

ARIZONA

IDENTITY THEFT RANKING BY STATE: Rank 1, 137.1 Complaints Per 100,000

Population, 8668 Complaints (2007)

Updated November 22, 2008

Current Laws: A person commits the crime of taking the identity of another person if he/she knowingly takes, purchases, manufactures, records, possesses or uses any personal identifying information of another person without consent and with the intent to use the other person's identity for an unlawful purpose or to cause loss. The crime occurs even if the other person does not suffer any economic loss as a result of the offense.

Violations are a class 4 felony, punishable by up to two and a half years in jail and/or a fine up to \$150,000. Prosecutors can consolidate identity theft crime complaints against one defendant so that violations committed in different precincts or counties can be heard in one court. This section does not apply to people under 21 who use false identification to gain access to an establishment licensed to sell alcohol.

Statute: §13-2008:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02008.htm&Title=13&DocType=ARS>

The crime becomes aggravated identity theft if it involves the personal identifying information of five or more persons or causes one person to suffer an economic loss of \$3000 or more. This is a class 3 felony, punishable by up to three and a half years in jail and/or a fine up to \$150,000.

Statute: §13-2009:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02009.htm&Title=13&DocType=ARS>

A person commits the crime of trafficking in the identity of another person if he/she knowingly sells, transfers, or transmits any personal identifying information of another person without consent and for any unlawful purpose, to cause loss, or to allow another person to obtain or continue employment. It does not matter if the person suffers no economic loss as a result. It is a class 2 felony, punishable by up to five years in prison and/or a fine up to \$150,000.

Statute: §13-2010:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02010.htm&Title=13&DocType=ARS>

“Personal identifying information” includes any written document or electronic data that provides information concerning a name, signature, electronic identifier or screen name, electronic mail signature, address or account, biometric identifier, driver or professional license number, access device, residence or mailing address, telephone number, employer, student or military identification number, social security number, tax identification number, employment information, citizenship status or alien identification number, personal identification number,

photograph, birth date, savings, checking or other financial account number, credit card, charge card or debit card number, mother's maiden name, fingerprint or retinal image, the image of an iris or deoxyribonucleic acid or genetic information.

Statute: §13-2001:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02001.htm&Title=13&DocType=ARS>

Payment Cards: A person commits theft of a credit card or obtaining a credit card by fraudulent means if the person controls a credit card without the cardholder's or issuer's consent; or sells, transfers, or conveys a credit card with intent to defraud. Violations are a class 5 felony, punishable by up to one and a half years in prison and/or a fine up to \$150,000.

Statute: §13-2102:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02102.htm&Title=13&DocType=ARS>

A person commits fraudulent use of a credit card if the person:

- With intent to defraud, uses, for the purposes of obtaining or attempting to obtain money, goods, services or any other thing of value, a credit card or credit card number obtained or retained fraudulently or a credit card or credit card number which the person knows is forged, expired, cancelled or revoked; or
- Obtains or attempts to obtain money, goods, services or any other thing of value by representing, without the consent of the cardholder, that the person is the holder to a specified card or by representing that the person is the holder of a credit card and the card has not in fact been issued.

Violations are a class 1 misdemeanor. However, if the value of the money, goods, services or other things of value is between \$250 and \$999 in a six-month period, it is a class 6 felony, and a class 5 felony is over \$1000 in a six-month period.

Statute: §13-2015:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02105.htm&Title=13&DocType=ARS>

The same penalties apply to a third party who receives anything of value obtained by the fraudulent use of a credit card by buying or receiving or attempting to buy or receive money, goods, services or any other thing of value obtained fraudulently, knowing or believing that it was so obtained.

Statute: §13-2103:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02103.htm&Title=13&DocType=ARS>

It is a class 4 felony for a person, other than the cardholder, with intent to defraud, to sign the name of any actual or fictitious person to a credit card or instrument for the payment of money that evidences a credit card transaction.

Statute: §13-2104:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02104.htm&Title=13&DocType=ARS>

It is a class 5 felony to make a false statement as to financial condition or identity when applying for a credit card, if the person knows it to be false.

Statute: §13-2107:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02107.htm&Title=13&DocType=ARS>

Scanning Devices: State law prohibits the possession or 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 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 6 felony, punishable by up to one year in prison and/or a fine up to \$150,000.

Statute: §13-2110:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02110.htm&Title=13&DocType=ARS>

Phishing: State law prohibits phishing scams, in which identity thieves try to trick consumers out of personal information by sending fraudulent e-mails, purporting to originate from a familiar institution, such as a bank. It is a class 5 felony to use a web page or electronic mail message or otherwise using the Internet to solicit, request or take any action to induce another person to provide identifying information by representing that the person, either directly or by implication, is an on-line business without the authority or approval of the on-line business.

In addition to the criminal penalty, violators may be targeted in a civil action. The attorney general, Internet service providers, or a person who owns a Web site or trademark that has been adversely affected may bring an action to stop further violations, and recover the greater of actual damages or \$500,000 for each violation. If the court determines there is a pattern of violations (multiple violations resulting from one act are a single violation), damages can be trebled.

Statute: §44-7201 through 7204 (must click on “next document” link to scroll through the four sections):

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/07201.htm&Title=44&DocType=ARS>

Spyware: State law prohibits the use of spyware to covertly gather personal information through a person’s Internet connection. The law 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. The attorney general, computer software provider or a Web site or trademark adversely affected can bring action against a violator to stop further violations or recover the greater of actual damages or \$100,000 for each separate violation. The court may

increase the damages up to three times if the defendant has a pattern of violating the law, and may also award costs and reasonable attorney fees to the prevailing party.

Statute: 44-7301 through 7304 (must click on “next document” link to scroll through the four sections):

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/07301.htm&Title=44&DocType=ARS>

Disposal of Customer Records: To prevent identity theft, state law restricts how businesses can dispose of paper records with confidential information about individuals. The law prohibits businesses from knowingly discarding paper records or documents with sensitive identifying data without first redacting the data or shredding or otherwise destroying the documents. It applies to data that includes a person’s name and Social Security, driver's license and financial account numbers. Violations are punishable by a civil penalty of \$500 for the first offense, \$1,000 for a second, and \$5,000 for each subsequent one.

Statute: §44-7601:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/07601.htm&Title=44&DocType=ARS>

Social Security Numbers: It is unlawful for any person or entity to:

- Intentionally communicate or otherwise make an individual’s Social Security number available to the general public.
- Print an individual’s Social Security number on any card required for the individual to receive products or services provided by the person or entity.
- Require the transmission of an individual’s Social Security number over the Internet unless the connection is secure or the social security number is encrypted.
- Require the use of an individual’s Social Security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the site.
- Print a number that the person or entity knows to be an individual’s Social Security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. This does not prohibit the mailing of documents that include Social Security numbers sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number.

However, a person or entity that before January 1, 2005 used an individual's Social Security number in a manner inconsistent the above provisions may continue using that individual’s Social Security number in that manner subject to the following conditions:

- The use of the Social Security number must be continuous. If the use is stopped for any reason, the above provisions apply.
- The person or entity must provide the individual with an annual written disclosure of the individual’s right to stop the use of the Social Security number in a manner prohibited by state law.
- If the individual requests in writing, the person or entity must stop using the Social Security number in a manner prohibited by state law within thirty days after receiving the request. No

fee or charge is allowed for implementing the request, and the person or entity may not deny services to the individual because of the request.

State law also prohibits any state or political subdivision of the state from using an individual's SSN on state-issued or political subdivision-issued forms of identification.

Statute: §44-1373:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/01373.htm&Title=44&DocType=ARS>

Beginning on January 1, 2009, a person or entity may not knowingly:

- Print any sequence of more than five numbers that are reasonably identifiable as being part of an individual's Social Security number on any card required for the individual to receive products or services provided by the person or entity.
- Print any sequence of more than five numbers that are reasonably identifiable as being part of an individual's Social Security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. This does not prohibit the mailing of documents to the individual that include Social Security numbers that is sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number or sequence of numbers.

Statute: §44-1373.02: <http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/01373-02.htm&Title=44&DocType=ARS>

Change of Address: State law requires creditors to verify a consumer's address before extending credit if the address differs from the one on record and verify the identity of a consumer if they do not use consumer credit reports.

Text of Legislation:

<http://www.azleg.gov/FormatDocument.asp?inDoc=/legtext/48leg/2r/bills/hb2587s.htm>

Victim Assistance:

Mandatory Police Reports: State law requires a peace officer in any jurisdiction in which an element of the offense is committed, a result of the offense occurs, or the person whose identity is taken resides or locates to take a police report upon request. The officer may provide a copy of the report to any other law enforcement agency that is located in a jurisdiction in which the violation occurred.

Statute: §13-2008:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/13/02008.htm&Title=13&DocType=ARS>

Criminal Identity Theft: Starting January 1, 2009, state law will allow a person who reasonably believes that he or she is the victim of identity theft to petition the superior court for a judicial determination of his or her factual innocence, if as a result of the person's personal identifying information being taken, the person's name was either used by another person who was arrested, cited, or charged with a criminal offense, or entered as of record in a judgment of

guilt in a criminal case. If the court finds by a clear and convincing evidence that the person is factually innocent, the court will issue an order certifying this determination.

Security Freeze: All Arizona consumers are allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened 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 or by telephone, fax, the Internet, or other electronic media if the credit reporting agency has developed procedures for consumers to do so.

The reporting agency must place the freeze within ten business days after receiving the request, and within ten days of placing the request, 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 if received by mail. If a consumer reporting agency offers the option to consumers to request a temporary unlocking of the freeze through Internet and telephonic methods, the freeze must be placed within 15 minutes after the consumer's request is received by the agency during normal business hours.

Consumer reporting agencies may charge a fee of \$5 to place the original security freeze or to temporarily unlock the freeze. However, victims of identity theft with a valid police report or investigative complaint may not be charged.

Statute: §44-1698:

<http://www.azleg.gov/FormatDocument.asp?inDoc=/legtext/48leg/2r/bills/sb1185s.htm>

Security Breaches: State law requires businesses and state and local government agencies (excluding law enforcement agencies, prosecution agencies, and courts) 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. If a business or agency becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes an individual's personal information, it must conduct a reasonable investigation to promptly determine if there has been a breach in the security system. If so, it must notify consumers in the most expedient manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the nature and scope of the breach or to identify the individuals affected or to restore the reasonable integrity of the data system. A business or agency is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur.

A security breach is defined as "an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by a person as part of a database of personal information

regarding multiple individuals and that causes or is reasonably likely to cause substantial economic loss to an individual.”

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 the data element is not encrypted, redacted, or secured by any other method rendering the element unreadable or unusable: Social Security number; driver's license or nonoperating identification license number; or a 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. Publicly available information is not included.

Notification can be provided to the affected persons by mail, e-mail, or by telephone. If the cost of providing regular notice would exceed \$50,000, the amount of people to be notified exceeds 100,000, or the 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 business's web site, and notification to major statewide media.

Statute: §44-7501:

<http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/44/07501.htm&Title=44&DocType=ARS>

Fraud Fight Accounts: Arizona has launched a program to provide Fraud Fight Accounts to consumers most vulnerable to identity theft due to disabilities, health issues, or because their financial security was already compromised. The accounts, offered by participating banks and credit unions, allow consumers to choose among several options to protect their accounts. The options include:

- Limiting daily and monthly withdrawals.
- Notifying a trusted third party if suspicious transactions are attempted.
- Delaying suspicious transactions.
- Limiting electronic access to accounts.

These options help keep people from becoming victims of high-pressure sales, financial scams, overreaching by caregivers and family, or identity theft, and work best for people who have consistent expenses.

For more information: <http://www.azag.gov/consumer/FraudFighterAccounts/index.html>

Brochure: “Fraud Fight Accounts”

(<http://www.azag.gov/consumer/FraudFighterAccounts/index.html>)

State Resources:

Office of the Attorney General: “Stop Identity Theft”
(http://www.azag.gov/cybercrime/ID_Theft.html)

“Credit Freeze Information”
(<http://www.azag.gov/messages/CreditFreezesCanPreventIdentityTheftDec2007.html>)

Brochure: “Protect Yourself Against Identity Theft”
(<http://www.azag.gov/cybercrime/IDTheftBrochure.pdf>)

This comprehensive document includes prevention tips and instructs victims of identity theft to: *“File a report with your local police department and, if the identity theft did not take place within your area, file a report with the police from the area where the theft took place. Make sure to get a copy of the police report. You may need that documentation to support your claims to credit bureaus, creditors, debt collectors or other companies. If you are unable to obtain a copy of the police report, be sure to get the report number.”*

Office of Crime Victims Services, Department of Public Safety: “Identity Theft”
(<http://www.azvictims.org/identity/default.asp>)

This document contains prevention tips and directs victims to: *“Contact the police immediately and file a report.”*

Tempe, Arizona, Police Department: “Identity Theft Victim’s Packet”
(<http://www.tempe.gov/police/forms/id%20Theft%20packet.pdf>)

This comprehensive document is from the Tempe Police Department, and is intended for victims from that jurisdiction who have already filed a police report. It is an extremely useful document for all identity theft victims in the state, and includes checklists, sample forms, and contact information for relevant government agencies and credit reporting agencies.

Legislation:

2008:

SB 1185 allows all Arizona 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.

HB 2587 requires creditors to verify a consumer’s address before extending credit if the address differs from the one on record and verify the identity of a consumer if they do not use consumer credit reports.

Under **HB 2321**, someone who believes his or her identity has been stolen may ask a judge for expedited determination of innocence, if the theft causes the person to be falsely arrested or blamed for fraud.

2007:

Starting January 1, 2009, **SB 1169** will require county recorders from a county with a population of more than 800,000 people to automatically redact references to complete 9-digit Social Security numbers (SSN) that are available on the recorder's website. SSNs may be retained on instruments that are not available on a website. They must also redact SSNs from documents that are posted from now on. For counties with a population less than 800,000, the bill requires a county recorder to redact references to a 9-digit SSN on the website at the request of the holder of the SSN. They must also redact SSNs on all future documents before placing them on the website

Online documents typically found on recorder sites include house deeds, court proceedings, liens and death certificates. Many include Social Security numbers, which are coveted by identity thieves. This bill builds on legislation passed last year requiring that Social Security numbers be removed from any new documents posted.

2006:

SB 1338 requires companies to notify consumers if a security breach puts unencrypted sensitive personal information at risk of identity theft. It covers unencrypted computerized personal data, including Social Security numbers and numbers for driver licenses, credit cards and financial accounts. The notification would have to include a description of the breach and of steps taken in response. Notifications can be delayed if a law enforcement agency decides that notification would impede criminal proceedings. Violations would be subject to civil proceedings leading to compensation for damages incurred and a civil penalty of up to \$10,000 per breach.

HB 2484 seeks to prevent identity theft by restricting how businesses dispose of paper records with confidential information about individuals. The bill prohibits businesses from knowingly discarding paper records or documents with sensitive identifying data without first redacting the data or shredding or otherwise destroying the documents. It applies to data that includes a person's name and Social Security, driver's license and financial account numbers. Violations would be punishable by a civil penalty of \$500 for the first offense, \$1,000 for a second and \$5,000 for each subsequent one.

HB 2024 requires government agencies to establish procedures ensuring that collected entity identifying information and personal identifying information, except public records, cannot be accessed by unauthorized persons.

2005:

SB 1058 creates the crime of aggravated identity theft if a person knowingly takes, purchases, manufactures, records, possesses or uses personal identifying information of either: five or more persons or entities or a person or entity and causes a loss to a person/entity of \$3,000 or more. Under the bill, proof of possession of the personal/entity identifying information of five or more persons/entities out of the course of regular business may give rise to an inference that the information was possessed for an unlawful purpose. It is a class 3 felony.

The bill also creates the crime of trafficking in the identity of another person or entity if a person knowingly sells, transfers or transmits personal/entity identifying information (real or fictitious)

for an unlawful purpose or to cause loss, whether the person or entity actually suffers any economic loss. It is a class 2 felony.

SB 1447 targets phishing scams, in which identity thieves try to trick consumers out of personal information by sending fraudulent e-mails, purporting to originate from a familiar institution, such as a bank. The bill makes it a class 5 felony, punishable by 1.5 years in jail and/or a \$150,000 fine, to impersonate an online business or financial institution to fool consumers into providing personal financial information. Specifically, it prohibits the solicitation of an individual's identifying information via a web page or e-mail by a person representing they are an on-line business who has not been approved to do so by the business they are representing. In addition to the criminal penalty, violators may be targeted in a civil action. The attorney general, Internet service providers, or a person who owns a Web site or trademark that has been adversely affected may bring an action to stop further violations, and recover the greater of actual damages or \$500,000 for each violation. If the court determines there is a pattern of violations, damages can be trebled (multiple violations resulting from one act are a single violation).

HB 2414 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.

The bill allows the attorney general and a computer software provider or a Web site or trademark adversely affected to bring action against a violator to stop further violations or recover the greater of actual damages or \$100,000 for each separate violation. The court may increase the damages up to three times if the defendant has a pattern of violating the provisions of the bill, and may also award costs and reasonable attorney fees to the prevailing party.

2004:

HB 2116 expands the crime of identity theft in several ways. The bill:

- Provides that a person commits criminal possession of a forgery device if the person makes or possesses any material, good, property or supply designed or adapted for use in forging written instruments or with the intent to aid or permit another person to use it for the purpose of forgery.
- Expands the definition of taking the identity of another person to include purchasing, manufacturing, recording or transmitting any personal identifying information.
- Provides that it is unlawful for a person to intentionally or knowingly make or possess with the intent to commit fraud
- Allows prosecutors to consolidate identity theft crime complaints against one defendant concerning identity theft crimes committed in different precincts or counties so that all the complaints can be heard in only one court.

The bill also requires a peace officer to take a report on the request of any person or entity whose identity has been taken in any jurisdiction in which that person resides or entity is located. It

also allows the peace officer who took the identity theft report to provide the report to any other law enforcement agency located in a jurisdiction in which an element or a result of the identity theft crime was committed or occurred. The bill also prohibits companies from using Social Security numbers on cards required for services, such as health insurance cards.

2003:

HB 2429 restricts the use of Social Security Numbers (SSNs). It makes it unlawful for a person or entity to: communicate an individual's SSN and make it available to the general public; print an individual's SSN on any card required for the individual to receive products or services provided by the person or entity; require an individual's SSN over the Internet unless the connection is secure or the SSN is encrypted; require the transmission of an individual's SSN to access an Internet web site, unless a password or unique identification is also required to access the Internet site; or print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document.

2002:

SB 2282 clarifies that identity theft may occur whether or not a victim suffers any economic loss because of the offense.