdiction, refer the matter to the law enforcement agency where the suspected crime was committed. Illinois law requires police departments to accept and provide reports. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime.”*

“Identity Theft Victim Kit” (<http://www.ag.state.il.us/publications/pdf/victim.pdf>)

This publication directs victims to: *“Report the fraud to law enforcement – local and ational. Identity theft is a felony under Illinois law. Report the fraud to your local police department as soon as possible and get a copy of the police report. This will alert the police to the crime as well as establish that you acted quickly. Make sure to get the police report, complaint number or other similar record; you may need this information when contacting your creditors. Keep a record of the police investigator's phone number.”*

“Identity Theft Brochure”

(http://www.illinoisattorneygeneral.gov/consumers/brochure_idtheft.pdf)

This brochure directs victims of identity theft to: *“File a police report. Illinois law requires police departments to accept and provide reports. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime.”*

“Identity Theft Hotline”: (<http://www.illinoisattorneygeneral.gov/consumers/Id-Theft-Poster.gif>).

“The hotline provides Illinoisans who have been victimized by identity theft with one-on-one assistance to take the steps necessary to report the crime to local law enforcement and financial institutions, repair their credit, and prevent future problems.

If you have been the victim of identity theft or believe your personal or financial information may have been compromised, please call the toll-free Identity Theft Hotline at: 1-866-999-5630 and 1-877-844-5461 (TTY).”

“Identity Theft Complaint Form”:

http://www.illinoisattorneygeneral.gov/consumers/consum_id_0106.pdf

Fact Sheets:

- “Consumer’s Checklist: Protecting Your Identity” (http://www.illinoisattorneygeneral.gov/consumers/savvy_consumer_IDtheft.pdf)
- “Reporting Identity Theft as a Victim” (<http://www.illinoisattorneygeneral.gov/consumers/reportidtheft0404.pdf>)
- “Protecting Your Social Security Number” (http://www.illinoisattorneygeneral.gov/consumers/Social_Securit_%20Fact_Sheet.pdf)
- “Credit Inquiries” (http://www.illinoisattorneygeneral.gov/consumers/credit_inquiries.pdf)
- “Phishing” (http://www.illinoisattorneygeneral.gov/consumers/facts_on_phishing.pdf)
- “Defending Yourself Against Identity Thieves” (<http://www.illinoisattorneygeneral.gov/consumers/defendidtheft0404.pdf>)

Legislation:

2008:

SB 2400 creates the Biometric Information Privacy Act that establishes guidelines for the collection and storage of biometric data and the rights of those whose data is collected. The legislation requires public agencies and private entities to inform a person in writing and to receive that person’s consent before collecting biometric information. Biometrics images and identifiers of the human body include fingerprints, hand geometry, an iris scan, a voice print, or unique facial features.

In addition, the new law requires all public agencies and private entities collecting biometric identifiers or information to establish a retention and destruction schedule. Under this schedule biometric identifiers or information must be destroyed after the initial purpose of collecting or obtaining the information has been fulfilled or within 3 years of the individual’s last interaction with the agency or entity. It provides certain exemptions for public agencies, especially law enforcement and prosecuting agencies and entities issuing driver’s licenses and permits.

HB 5586 requires county recorders to, on request, redact or remove personal information from documents posted on the Internet. It also calls for any person or agency filing deeds with county recorders to leave Social Security numbers off those documents. Those recorders offices without

an online database cannot display public documents on the Web until they have a policy in place that addresses what steps they will take to protect residents' personal information. Within twelve months, all county recorders will have to have a policy in place that details how they address the question of protecting personal information.

2007:

HB 449 adds identity theft offenses committed in furtherance of the activities of an organized gang to the definition of aggravated identity theft, which provides for enhanced penalties.

HB 1236 increases the penalties for identity theft by one class if the victim of the offense is an active duty member of the Armed Services or Reserve Forces of the United States or of the Illinois National Guard serving in a foreign country.

SB 137 prohibits phishing the act of posing as a legitimate company or government agency in an email, Web page, or other Internet communication in order to trick a recipient into revealing his or her personal information. It is unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing himself, herself, or itself to be a business without the authority or approval of the business. A person who is engaged in the business or providing Internet access service to the public, owns a Web page, or owns a trademark and is adversely affect by a phishing violation may bring an action against a the violator to recover the greater of actual damages or \$500,000. Individual victims may bring an action to seek greater of three times the amount of actual damages or \$5,000 per violation.

SB 1398 requires debt collectors to cease collection activities of a debt when an alleged debtor provides a police report of identity theft and other proof of his status as an identity theft victim. The debt collector must review and consider the information provided by the alleged victim and may only recommence debt collection activities only after making a good faith determination that the information does not establish that the information does not establish that the debtor is not responsible for the specific debt in question. The debtor must be notified of this determination. The bill also helps identity theft victims clear up their records by requiring debt collectors who cease collection activities to notify the creditors and consumer credit reporting agencies to which the collector previously provided adverse information.

2006:

HB 2310 allows all Illinois consumers to place a security freeze on their credit reports. Previously, only victims of identity theft had the right to place such a freeze. To obtain a freeze, a person must request one in writing by certified mail to the credit reporting agency. A security freeze prohibits, with certain specific exceptions, the credit reporting agency from releasing the consumer s credit report or any information from it without the express authorization of the consumer. The credit reporting agency may charge up to \$10 for each placing, removing or temporary lifting of a security freeze. Senior citizens 65 years or older will not be charged to place or permanently lift the security freeze, but may be charged up to \$10 for each temporary lifting of a security freeze. Victims of identity theft will not be charged any fees in connection with the placing, removing, or temporary lifting of a security freeze.

HB 4297 increases the penalty for people convicted of identity theft who use the person identification information or document of another to purchase methamphetamine material with the intent to manufacture the drug. It will be a Class 2 felony for a first offense, and a Class 1 felony for a second or subsequent offense.

HB 4438 creates the offense of facilitating identity theft for state employees who do not properly destroy documents that contain personal identifying information. A person commits the offense when he or she has access to personal identifying information of another person and knowingly, with the intent of committing identity theft, disposes of the information in any receptacle that the public could gain access to without shredding or otherwise destroying the information. A first violation is a class A misdemeanor (up to one year in county jail) and a second or subsequent offense is a Class 4 felony (one to three years in prison).

SB 2554 targets the practice of “pretexting,” which occurs when someone pretends to be an account holder, or to have authorization to access an account, to obtain private account information. It makes it illegal for an identity thief to use somebody else's personal identification information or personal identification document to portray himself or herself as that person without permission, for the purpose of gaining access to any personal identification information or personal identification document of that person. It also makes it illegal to use personal identifying information to gain access to a person's transactions, actions or communications such as cell phone call records.

The legislation also adds user names, passwords, and any other information used to access information about an individual or their actions, transactions, or communications to the list of information protected as personal identifying information. The first violation is a Class 3 felony, punishable by two to five years in jail. If someone pretexts to get information about three or more separate people within a 12-month period, it is a Class 2 felony, carrying a sentence of three to seven years in jail. If a person is convicted of this crime, in the absence of proof of actual damages, the identity theft victim may recover \$2,000 in damages.

2005:

Under **HB 1058**, victims of identity theft will have the right to put a security freeze on their credit file to prevent others from opening new accounts in their names. A security freeze enables the 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 the consumer control over who has access to the information needed to process a credit application and prevents crooks from opening new accounts in the consumer's name. When the consumer is applying for credit, the freeze can be lifted temporarily so the application can be processed.

The passage of **HB 1663** made Illinois the second state (after California) to require companies to quickly notify consumers in the state if their personal information is compromised due to a breach in company security. The law requires any data collector that owns or licenses personal information concerning an Illinois resident to notify the resident that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure

notification would have to be made in "the most expedient time possible and without unreasonable delay." consistent with any measures necessary to determine the scope of the breach.

HB 2699 increases the penalties by one felony class for identity theft and aggravated identity theft crimes. This legislation also increases the penalties against those persons who steal the identities of more than three victims.

HB 2696 prohibits businesses from denying a person credit or utility services, or from increasing a person's credit limits based solely on their status as an identity theft victim.

HB 2697 makes unauthorized copying and transmitting of any financial transaction devices including credit and debit cards, or other devices used to make a payment, get cash, or make a deposit, a Class A misdemeanor.

HB 457 extends the statute of limitations and allows for the commencement of prosecution for identity theft or aggravated identity theft within five years after the discovery of the offense by the victim. Previously, the statute of limitations was one year and six months for a misdemeanor identity theft offense and within three years for a felony identity theft crime or aggravated identity theft offense.

HB 2700 allows for an identity theft prosecution to occur in either the county where the theft occurred, the county where the information was illegally used, or where the victim resides.

2003:

SB 242 aims to give authorities more tools to fight the growing problem of identity theft. The bill expands the legal definition of identity theft, which previously dealt only with the crime's financial aspects. Under one part of the new law, a person is guilty of committing identity theft if he or she obtains, possesses, sells or manufactures someone else's personal identification information or an identification document. Previously, the definition of identity theft only addressed using someone else's identification information to fraudulently get credit, money or other property. The new law also sets a broader definition for a "personal identifying document." The revised definition includes any government-issued document meant to identify a person. It also includes documents issued by a quasi-governmental organization. First-time offenders of the identity theft law could be found guilty of a Class 4 felony, generally punishable by one to three years in prison. Subsequent offenses could draw stiffer punishment, a Class 3 felony and two to five years in prison.

HB 2188 requires law enforcement agencies to take a police report from people in their jurisdiction who have learned or reasonably suspect that his or her personal identifying information has been unlawfully used by another. The agency must give the complainant a copy of the report and begin an investigation. If the crime was committed in another jurisdiction, the agency can refer the matter to the law enforcement agency where the crime was committed. The bill also gives victims of identity theft a clear-cut legal procedure for clearing their names. The bill also provides that a credit card company must verify any address on an application that does not match the address previously attributed to that person's name.