

ARKANSAS

IDENTITY THEFT RANKING BY STATE: Rank 33, 56.5 Complaints Per 100,000
Population, 1601 Complaints (2007)
Updated September 1, 2008

Current Laws: A person commits financial identify fraud if, with the intent to create, obtain, or open a credit account, debit account, or other financial resource for his or her benefit or for the benefit of a third party, he or she accesses, obtains, records, or submits to a financial institution another person's identifying information without the authorization of the person identified by the information; or appropriates a financial resource of another person to his or her own use or to the use of a third party without the authorization of that other person.

“Identifying information” includes, but is not limited to, a Social Security number; driver’s license number; checking or savings account number; credit or debit card number; personal identification number or electronic identification number; digital signature; or any other number or information that can be used to access a person’s financial resources.

Financial identity fraud is a Class C felony, punishable by between three and ten years in prison and/or up to a \$10,000 fine. However, the punishment is increased to a Class B felony, punishable by between five and twenty years in prison and/or a fine up to \$15,000, if the victim is an elderly person (60 and older) or disabled, defined as a person with a physical or mental impairment that substantially limits one or more of his/her major life activities.

Statute: §5-37-227: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Scanning Devices: Financial identity fraud also includes the use of a scanning device or re-encoder that is used to obtain or record encoded information from the magnetic strip of a payment card. 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.

A person commits nonfinancial identity fraud if he or she knowingly obtains another person’s identifying information without the other person’s authorization, and uses the identifying information for any unlawful purpose, including to avoid apprehension or criminal prosecution, to harass another person, or to obtain or attempt to obtain a good, service, real property, or medical information of another person. Violations are a Class D felony, punishable by up to six years in prison and/or a fine up to \$10,000, unless the victim is an elderly person or a disabled person, in which case it is a Class C felony. These provisions do not apply to any person who obtains another person's driver's license or other form of identification for the sole purpose of misrepresenting the actor's age.

Statute: §5-37-227: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Jurisdiction: The venue for any criminal prosecution or civil action to recover damages relating to financial or nonfinancial identity fraud may be in any county where any element of the violation occurred, in the county where the victim resides, or in the county where property was fraudulently used or attempted to be used was located at the time of the violation.

Statute: §5-37-227: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Payment Cards: A person commits the offense of fraudulent use of a credit card or debit card, if with purpose to defraud, he or she uses a credit card, credit card account number, debit card, or debit card account number to obtain property or a service with knowledge that the card or account number is stolen; has been revoked or cancelled; is forged; or is unauthorized by either the issuer or the person to whom the credit card or debit card is issued. Fraudulent use of a credit or debit card is a Class C felony if the value of all moneys, goods, or services obtained during any six-month period exceeds \$100, and a Class A misdemeanor if it is less than \$100. Class A misdemeanors are punishable by up to one year in prison and/or a fine up to \$1000.

Statute: §5-37-207: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Spyware: State law prohibits a person that is not an authorized user of a computer from knowingly or willfully causing computer software to be copied on to any computer or use 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.

Personally identifiable information means any of the following if it allows the entity holding the information to identify an authorized user by first name or first initial in combination with last name; credit or debit card numbers or other financial account numbers; a password or personal identification number or other identification required to access an identified account; a Social Security number; account balances, overdraft history, payment history, history of websites visited, home or work address, or a record of a purchase or purchases.

Statute: §4-111-101 to 105: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Computer Fraud: A person commits computer fraud if he intentionally accesses or causes to be accessed any computer, computer system, computer network, or any part of a computer, computer system, or computer network for the purpose of: devising or executing any scheme or artifice to defraud or extort; or obtaining money, property, or a service with a false or fraudulent intent, representation, or promise. Computer fraud is a Class D felony.

Statute: §5-41-103: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Phishing: State law prohibits phishing, defined as the use of electronic mail or other means to imitate a legitimate company or business in order to entice the user into divulging passwords, credit card numbers, or other sensitive information for the purpose of committing theft or fraud. Statute: §4-110-102 to 103: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Social Security Numbers: State law prohibits any business, organization, or individual from publicly posting or displaying in any manner an individual's Social Security number (SSN). It also prohibits printing an SSN on any card required for the individual to access products or services; printing a SSN on a postcard or in a manner in which the SSN is visible on an envelope or without opening the envelope; or requiring an individual to transmit his SSN over the Internet unless the connection is secure or the SSN is encrypted. Statute: §4-86-107: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Destruction of Records: State law requires businesses and state agencies to take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control that contain personal information that is no longer to be retained. The records must be shredded, erased, or otherwise modified so that the personal information in the records is unreadable or undecipherable. Statute: §4-110-104: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Victim Assistance:

Mandatory Police Reports: A person who learns or reasonably suspects that he or she is the victim of financial identity fraud may contact the local law enforcement agency that has jurisdiction over the city or county where the person resides. The local law enforcement agency must take a police report of the matter, whether or not the agency has jurisdiction to investigate and prosecute a crime of financial identity fraud against the victim, and must provide the victim with a copy of the police report. The agency may refer the police report to a law enforcement agency with jurisdiction to investigate and prosecute a crime of financial identity fraud. A police report filed by a victim of financial identity fraud under this section is not required to be counted as an open case for purposes such as compiling open case statistics.

Statute: §5-37-228: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Restitution: State law provides that in addition to any other penalty, a judge may order a defendant convicted of financial or nonfinancial identity fraud to make restitution to any victim whose identifying information was appropriated. This may include any costs incurred by the victim in correcting his/her credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation resulting from the theft of the victim's identifying information, including lost wages and attorney's fees. Statute: §5-37-227: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

Security Freeze: Victims of identity theft 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, an identity theft victim must request one in writing by certified mail to the credit reporting agencies, and must provide a copy of a valid investigative report, an incident report, or a complaint with a law enforcement agency about the unlawful use of their identifying information. Credit reporting agencies may charge \$10 for each security freeze, removal of a security freeze, or temporary lifting of a freeze for a period of time.

The reporting agency must place the freeze within five business days after receiving the request. Within ten days of receiving the request, they 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: §4-112-101: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

To Place a Security Freeze in Arkansas: www.consumersunion.org/pdf/security/securityAR.pdf

Security Breach: State law requires state agencies and 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 compromises the security, confidentiality or integrity" of personal information. Disclosure must occur to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible, and without unreasonable delay, consistent with legitimate needs of law enforcement. Notification is not required if after a reasonable investigation the person or business determines that there is no reasonable likelihood of harm to customers.

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, when either the name or the data elements are not encrypted or redacted: Social Security number; driver's license or Arkansas identification card number; an account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account; or medical information. 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 entity or business 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 entity's web site, and notification to statewide media.

Statute: §4-110-105: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

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. To obtain a passport, victims must apply through the Office of the Attorney General, by submitting a copy of the police report, an application for an identity theft passport, and any other supporting documentation requested by the Attorney General.

Statute: §5-37-228: http://www.arkleg.state.ar.us/data/ar_code.asp (and search for specific statute)

“Identity Theft Passport Request, Victim Information Sheet”
(<http://www.ag.arkansas.gov/pdfs/idtheftpassport.pdf>)

State Resources:

Office of the Attorney General, “Identity Theft” (http://ag.arkansas.gov/identity_theft.html)

“How Can I Protect Myself from Identity Theft?”
(http://ag.arkansas.gov/identity_theft_how_protect.html)

This document provides consumers with important prevention tips.

“If I Believe I Am A Victim Of Identity Theft, What Do I Do?”
(http://ag.arkansas.gov/identity_theft_what_to_do.html)

This document advises victims to “*File an identity theft report with your local law enforcement agency.*”

“Arkansas Credit Report Security Freeze Act”
(http://ag.arkansas.gov/identity_theft_ar_security_freeze.html)

This document explains how Arkansas consumers can take advantage of the security freeze provisions passed by the Legislature in 2007.

“Identity Theft Passports” (http://ag.arkansas.gov/identity_theft_passport.html)

“Consumer Issues: A Guide for Senior Citizens”
(<http://ag.arkansas.gov/pubs/SeniorBrochure.pdf>)

The section on identity theft directs victims to “*report it to local law-enforcement officials immediately, as well as to the Attorney General’s Office.*”

Legislation:

2007:

HB 2215 allows victims of identity theft to place a security freeze on their credit files. A security freeze enables a consumer to prevent anyone from looking at his or her own credit reporting file for purposes of granting credit unless the consumer chooses to let that particular business look at the information. This gives consumers control over who has access to their information needed to process a credit application and effectively prevents thieves from opening new accounts in their name. When the consumer is applying for credit, the security freeze can be lifted temporarily so the application can be processed. A victim must submit a copy of a valid investigative report, an incident report, or a complaint with a law enforcement agency about the unlawful use of their identifying information

The legislature also passed a bill (**HB 2870**) that would have allowed all Arkansas consumers to place a security freeze. However, this bill was vetoed by the governor.

HB 1309 increases the penalty for financial identity fraud from a Class C felony to a Class B felony if the victim is an elderly person (60 or older) or a disabled person, defined as a person with a physical or mental impairment that substantially limits one or more of his/her major life activities. Financial identity fraud is currently punishable by between three and 10 years in prison and/or up to a \$10,000 fine. The punishment would increase to between five and 20 years in prison and/or up to a \$15,000 fine for elderly and disabled victims.

The bill also creates the offense of nonfinancial identity fraud, which is committed if a person obtains another person's identifying information without authorization and uses the information for any unlawful purpose. This includes situations where the information is used to avoid apprehension or criminal prosecution; to harass another person; or to obtain or to attempt to obtain a good, service, real property, or medical information of another person. Violations are a Class D felony unless the victim is an elderly person or a disabled person, in which case it is a Class C felony.

It also provides that in addition to any other penalty, a judge may order a defendant convicted of financial or nonfinancial identity fraud to make restitution to any victim whose identifying information was appropriated. This may include any costs incurred by the victim in correcting his/her credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation resulting from the theft of the victim's identifying information, including lost wages and attorney's fees.

2005:

SB 1167 requires a person, business, or state agency that acquires, owns, or licenses personal information about an Arkansas resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. The bill also requires that consumers be given notice of the disclosure of their personal information due to breaches in the security of data stored by a person, business, or state agency.

HB 1354 clarifies that the offense of financial identity fraud pertains to the use of identifying information to open or create an account or financial resource. The act also changes the classification of financial identity fraud from a Class D felony to a Class C felony.

HB 1740 authorizes the Attorney General to issue an “identity theft passport” to a person who has been or may have been a victim of financial identity fraud if the person is a resident of Arkansas and files a police report. The passport may be used in the event that the person is arrested for offenses committed by another person using the passport holder's identity or to aid creditors in the investigation of credit card fraud or other fraud. The bill also requires law enforcement agencies to take a report from people who live in their jurisdiction who believe they are victims of identity fraud.

HB 2619 provides that the offense of financial identity fraud includes the use of a scanning device or a re-encoder in order to appropriate a financial resource of another person without the person's authorization to the offender's own use or to the use of a third party.

SB 335 seeks to make Social Security numbers less accessible to the general public. Among other things, the bill would bar an individual, business or other entity from publicly posting or publicly displaying an individual's Social Security number. It also would prohibit printing the number on a postcard or any piece of mail not requiring an envelope or in a way that the number is visible on the envelope or without the envelope being opened. It also prohibits any requirement that a person provide his or her Social Security number over the Internet unless the connection is secure or the social security number is encrypted.

HB 2904 prohibits the improper use of computer spyware and provides that any violation of the act is punishable by the Attorney General under the Deceptive Trade Practices Act. It also creates the Spyware Monitoring Fund to be used by the Attorney General to enforce the act and maintain a website to inform consumers about computer and spyware fraud.