

IOWA

IDENTITY THEFT RANKING BY STATE: Rank 48, 35.6 Complaints Per 100,000
Population, 1063 Complaints (2007)
Updated December 15, 2008

Current Laws: A person commits the offense of identity theft if he fraudulently uses or attempts to fraudulently use identification information of another person, with the intent to obtain credit, property, services, or other benefit.

“Identification information” includes, but is not limited to, a person’s name, address, date of birth, telephone number, driver’s license number, nonoperator’s identification card number, Social Security number, student identification number, military identification number, alien identification or citizenship status number, employer identification number, signature, electronic mail signature, electronic identifier or screen name, biometric identifier, genetic identification information, access device, logo, symbol, trademark, place of employment, employee identification number, parent's legal surname prior to marriage, demand deposit account number, savings or checking account number, or credit card number of a person.

If the value of the credit, property, or services exceeds \$1000, the person commits a class D felony, punishable by up to five year in prison and a fine of \$750 to \$7500. If the value of the credit, property, or services is less than \$1000, it is an aggravated misdemeanor, punishable by up two years in prison and a fine of \$625 to \$6250. In addition, any real or personal property obtained by a person as a result of a violation will be subject to seizure and forfeiture.

Statute: §715.A8:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates\\$fn=document-frame.htm\\$3.0\\$Q=\\$Uq=1\\$x=\\$Up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates$fn=document-frame.htm$3.0$Q=$Uq=1$x=$Up=1)

The value of property or services is its highest value by any reasonable standard at the time the identity theft is committed. Any reasonable standard includes but is not limited to market value within the community, actual value, or replacement value. If credit, property, or services are obtained by two or more acts from the same person or location, or from different persons by two or more acts which occur in approximately the same location or time period so that the identity thefts are attributable to a single scheme, plan, or conspiracy, the acts may be considered as a single identity theft and the value may be the total value of all credit, property, and services involved.

Statute: §715A.9:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26792?f=templates\\$fn=document-frame.htm\\$3.0\\$Q=\\$Uq=1\\$x=\\$Up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26792?f=templates$fn=document-frame.htm$3.0$Q=$Uq=1$x=$Up=1)

Jurisdiction: Violations may be prosecuted in any of the following venues: in the county in which the violation occurred; if the violation was committed in more than one county, or if the elements of the offense were committed in more than one county, then in any county where any

violation occurred or where an element of the offense occurred; in the county where the victim resides; or in the county where the property that was fraudulently used or attempted to be used was located at the time of the violation.

Statute: §715.A8:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates\\$fn=document-frame.htm\\$3.0\\$eq=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates$fn=document-frame.htm$3.0$eq=$uq=1$x=$up=1)

Payment Cards: It is unlawful for a person to use a credit card for the purpose of obtaining property or services with knowledge that the credit card is stolen or forged; has been revoked or cancelled; or that for any other reason the use of the card is unauthorized. It is a class C felony (punishable by up to ten years in prison and/or a fine of \$1000 to \$10,000) if the property or services secured or sought to be secured is greater than \$10,000, a class D felony if between \$1000 and \$10,000, and an aggravated misdemeanor if less than \$1000.

Statute: §715A.6:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26788?f=templates\\$fn=document-frame.htm\\$3.0\\$eq=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26788?f=templates$fn=document-frame.htm$3.0$eq=$uq=1$x=$up=1)

Scanning Devices: State law prohibits the use of a scanning device or re-encoder to obtain or record encoded information from the magnetic strip of a payment card with the intent to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A re-encoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are a class D felony, and a second or subsequent violation is a class C felony.

Statute: §715.A10:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26794?f=templates\\$fn=document-frame.htm\\$3.0\\$eq=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26794?f=templates$fn=document-frame.htm$3.0$eq=$uq=1$x=$up=1)

Spyware: State law prohibits the misuse of the Internet or e-mail to steal personal information or to cause harm to another person's computer with spyware, computer software that can be sent through the Internet into a home or business computer to modify settings or record information without the user's knowledge. It prohibits the transmission of computer software that:

- Modifies computer setting through intentionally deceptive means;
- Collects, through intentionally deceptive means, personally identifiable information through the use of a keystroke-logging function, by correlating identifiable information with data on the sites visited, or by extracting from the hard drive a person's Social Security number, tax identification number, driver's license number, passport number, or any other government-issued identification number, account balances, or overdraft history;
- Prevents, through intentionally deceptive means, an owner's or an operator's reasonable efforts to block the installation of, or to disable, computer software by causing computer software that the owner or operator has properly removed or disabled to automatically reinstall or reactivate on the computer;
- Intentionally misrepresents that computer software will be uninstalled or disabled by an owner's or an operator's action;

- Removes, disables, or renders inoperative security, antispyware, or antivirus computer software installed on an owner's or an operator's computer;
- Modifies any of the following settings related to an owner's or an operator's computer access to, or use of, the internet: settings that protect information about an owner or operator for the purpose of taking personally identifiable information of the owner or operator; or security settings for the purpose of causing damage to a computer; or
- Prevents an owner's or an operator's reasonable efforts to block the installation of, or to disable, computer software.

Violations that cause pecuniary losses exceeding \$1000 to a victim are a class D felony. If it causes less than \$1000 in losses, it is an aggravated misdemeanor.

Statute: §715.4:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26772/26776?f=templates\\$fn=document-frame.htm\\$3.0\\$Q=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26772/26776?f=templates$fn=document-frame.htm$3.0$Q=$uq=1$x=$up=1)

Victim Assistance:

Restitution: A victim injured by a violation or any financial institution that indemnified a victim injured by a violation may file a claim for payment of damages suffered, including costs of recovery and reasonable attorney fees.

Statute: §715.A8:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates\\$fn=document-frame.htm\\$3.0\\$Q=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates$fn=document-frame.htm$3.0$Q=$uq=1$x=$up=1)

Mandatory Police Reports: Upon the request of a victim, a peace officer in any jurisdiction for an identity crime must take a report regarding an alleged identity crime violation and provide a copy of the report to the victim. The report may also be provided to any other law enforcement agency in any of the other possible jurisdictions.

Statute: §715.A8:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates\\$fn=document-frame.htm\\$3.0\\$Q=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26791?f=templates$fn=document-frame.htm$3.0$Q=$uq=1$x=$up=1)

Civil Suits: A victim who suffers a pecuniary loss as a result of identity theft may bring an action against the perpetrator to recover \$5000 or three times the actual damages, whichever is greater, and costs for repairing the victim's credit history or credit rating, costs incurred for bringing a civil or administrative proceeding to satisfy a debt, lien, judgment, or other obligation of the victim, and punitive damages, attorney fees, and court costs. Financial institutions may file a civil action on behalf of the account holder who is a victim of identity theft.

Statute: §714.16B:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26710/26733?f=templates\\$fn=document-frame.htm\\$3.0\\$Q=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26710/26733?f=templates$fn=document-frame.htm$3.0$Q=$uq=1$x=$up=1)

Identity Theft Passport: Victims may apply for an identity theft passport, which can be presented to law enforcement to help prevent arrest or detention for an offense committed by another person. It may also be presented to a creditor to aid in the investigation of a fraudulent accounts or charges. A victim who has filed a report of identity theft with a law enforcement

agency may apply for an identity theft passport through the law enforcement agency. The law enforcement agency will send a copy of the police report and the application to the attorney general, who will process the application and supporting report and may issue the victim an identity theft passport in the form of a card or certificate.

Statute: §715A.9A:

[http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26793?f=templates\\$fn=document-frame.htm\\$3.0\\$eq=\\$uq=1\\$x=\\$up=1](http://nxtsearch.legis.state.ia.us/NXT/gateway.dll/current/2007codesupp/1/26407/26408/26781/26793?f=templates$fn=document-frame.htm$3.0$eq=$uq=1$x=$up=1)

Security Freezes: 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 by certified mail to the credit reporting agencies. A consumer reporting agency may charge up to \$10 to place or remove a security freeze, and a fee up to \$12 for each temporary suspension of 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 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. Requests for a temporary unlocking of the freeze must be completed within three business days. In addition, consumer reporting agencies may develop procedures to expedite the receipt and processing of requests by telephone, fax, the Internet, or other electronic media. If such procedures are developed, the temporary unlocking of the freeze must be completed within fifteen minutes if received during normal business hours.

Legislation: <http://coolice.legis.state.ia.us/Cool-ICE/default.asp?category=billinfo&service=billbook&GA=82&hbill=SF2277>

Security Breaches: State law requires individuals, businesses, and state and local government agencies that own or license computerized data that include a consumer's personal information that is used in the course of a person's business, vocation, occupation, or volunteer activities to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft.

A security breach is defined as "unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of personal information. If an individual, business, or agency discovers a breach of security, it must notify affected consumers in the most expeditious manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, and consistent with any measures necessary to sufficiently determine contact information for the affected consumers, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data.

However, notification is not required, if after an appropriate investigation or after consultation with the relevant federal, state, or local agencies responsible for law enforcement, the person determines that no reasonable likelihood of financial harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be made in writing and the documentation must be maintained for five years.

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 that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: Social Security number; driver's license or other unique identification number created or collected by a government body; financial 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; unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. Publicly available information is not included.

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 350,000, or the business or agency 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 business's web site, and notification to major statewide media. The notice must include, at a minimum, all of the following: a description of the breach of security, the approximate date of the breach, the type of personal information obtained as a result; contact information for consumer reporting agencies; or advice to the consumer to report suspected incidents of identity theft to local law enforcement or the attorney general;

Legislation: <http://coolice.legis.state.ia.us/Cool-ICE/default.asp?category=billinfo&service=billbook&GA=82&hbill=SF2308>

State Resources:

Office of the Attorney General, "A Guide for Identity Theft Victims"

(http://www.state.ia.us/government/ag/consumer/brochures/identitytheft_victims.html)

This comprehensive document directs victims to: *"Report the crime to all police and sheriff's departments with jurisdiction in your case. Give them as much documented evidence as possible. Get a copy of your police report. Keep the telephone number of your fraud investigator handy and give it to creditors and others who require certification of your case. Banks and credit card companies may require you to produce the police report in order to verify the crime."*

"How to Avoid Identity Theft"

(http://www.state.ia.us/government/ag/consumer/brochures/avoid_identitytheft.html)

“Identity Theft – Don’t Let It Happen to You”

(http://www.state.ia.us/government/ag/images/pdfs/Identity_Theft_DONT.pdf)

“Freezing Your Credit Reports”

(http://www.iowa.gov/government/ag/consumer_advisories/credit_finance/Freezing_Your_Credit_Reports_Advisory.pdf)

Department of Transportation, Office of Motor Vehicle Enforcement, “When Bad Things Happen to Your Good Name” (<http://www.dot.state.ia.us/mvd/omve/theft.htm>)

Legislation:

2008:

SF 2308 requires businesses and government agencies that collect and maintain computerized records containing consumer’s personal information to notify affected consumers if that personal data is compromised in a security breach, putting them at risk for identity theft.

SF 2277 allows Iowans to freeze their credit information, restricting access from unwanted viewers. This can help prevent identity theft because most businesses will not open a new credit account without checking the customer's credit history. Consumer reporting agencies can charge up to \$10 to place or lift a security freeze, and \$12 to temporarily lift a freeze. Credit reporting agencies would be prohibited from charging Iowans any fees if they've been the victim of ID theft. They'd be able to charge other Iowans up to \$10 per security freeze. The freeze would remain in effect until the Iowan requests its removal.

2006:

HF 2506 authorizes an identity theft passport program for victims of the crime. Victims can present the passport to law enforcement to help prevent arrest or detention for an offense committed by another person using the passport owner’s personal identifying information. It may also be presented to a creditor to aid in the investigation of a fraudulent account that is opened in his/her name or a fraudulent charge that is made against an account. To obtain a passport, victims must file a police report and apply through a law enforcement agency.

2005:

SF 270 seeks to provide greater protections for victims of identity theft. The bill:

- Provides for the recovery of costs for the repair of a victim's credit history, costs incurred for bringing an action to satisfy an obligation of the victim, and for punitive damages. The law already provided for recovery of attorney fees and court costs.
- Increases the monetary damages that can be collected by identity theft victims from \$1000 or three times the actual loss to \$5,000 or three times the actual loss.
- Expands the definition of “identification information” to include a student or military identification number, alien or citizenship number, employer identification number, signature or electronic signature, electronic identifier or screen name, biometric identifier, genetic identification information, access device, logo, symbol, or trademark.

- Expands the venues for prosecution to include the county in which the violation occurred or if the violation was committed in more than one county, then in any county where the violation occurred; in the county where the victim resides; or the county where the property that was fraudulently used was located at the time of the violation.
- Makes any property obtained as a result of the commission of identity theft subject to forfeiture.
- Provides that victims of identity theft are entitled to a copy of the police report of the crime and allows certain financial institutions to file a criminal complaint on behalf of the victim.
- Expands the remedies available for civil causes of action against people who commit identity theft and allows certain financial institutions to file a civil action on behalf of the account holder who is the victim of identity theft.

HF 614 makes it a crime to misuse the Internet or e-mail to steal personal information or to cause harm to another person's computer. It prohibits the use of Spyware, which can be sent through the Internet into a home or business computer to modify settings or record information without the user's knowledge. The bill makes it an aggravated misdemeanor or a class D felony if the loss to the victim is at least \$1,000. Punishment could range from two years in prison to a five-year sentence and fines.

2003:

HF 170 strengthens state law against identity theft by eliminating the requirement that a person “fraudulently” obtain and use the identification information. The bill also expands the definition to include the intent to obtain any benefit from the identity theft. Previous law limited the definition to receiving credit, property, or services.

HF 504 prohibits the use of a scanning device or re-encoder to obtain or record encoded information from the magnetic strip of a payment card with the intent to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A re-encoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are a class D felony, and a second or subsequent violation is a class C felony.