



# Arizona State Senate Issue Paper

September 26, 2008

## Note to Reader:

The Senate Research Staff provides nonpartisan, objective legislative research, policy analysis and related assistance to the members of the Arizona State Senate. The *Research Briefs* series, which includes the *Issue Brief*, *Background Brief* and *Issue Paper*, is intended to introduce a reader to various legislatively related issues and provide useful resources to assist the reader in learning more on a given topic. Because of frequent legislative and executive activity, topics may undergo frequent changes. Additionally, nothing in the *Brief* should be used to draw conclusions on the legality of an issue.

## **IDENTITY THEFT AND CONSUMER PROTECTION**

### **INTRODUCTION**

Identity theft and identity fraud refer to crimes in which an individual's personal information, such as the individual's name, Social Security number (SSN), credit card number or other identifying information, is fraudulently obtained for use by another person.

Nationally, identity theft is one of the fastest growing crimes. The Federal Trade Commission (FTC) estimates that as many as nine million Americans have their identities stolen each year. The most common identity theft complaints relate to credit card fraud, phone or utilities fraud, bank fraud and employment-related fraud. According to the FTC, more than 27 million people have been victims of identity theft in the last five years, costing them \$5 billion and businesses and financial institutions almost \$48 billion.

In May 2006, President George W. Bush created an Identity Theft Task Force to develop a comprehensive national strategy to combat identity theft. In September 2006, the Task Force made seven interim recommendations. Generally, the Task Force's recommendations related to data breach guidelines for governmental agencies, data security, governmental response to data breaches, developing a universal police report for identity theft victims, allowing federal identity theft victims to recover for the value of the time that they spent attempting to rectify the identity theft, reducing access to SSNs and developing alternative methods for authenticating an individual's identity.

### **IDENTITY THEFT**

Federal law prohibits knowingly transferring or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law. State laws relating to identity theft vary in the definition of the offense.

In Arizona, identity theft is defined as knowingly taking, purchasing, manufacturing, recording, possessing or using any personal identifying information or entity identifying information of another, including a real or fictitious person or

entity, without consent, with the intent to obtain or use the identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense, or with the intent to obtain or continue employment. Arizona classifies identity theft as a class 4 felony.

Arizona also penalizes other acts of identity theft. A person commits knowingly accepting the identity of another person, a class 4 felony, if the person, in hiring an employee, knowingly accepts from an individual another person's personal identifying information knowing that the individual is not the actual person identified by that information and uses that information to determine if the individual is authorized to work in the U.S. Aggravated identity theft, a class 3 felony, occurs when a person commits identity theft that results in an economic loss of \$3,000 or more or commits identity theft against three or more persons or entities or against another person with the intent to obtain employment. Additionally, trafficking in identities is penalized as a class 2 felony. The identity theft statutes do not apply to a person under the age of 21 utilizing a forged identification to purchase or consume alcohol or gain admittance to an age restricted venue. Arizona law also protects against identity theft by protecting against credit card fraud.

### ***PROTECTING YOUR SSN: FEDERAL LAW***

A SSN is a unique nine-digit personal identifier issued by the Social Security Administration to an individual. An individual's SSN is used as a unique identifier primarily for taxation purposes. Government agencies and businesses also use SSNs to identify and track service use and financial activities.

While there is no federal law that universally addresses the use of SSNs by public and private entities, there are several federal laws that address the use and disclosure of SSNs by specific industries. For example, the Social Security Number Confidential Act of 2000 prohibits the appearance of SSNs on or through unopened mailings of checks or other drafts issued on public money in the Treasury.

The Intelligence Reform and Terrorism Prevention Act of 2004, applicable to documents issued after December 17, 2005, restricts the issuance of replacement Social Security cards to three per year and ten in a lifetime and establishes minimum standards for verification of documents submitted to establish eligibility for Social Security cards. It also prohibits any government from displaying SSNs or any derivative on driver licenses, motor vehicle registrations or other identification documents issued by any department of motor vehicles.

### ***PROTECTING YOUR SSN: ARIZONA LAW***

Arizona law prohibits a person or entity from doing the following: 1) intentionally communicating or making an individual's SSN available to the public; 2) printing an individual's SSN on any card required for the individual to receive goods or services from the person or entity; 3) requiring an individual to transmit the individual's SSN over an unsecured Internet connection; and 4) requiring the use of an individual's SSN as an Internet password without some other kind of authentication device. Statute prohibits documents or records that are recorded and made available on an entity's public website from containing more than five numbers that are identifiable as part of the person's SSN. Beginning January 1, 2009, a person or entity may not knowingly print any sequence of more than five numbers that are reasonably identifiable as part of an individual's SSN on any card required to receive products or services or on any materials mailed to the individual, with certain exceptions.

Statute allows state agencies to use or disseminate the last four digits of an individual's SSN; however, the Department of Revenue and state and local law enforcement agencies are authorized to utilize the full number, with some exceptions. Statute also allows the use of SSNs by state agencies for the administration of payroll and workers' benefits, with some exceptions.

In 2007, legislation was enacted requiring recorders from counties with populations over 800,000 persons to redact references to complete

nine-digit SSNs that are, or will be, available on their county website. Similarly, recorders from counties with populations less than 800,000 persons must redact references to complete nine-digit SSNs that are, or will be, available on their county website at the holder's request.

The Attorney General or a county attorney may commence a legal action for a violation of the SSN use statutes.

In addition to those statutes pertaining directly to SSNs, other statutes limit the use of SSNs by specific entities. Universities are prohibited from assigning an individual identification number that is identical to the individual's SSN, and community colleges are required to assign an identification number different from a student's SSN upon request. Additionally, a university or community college may not display any four or more consecutive numbers of an individual's SSN on any university Internet site or other publicly accessible document. Schools may still electronically transfer student transcripts to other schools.

The Arizona Department of Real Estate prohibits the release of a licensee's SSN for inspection by any person other than the court or a government agency; and any employee of the Department of Economic Security (DES) who discloses personal information, including a SSN, collected by DES for a specified purpose without authorization may be subject to a \$1,000 civil penalty, in addition to other sanctions.

#### ***OTHER ARIZONA LAWS AIMED AT PROTECTING CONSUMERS AGAINST IDENTITY THEFT***

##### ***Security Breach***

In February 2005, ChoicePoint, a corporation that collects and compiles consumer information, including personal and financial information, disclosed that it had been the victim of a security breach. In this case, the personal identifying information of approximately 145,000 people was sold to a criminal enterprise. At first, the corporation only disclosed the breach to California residents as required by California state law. However, the corporation

later disclosed that residents in other states may have been affected by the security breach. Breaches of security at corporations, government agencies and educational institutions have since been reported, such as breaches at Card Systems, Western Illinois University and the United States Department of Veterans Affairs. These instances have led many states, including Arizona, to enact legislation requiring that companies and/or state agencies disclose to consumers information about security breaches of personal information.

When a person, business or governmental entity conducting business in Arizona that owns or licenses unencrypted computerized data, which includes personal information, becomes aware of an incident of unauthorized access to unencrypted or unredacted computerized data, it is required to conduct an investigation to promptly determine if a security breach has occurred. Personal information is defined as a person's first name or first initial and last name in combination with the individual's SSN, driver license or nonoperating identification license, or financial account number or credit or debit card number with the required access code. These notification requirements apply to a natural person, business entity or a governmental entity. If the person or entity determines that a security breach has occurred, the person is required to notify the affected Arizona residents.

Notification must be made in the most expedient manner possible without unreasonable delay subject to the needs of law enforcement. The notification is required to be made either in written, electronic or telephonic means or provided by a substitute notice if specified requirements are met.

A breach in security that may result in personal identifying information being obtained does not necessarily mean that an individual whose information may have been accessed is a victim of identity theft. A security breach notification is a precaution to alert consumers that their personal information has been breached and they should closely monitor their consumer activity.

## ***Destruction of Documents***

A business or governmental entity is prohibited from knowingly discarding or disposing of paper records or paper documents without redacting the information or destroying the records or documents if they contain an individual's first and last name or first initial and last name in combination with a corresponding complete:

1. SSN.
2. credit card, charge card or debit card number.
3. retirement account number.
4. savings, checking or securities entitlement account number.
5. driver license number or nonoperating identification license number.

Also, in response to concerns that personal information, which could be used to commit identity theft, was inadvertently available to the public after a consumer transaction, state law requires that no more than the last five digits of a credit card account number or the credit card expiration date may be printed on the credit card receipt provided to the cardholder if the receipt is electronically printed. A violation is a violation of the Consumer Fraud Act.

## ***Documents Obtained by Governmental Entities***

Many documents are recorded with various governmental entities and are available online. In order to protect consumers' personal information, beginning January 1, 2005, it is prohibited to record to a public website documents or records that contain any of the following personal identifying information of an Arizona resident: 1) more than five digits of a SSN; 2) credit card, charge card or debit card numbers; 3) retirement account numbers; or 4) savings, checking or securities entitlement account numbers. The Attorney General or a county attorney, or both, may initiate legal action for a violation. There is a civil penalty of up to \$500 for each act of recording personal identifying information, but statute limits the

penalties to the person or entity that authorizes the creation of the documents for recording.

## ***Disclosure of Confidential Information***

Current and former employees of county treasurers are prohibited from disclosing confidential information except: 1) with written authorization; 2) to a taxpayer's licensed title company; 3) pursuant to a court order or a subpoena; and 4) to the state Auditor General pursuant to an official audit. Confidential information includes images of checks and banking information used for the payment of property taxes.

## ***Retailer Use of Identification Information***

A retailer may retain and use information from a customer's state issued identification only for the following purposes: 1) establishing the customer's identity; 2) verifying the customer's age; 3) confirming that the customer is properly licensed to operate a vehicle; 4) disclosing the information to specified persons and entities or to a law enforcement agency for a law enforcement investigation; or 5) in a court or administrative proceeding. A violation is a violation of the Consumer Fraud Act and the Attorney General or a county attorney may initiate legal action. There is a civil penalty, not to exceed \$500 for a first violation, \$1,000 for a second violation and \$5,000 for a third or subsequent violation, for each violation.

## ***Extension of Credit***

In 2008, Arizona enacted legislation that prohibits any person, who does not use a consumer credit report in the approval of a credit application, from lending money or extending credit without taking reasonable steps to verify the consumer's identity and confirm that the application for extension of credit is not the result of identity theft or aggravated identity theft. The same reasonable steps and identity verification requirements are also required when a credit report is used during the credit approval process if the creditor has received notification that either: 1) a police report has been filed with a consumer reporting agency and that the applicant has been a victim of identity theft; or

2) the consumer has placed a fraud alert or security freeze on the consumer's credit report.

## ***Pretexting***

According to the FTC, pretexting is the practice of obtaining personal information under false pretenses. Pretexters sell personal identifiers to others who may use it to obtain credit in another person's name, steal assets or investigate or sue another person. For example, data brokers have fraudulently gained access to telephone records by posing as the customer, then offering the records for sale on the Internet without the customer's consent or knowledge.

A person is prohibited from knowingly procuring, selling or receiving a telephone record, public utility record or communication service record of any Arizona resident without the resident's authorization, with specific exceptions. Additionally, entities that maintain communication service records, telephone records and public utility records must establish reasonable procedures to protect against unauthorized or fraudulent disclosure of such records. Any violation of the requirements is a violation of the Consumer Fraud Act and is a class 1 misdemeanor. For a civil action, a person is entitled to receive at least \$1,000 in damages, appropriate relief and reasonable attorney's fees and costs.

## ***Protections on the Internet***

Phishing is a form of online identity theft that uses spoofed electronic mail messages (emails) designed to lure recipients to fraudulent websites that attempt to trick them into divulging personal financial data such as credit card numbers, account usernames passwords and SSNs.

In Arizona, solicitation of an individual's identifying information via a web page or email by a person falsely representing an online business is prohibited and is a class 5 felony. The Attorney General or a person who either is engaged in the business of providing Internet access service to the public or owns a web page or trademark and who is adversely affected by the unauthorized solicitation may institute an action against violators to stop them from

conducting any further phishing and/or to recover actual damages or \$500,000 for each separate violation, whichever is greater. The court may increase the damage award up to three times for an established pattern and practice of unauthorized solicitation.

According to the FTC, computer software known as spyware can be installed on a computer without the owner or operator's consent. The spyware software then monitors or controls computer use and can be used to send pop-up ads, redirect the computer to particular websites, monitor Internet surfing or record keystrokes, which, in turn, could lead to identity theft. In October of 2004, the FTC filed its first spyware case against a company, alleging the company acted unfairly in downloading software without any notice or authorization.

In Arizona, it is unlawful for a person to transmit spyware to a computer the person does not own or operate in order to modify, through intentionally deceptive means, computer software or settings or to collect personal identifying information of the computer owner or operator. The spyware statutes preempt all rules, regulations, codes, ordinances and other laws adopted regarding spyware, and the Attorney General and others may bring action against a person who violates the computer spyware provisions to recover the greater of actual damages or \$100,000 for each separate violation. The court may increase the damages up to three times the allowed amount if a pattern and practice of violating the provisions can be established.

Unsolicited commercial email (UCE), also known as unsolicited bulk mail, junk mail or spam, is regulated in Arizona. The transmission of commercial emails that contain false information regarding the origin of the message or content is prohibited. The first characters on the subject line of a UCE must be the characters "ADV." A person who sends UCE or maintains a database for the purpose of sending UCE must provide a free procedure for recipients to remove themselves from the sender's email address list and must restrict the future sale of their email address information. The sender of UCEs is

allowed three business days to remove a recipient's email address from the list.

The following is permitted, however: 1) commercial emails if there is an established business relationship; 2) damages to be collected by a person or email service provider if injured as a result of intentional transmission of UCE; and 3) establishment and enforcement of an email service provider's company policies to block the receipt or transmission of commercial email advertisements that it believes are sent or will be sent in violation of the law. It is a class 2 misdemeanor to violate the statutes governing commercial email.

Additionally, unsolicited faxes have been common in the past. In Arizona, each unsolicited commercial fax advertisement is required to include the name, address, fax number and toll free or local contact telephone number of the vendor that sends the fax. A person who receives unsolicited commercial faxes from a vendor after requesting that no further faxes be sent may charge the vendor \$5 for each faxed page received after a three-day grace period. This does not alter or restrict the rights of a person to recover damages for the sending of an unsolicited commercial fax advertisement under federal law.

## ***Security Freeze***

In 2008, Arizona enacted legislation to establish procedures and requirements for consumers to request, and a credit reporting agency to place or lift, a security freeze on a consumer's credit report. The legislation requires consumer reporting agencies to place a security freeze on a consumer's credit report or score within ten business days of receiving a written request from the consumer. It further requires the agency to send notification to the consumer that a freeze has been placed, along with a personal identification number so that the consumer may gain access to a frozen report or score. Additionally, it prohibits a consumer reporting agency from charging more than five dollars to place, remove or lift a security freeze.

## ***Victim Recourse***

In 2008, legislation was enacted that establishes procedures for judicial determinations of factual innocence or factual improper party status to aid identity theft victims with clearing their name in legal matters resulting from a stolen identity. Beginning January 2, 2009, identity theft victims may petition the superior court for a judicial determination hearing, if their personal identifying information was taken and used by another person who was implicated in a criminal offense or the name was entered into a judgment on record in a criminal case or civil action. Upon a finding of factual innocence in a criminal case or a finding of improper party status in a civil case, the court must notify applicable legal and law enforcement personnel and provide the victim with a copy of the court order.

## ***ADDITIONAL RESOURCES***

- Federal Trade Commission  
[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)
- National Consumer Protection Week, Identity Theft  
[www.consumer.gov/ncpw/index.htm](http://www.consumer.gov/ncpw/index.htm)
- Phoenix Police Department, Identity Theft  
<http://phoenix.gov//POLICE/dcd1.html>
- National Conference of State Legislatures  
[www.ncsl.org/programs/lis/privacy/idtheft.htm](http://www.ncsl.org/programs/lis/privacy/idtheft.htm)
- Arizona Motor Vehicle Division (to remove a SSN from a driver's license)  
<http://www.azdot.gov/mvd/index.asp>
- U.S. Social Security Administration  
[www.socialsecurity.gov](http://www.socialsecurity.gov)
- U.S. General Accounting Office  
[www.gao.gov](http://www.gao.gov)
- Free annual credit report from each company  
[www.annualcreditreport.com](http://www.annualcreditreport.com)
- Equifax  
[www.equifax.com](http://www.equifax.com)

- TransUnion  
[www.transunion.com](http://www.transunion.com)
- Experian  
[www.experian.com](http://www.experian.com)
- National Do Not Call Registry  
[www.donotcall.gov](http://www.donotcall.gov)
- FTC website on Spam  
<http://www.ftc.gov/spam/>
- Consumer Sentinel  
<http://www.ftc.gov/sentinel/>
- The Driver's Privacy Protection Act of 1994: 18 U.S.C. §§ 2721 to 2725
- Fair and Accurate Transaction Act of 2003: 15 U.S.C. §§ 1681 *et seq.*; 20 U.S.C. §§ 9701 *et seq.*
- Fair Credit Reporting Act: 15 U.S.C. §§ 1681 *et seq.*
- The Gramm-Leach Bliley Act of 1999: 12 U.S.C. §§ 24a, 248b, 1820a, 1828b, 1831v to 1831y, 1848a, 2908, 4809; 15 U.S.C. §§ 80b-10a, 6701, 6711 to 6717, 6731 to 6735, 6751 to 6766, 6781, 6801 to 6809, 6821 to 6827, 6901 to 6910
- The Health Insurance Portability and Accountability Act of 1996: 18 U.S.C. §§ 24, 669, 1035, 1347, 1518, 3486; 26 U.S.C. §§ 220, 4980C to 4980E, 6039F, 6050Q, 7702B, 9801 to 9806; 29 U.S.C. §§ 1181 to 1187; 42 U.S.C. §§ 300gg, 300gg-11 to 300gg-13, 300gg-21 to 300gg-23, 300gg-41 to 300gg-47, 300gg-91, 300gg-92, 1320a-7c to 1320a-7e, 1320d, 1320d-1 to 1320d-8, 1395b-5, 1395ddd
- Identity Theft Penalty Enhancement Act: 18 U.S.C. §§ 1028 *et seq.*
- Arizona Forgery and Related Offenses, including Identity Theft, Statutes: A.R.S. Title 13, Chapter 20
- Arizona Credit Card Statutes: A.R.S. Title 13, Chapter 21
- Arizona Internet Representations Statutes: A.R.S. Title 44, Chapter 29
- Arizona Confidentiality of Personal Identifying Information Statutes: A.R.S. Title 44, Chapter 9, Article 17
- Arizona Telephone, Utility and Communication Service Records Statutes: A.R.S. Title 44, Chapter 9, Article 20
- Arizona Retailer Use of Identification Information Statutes: A.R.S. Title 44, Chapter 34
- Consumer Credit Statutes; Arizona Revised Statutes, Title 44, Chapter 11, Article 6, and A.R.S. § 44-1698