ID Safety
Protecting the *real* you, and *only* you.

In partnership with: INTERNATIONAL ASSOCIATION of CHIEFS OF POLICE Bank of America

INDIANA
IDENTITY THEFT RANKING BY STATE: Rank 26, 63.4 Complaints Per 100,000 Population, 4026 Complaints (2007)
Updated November 30, 2008

Current Laws: A person commits the crime of identity deception if he knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person, including the identifying information of a person who is deceased, without the person's consent, and with intent to harm or defraud another person; assume another person's identity; or profess to be another person. Violations are a Class D felony, punishable by six months to three years in prison and a fine up to $10,000. The crime is a Class C felony, punishable by two to eight years in prison and a fine up to $10,000, if a person obtains, possesses, transfers, or uses the identifying information of more than 100 people, or the fair market value of the fraud or harm caused by the offense is at least $50,000.

This does not apply to a person under 21 who uses the identifying information of another person to acquire an alcoholic beverages, or to a minor who uses the information of another to acquire a cigarette or tobacco product; a periodical, videotape or other communication medium that contains or depicts nudity; admittance to a performance that prohibits the attendance of a minor based on age; or an item that is prohibited by law for use or consumption by a minor.
Statute: §35-43-5-3.5: http://www.ai.org/legislative/ic/code/title35/ar43/ch5.html#IC35-43-5-3.5

A person who knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person with intent to commit terrorism or obtain or transport a weapon of mass destruction commits terroristic deception, a Class C felony.
Statute: 35-43-5-3.6: http://www.ai.org/legislative/ic/code/title35/ar43/ch5.html#IC35-43-5-3.6

"Identifying information" is defined as information that identifies an individual that can be used to obtain money, goods, services, or any other thing of value, or initiate a transfer of funds, including an individual's:

- Name, address, date of birth, place of employment, employer identification number, mother's maiden name, Social Security number, or any identification number issued by a governmental entity;
- Unique biometric data, including the individual's fingerprint, voice print, or retina or iris image;
- Unique electronic identification number, address, or routing code;
- Telecommunication identifying information; or
- Telecommunication access device, including a card, a plate, a code, a telephone number, an account number, a personal identification number, an electronic serial number, a mobile identification number, or another telecommunications service or device or means of account access.

Statute: §35-43-5-1: http://www.ai.org/legislative/ic/code/title35/ar43/ch5.html#IC35-43-5-1

Jurisdiction: A person who commits the offense of identity deception may be tried in a county in which the victim resides; or where the person obtains, possesses, transfers, or uses the information used to commit the offense. If a person is charged with more than one offense of identity deception, and either the victims of the crimes reside in more than one county or the commits the crime in more than one county, the person may be tried in any of the counties.
Statute: §35-32-2-6: http://www.ai.org/legislative/ic/code/title35/ar32/ch2.html#IC35-32-2-6

Government-Issued Identification Cards: It is a Class D felony to knowingly or intentionally use false information or make a false statement in an application for a driver's license or identification card or for a renewal or duplicate of an identification card.
Statute: 35-43-5-2: http://www.ai.org/legislative/ic/code/title35/ar43/ch5.html#IC35-43-5-2

It is a Class A misdemeanor, punishable by up to one year in prison and a fine up to $1000, to knowingly possess, produce, or distribute a document not issued by a government entity that purports to be a government-issued identification:
Statute: 35-43-5-2.5: http://www.ai.org/legislative/ic/code/title35/ar43/ch5.html#IC35-43-5-2.5

Payment Cards: A person commits fraud, a Class D felony, if he:

- With intent to defraud, obtains property by using a credit card, knowing that it was unlawfully obtained or retained, forged, revoked, or expired; using a card issued to another person without consent; representing, or without the consent of the credit card hold, that the person is the authorized user of the card.
- Not being the issuer, knowingly or intentionally sells a credit card.
- Not being the issuer, receives a credit card, knowing that it was unlawfully obtained or retained or that the card is forged, revoked, or expired.

Statute: 35-43-5-4: http://www.ai.org/legislative/ic/code/title35/ar43/ch5.html#IC35-43-5-4

Scanning Devices: State law prohibits the possession and use of card skimming devices, which are designed to read, record, or transmit information encoded on a credit card. A person who possesses a card skimming device with intent to commit identity deception or fraud commits the crime of unlawful possession of a card skimming device, a Class D felony. It is a Class C felony if used to commit terroristic deception.
Statute: 35-43-5-4.3: http://www.ai.org/legislative/ic/code/title35/ar43/ch5.html#IC35-43-5-4.3

Spyware: State law prohibits the use of 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 knowing or intentional 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 credit or debit card number, bank account number, or any password or access code associated with these numbers, 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.

Statute: §24-4.8: http://www.ai.org/legislative/ic/code/title24/ar4.8/index.html

Social Security Numbers: With certain exceptions, state agencies are prohibited by law from releasing an individual's Social Security number (SSN). Disclosure of the last four digits of an individual's Social Security number is not a disclosure of the individual's Social Security number. Before disclosing a public record, an agency must remove or completely and permanently obscure a SSN. If an agency releases an SSN, it must provide notice to the person whose SSN was disclosed in violation of law. An employee of a state agency who knowingly, intentionally, or recklessly discloses a Social Security number commits a Class D felony. If the disclosure is due to negligence, it is a Class A misdemeanor. A person who knowingly, intentionally, or recklessly makes a false representation to a state agency to obtain a Social Security number from the state agency commits a Class D felony.
Statute: §4-1-10: http://www.ai.org/legislative/ic/code/title4/ar1/ch10.html#IC4-1-10-1

Disposal of Customer Records: State law restricts how businesses can dispose of records that contain the personal information of customers. It prohibits the disposal of unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable. Personal information is considered redacted if it has been altered or truncated so that no more than the last four digits of a driver's license number, state identification number, or account number is accessible, or no more than the five digits of a Social Security number are accessible. Violations are a Class C infraction, and a Class A misdemeanor if the person disposes of the unencrypted, unredacted personal information of more than 100 customers or has previously been convicted of this violation.
Statute: §24-4-14: http://www.ai.org/legislative/ic/code/title24/ar4/ch14.html

Victim Assistance:

Restitution: The court may order a person convicted of identity deception to make restitution to the victim, the victim's estate, or the family of a victim who is deceased. The restitution amount will be based upon consideration of the amount of fraud or harm caused by the convicted person and any reasonable expenses, including lost wages, incurred by the victim in correcting his/her credit report and addressing any other issues caused by the commission of the offense. For five

years after sentencing, the court has the discretion to increase restitution if a victim or his/her family discovers or incurs additional expenses that result from the offense.
Statute: §35-50-5-3: http://www.ai.org/legislative/ic/code/title35/ar50/ch5.html#IC35-50-5-3

Court Orders: When an offender is convicted of a crime of deception, including identity deception, the court may, upon motion by the state or upon application by a victim, issue an order that describes the person whose credit history may be affected by the offender's crime of deception, with sufficient identifying information to assist another person in correcting the credit history; and states that the person was the victim of a crime of deception that may have affected the person's credit history.
Statute: §35-38-1-2.5: http://www.ai.org/legislative/ic/code/title35/ar38/ch1.html#IC35-38-1-2.5

Security Freeze: All Indiana consumers are allowed to place security freezes on their consumer credit reports to prevent others 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 mail to the credit reporting agencies. By January 1, 2009, the consumer reporting agencies must make available to consumers a secure electronic method for requesting the freeze. There is no fee for placing, removing, or temporarily lifting a security freeze.

The reporting agency must place the freeze within five business days after receiving the request, and within ten days 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. Starting January 1, 2009, however, temporary unlocking must be completed within 15 minutes after the consumer's request is received through an electronic contact method or by telephone, during normal business hours.
Statute: §24-5-24: http://www.in.gov/legislative/ic/code/title24/ar5/ch24.html

Office of the Attorney General, Security Freeze Law:
http://www.indianaconsumer.com/idtheft/SecurityFreeze.asp

How to Place a Security Freeze in Indiana:
www.consumersunion.org/pdf/security/securityIN.pdf

Security Breach: State law requires businesses operating in the state that own or license computerized data that include consumers' personal information to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. A security breach occurs upon "unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity" of personal information. The unauthorized acquisition of a portable electronic device on which personal information is stored will not be considered a security breach if the contents of the device are encrypted and if the encryption key is not compromised.

After discovering or being notified of a breach of the security of the system, the database owner must disclose the breach to an Indiana resident whose unencrypted personal information was or may have been acquired by an unauthorized person, or whose encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key, if the business knows or should know that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity fraud, or fraud. Notification must occur without unreasonable delay, consistent with the legitimate needs of law enforcement. If more than 1000 consumers must be notified, consumer reporting agencies must also be notified.

Personal information means an individual's first name or first initial and his/her last name, in combination with any one or more of the following data elements that is not encrypted or redacted: Social Security number; driver's license or Indiana identification card number; an account number, credit card number; financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account. Publicly available information is not included.

Notification can be provided to the affected persons by mail, e-mail, telephone, or fax. If the cost of providing regular notice would exceed $250,000 or the amount of people to be notified exceeds 500,000, the business may make the disclosure by conspicuous posting of the notice on its web site and notice to major news reporting media in the geographic area where Indiana residents affected by the breach reside.
Statute: §24-4.9-3: http://www.in.gov/legislative/ic/code/title24/ar4.9/ch3.html

State government agencies that maintain, own, or license computerized data that include consumers' personal information are required to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. A security breach occurs upon "unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity" of personal information. Consumers must be notified without unreasonable delay, consistent with the legitimate needs of law enforcement.

Personal information means an individual's first name or first initial and his/her last name, in combination with any one or more of the following data elements: Social Security number; driver's license or Indiana identification card number; an account number, credit or debit card number, security code, access code, or password of an individual's financial account. 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 500,000, or the agency does not have sufficient contact information, an alternate form of notice may be provided, including conspicuous posting on the agency's web site and notification to media.
Statute: §4-1-11: http://www.in.gov/legislative/ic/code/title4/ar1/ch11.html

---

State Resources:

Office of the Attorney General, "Identity Theft"
(http://www.indianaconsumer.com/idtheft/index.asp)

"Identity Theft Victim Kit"
(http://www.indianaconsumer.com/consumer_guide/pub/IdentityTheft_Kit.pdf)
This document is designed to assist Indiana consumers who are victims of identity theft in resolving their cases and clearing their names. It directs victims to: "*Report the incident to law enforcement: Contact your local police department or sheriffs office to file a report. When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit. Request a copy of the police report. Some creditors will request to see the report to remove the debts created by the identity thief.*"

"Identity Theft E-Book" (http://indianaconsumer.com/ebook-idtheft/index.asp)

"Identity Theft Fact Sheet" (http://indianaconsumer.com/consumer_guide/pub/20050802.4.pdf)

"Identity Theft Interactive Quiz" (http://www.indianaconsumer.com/idtheft/id_theft_quiz.asp)

"Phishing" (http://indianaconsumer.com/consumer_guide/phishing.asp)

"Beware of Spyware – Learn the Clues"
(http://www.indianaconsumer.com/consumer_guide/safe_computing.asp)

Legislation:

2008:
Under **HB 1197**, the unauthorized acquisition of a laptop or other portable storage device on which personal information is stored will not be considered a security breach if the contents of the device are encrypted and if the encryption key is not compromised. It also authorizes the attorney general to initiate a program to educate consumers of risks posed by a security breach. As introduced, the bill would have required industry-standard encryption practices designed to protect consumer data, as well as centralized reporting of security breaches. It also would have made Indiana the first state in the U.S. to require that all breach reports be posted online on the attorney general's Web site. However, these provisions were stripped from the bill before passage.

2007:

SB 403 allows 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. There is no fee for placing, removing, or temporarily lifting the freeze.

2006:

HB 1101 includes several new protections for victims of identity theft. The bill:

- Requires disclosure of security breaches and encryption of data by companies holding customers' and clients' personal identification information in computer databases if it could cause identity theft, identity deception, or fraud. This would help protect consumers by making them aware when their personal information may have been stolen. People would then be able to take the necessary steps to protect themselves from any further damage.
- Restricts how businesses can dispose of records that contain the personal information of consumers. It prohibits the disposal of unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable. Violations are a Class C infraction, and a Class A infraction if the person disposes of the unencrypted, unredacted personal information of more than 100 customers or has previously been convicted of this violation.
- Provides that a person who commits the offense of identity deception may be tried in a county in which the victim resides; or where the person obtains, possesses, transfers, or uses the information used to commit the offense. If a person is charged with more than one offense of identity deception, and either the victims of the crimes reside in more than one county or the commits the crime in more than one county, the person may be tried in any of the counties.
- Adds obtaining the identifying information of a deceased person to the definition of identity deception.
- Makes identity deception a Class C felony if a person unlawfully obtains the identities of more than 100 persons or the fair market value of the fraud or harm caused by the identity theft is at least $50,000.
- Makes possession of a card skimming device with the intent to commit identity deception or fraud a Class D felony and a Class C felony if the device is possessed with the intent to commit terroristic deception.
- Permits a court to enter a restitution order requiring a person convicted of identity deception to reimburse the victim for additional expenses that arise or are discovered after sentencing or after the entry of a restitution order, and grants a court a five-year period in which to order a person convicted of identity deception to pay additional restitution.

2005:

SB 49 prohibits the use of illicit software, known as spyware, to covertly gather personal information through the user's Internet connection. The bill prohibits any person from transmitting, through intentionally deceptive means, computer software and using the software to change Internet control settings; collect personally identifiable information, prevent the operator's efforts to block the installation or execution of the software; falsely claim that

software will be disabled by the operator's actions; remove or disable security software installed on the computer; or take control of the computer.

SB 503 prohibits state agencies from releasing an individual's Social Security number, and requires agencies to notify consumers of any security breaches that may have compromised their personal identifying information.

2003:
SB 320 strengthens state laws on identity theft, making it easier to prosecutor violators. Previously, in order to charge someone with identity deception, a prosecutor had to prove that the thief stole information with the intent to harm or defraud another person. Under the new law, the threshold will be lowered so the prosecutor would have to prove only that a thief stole information in order to assume another person's identity. Victims of identity theft also would get some help under the bill, which allows a court to issue an order correcting a person's credit history.

2001:
HB 1106 increases penalties for identity fraud and deception. The new law provides that a person commits the crime of identity deception, a Class D felony, if the person knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person without the other person's consent and with intent to harm or defraud another person. The law provides for certain exceptions, including people who use false identification to purchase alcohol, cigarettes, or certain magazines, or to gain access to certain movies. Under the law, a person commits fraud, a Class D felony, if the person knowingly and with intent to defraud presents to an insurance claimant a false, incomplete, or misleading claim statement.