



Arizona State Senate Issue Brief

September 13, 2016

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 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 personally identifiable information, is fraudulently obtained for use by another individual or entity.

Nationally, identity theft is one of the fastest growing crimes. According to the U.S. Department of Justice (DOJ) Bureau of Justice Statistics (BJS), an estimated 17.6 million people nationwide were victims of identity theft in 2014 resulting in \$15.4 billion in financial losses.¹ The Federal Trade Commission (FTC) states that identity theft was its top complaint category in 2014. According to FTC data, Florida had the highest per capita rate of reported identity theft complaints in the country; Arizona had the ninth highest. One out of every six Arizona residents reported being a victim of an identity theft-related crime, according to the Arizona Criminal Justice Commission's (ACJC) *2013 Arizona Crime Victimization Survey* – a larger percentage than any other victimization type in the survey.²

The most common identity theft complaints relate to credit card fraud, government documents or benefits fraud, phone or utilities fraud, bank and loan fraud, and employment-related fraud.

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.³ According to the DOJ, such an offense is subject to a maximum of 15 years in prison along with a fine and criminal forfeiture of any personal property used or intended to be used to commit the offense. State laws relating to identity theft vary in the definition of the offense.

¹ U.S. Department of Justice Bureau of Justice Statistics, [Victims of Identity Theft, 2014](#)

² Arizona Criminal Justice Commission, [The 2013 Arizona Crime Victimization Survey](#)

³ Public Law 105-318

Arizona law defines identity theft as knowingly taking, purchasing, manufacturing, recording, possessing or using any personal identifying information or entity identifying information of another person or entity, including a real or fictitious person or entity, without consent. It is illegal to obtain or use that identity for any unlawful purpose or to cause loss to a person or entity whether or not that person or entity actually suffers any economic loss as a result of the offense, or with the intent to obtain or continue employment. Taking the identity of another person or entity is a class 4 felony. Arizona law also penalizes other acts of identity theft. For instance, a person commits a class 4 felony if, in the process of hiring an employee, they knowingly accept falsified information and use it to determine if the individual is authorized to work in the U.S.⁴

Aggravated identity theft, a class 3 felony, occurs when a person commits identity theft resulting in an economic loss of \$1,000 or more or commits identity theft against three or more persons or entities or against another person with the intent to obtain employment.⁵

Additionally, trafficking in identities is a class 2 felony. The identity theft statutes do not apply to persons under the age of 21 who use forged identification to purchase alcohol or access age restricted venues.⁶ Arizona law also protects against identity theft by targeting credit card fraud and allowing individuals to place security freezes on their or their children's credit reports or credit scores in instances of fraud.^{7,8,9}

Protecting Your SSN: Federal Law

An SSN is a unique nine-digit personal identifier issued by the Social Security Administration to an individual 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 universally addressing 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 Confidentiality 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.¹⁰

The Intelligence Reform and Terrorism Prevention Act of 2004, applicable to documents issued after December 17, 2005, restricts issuance of replacement Social Security cards to three per year and 10 in a lifetime and establishes minimum standards for document verification to obtain a Social Security card. It also prohibits any government agency from displaying SSNs or any derivative on driver licenses or other forms of identification issued by a department of motor vehicles.¹¹

The Identity Theft Penalty Enhancement Act of 2004 establishes penalties for aggravated identity theft. It prescribes sentences, which are to be imposed in addition to punishments already provided for related felonies, as follows: 1) two years of imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations; and 2) five years of imprisonment for knowingly taking such action with respect to a means of identification or a false identification document during and in relation to specified felony violations pertaining to terrorist acts.¹²

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 products or services from the person or entity; 3) requiring an individual to transmit their 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.¹³

⁴ A.R.S. § 13-2008

⁵ A.R.S. § 13-2009

⁶ A.R.S. § 13-2010

⁷ A.R.S. § 13-2102

⁸ A.R.S. § 44-1698

⁹ A.R.S. § 44-1698.02

¹⁰ Public Law 106-433

¹¹ Public Law 108-458

¹² Public Law 108-275

¹³ A.R.S. § 44-1373

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.¹⁴

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 use the full number, with exceptions. Statute also allows the use of SSNs by state agencies for administering payroll and workers' benefits, with exceptions.^{15,16}

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.¹⁷

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, for instance, 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. The electronic transfer of

student transcripts between educational institutions, however, is permitted.¹⁸

OTHER ARIZONA LAWS AIMED AT PROTECTING CONSUMERS AGAINST IDENTITY THEFT

Security Breach

In February 2005, ChoicePoint, a company that collected and compiled 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 163,000 people was sold to a criminal enterprise. At first, the company only disclosed the breach to California residents as required by California state law. However, the company later disclosed that residents in other states may have also been affected. Numerous breaches of security at corporations, government agencies and educational institutions have since been reported. A 2013 data breach affecting Target Corporation stores, for instance, resulted in as many as 70 million people having their personal data, including credit and debit card information, stolen. In the same year, the Maricopa County Community College District also became the target of a large security breach, compromising the personal and financial data of over 2 million people and resulting in a cost of more than \$26 million to taxpayers to deal with the aftermath.

Such instances have led many states, including Arizona, to enact legislation requiring that companies and government 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 identifying 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.¹⁹ Personal identifying information is any written document or electronic data that does or purports to provide

¹⁴ A.R.S. § 44-1373.02

¹⁵ A.R.S. § 44-1373

¹⁶ A.R.S. § 44-1373.01

¹⁷ A.R.S. § 11-461

¹⁸ A.R.S. § 15-823

¹⁹ A.R.S. § 18-545

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 and other sensitive information. 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.

A breach in security 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 that 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; or 5) driver license number or nonoperating identification license number.²⁰

Also, in response to concerns that sensitive personal information 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. Failure to comply is a violation of the Arizona Consumer Fraud Act.²¹

²⁰ A.R.S. § 44-7601

²¹ A.R.S. § 44-1367

Documents Obtained by Governmental Entities

Many documents are recorded with various governmental entities and are available online. In order to protect consumers' personal information, 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 unless: 1) there is written authorization; 2) it is to a taxpayer's licensed title company; 3) it is pursuant to a court order or a subpoena; or 4) it is pursuant to an official audit by the Office of the Auditor General. Confidential information includes images of checks and banking information used for the payment of property taxes.²²

Retailer Use of Customer 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. While either the Attorney General or a county attorney may initiate a legal action for a violation of this statute, only the Attorney General may enforce it as a violation of the Arizona Consumer Fraud Act. There is a civil penalty, not to exceed \$500

²² A.R.S. § 11-505

for a first violation, \$1,000 for a second violation and \$5,000 for a third or subsequent violation.²³

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. A consumer credit report is the record of an individual's credit history, including credit card accounts, revolving credit accounts, borrowing and payment history, credit inquiries and credit limits. Additional information typically contained in the report consists of past and present residences of the consumer, whether the consumer has been sued or arrested and any bankruptcy filings by the consumer. Companies that gather and sell such information are called consumer reporting agencies; the three main agencies are Equifax, Experian and Trans Union.

The same reasonable steps and identity verification requirements apply 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 their credit report.²⁴

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.

With specific exceptions, a person is prohibited from knowingly procuring or selling a telephone record, public utility record or communication service record of any Arizona resident without the resident's authorization. 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.²⁵

Protections on the Internet

Phishing is a form of online identity theft that uses spoofed 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, it is a class 5 felony to solicit an individual's identifying information via a web page or email by a person falsely representing an online business. 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 bring an action against violators. The court may increase the damage award up to three times for an established pattern and practice of unauthorized solicitation.

According to the FTC, scammers have often illegally installed computer software known as spyware 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

²³ A.R.S. § 44-7701

²⁴ A.R.S. § 44-1698.01

²⁵ A.R.S. § 44-1376.01

software or settings or to collect personal identifying information of the computer owner or operator.²⁶ The spyware statutes preempt all rules, regulations, codes, ordinances, and other laws adopted regarding spyware.²⁷ 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.²⁸

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.²⁹ It is a class 2 misdemeanor to violate statutes governing commercial email.³⁰

Security Freeze

A security freeze, also known as a credit freeze, allows an individual to control access to and dissemination of the individual's credit report by restricting the release of information without the consumer's express authorization. A credit freeze stops access to the credit report, blocking lenders and credit card issuers from viewing that information, effectively preventing new accounts from being opened. Because new accounts cannot be created, placing a credit freeze on a consumer report may prevent financial identity theft.

Equifax, Experian and TransUnion currently allow consumers to freeze their credit reports for a fee. All 50 states and the District of Columbia have enacted laws further regulating consumer reporting agencies when consumers request a security freeze to be placed on their credit reports.

In 2008, Arizona enacted legislation to establish procedures and requirements for consumers to request, and a consumer reporting agency to place or lift, a security freeze on a consumer's credit report. The law requires consumer reporting agencies to place a security freeze on a consumer's credit report or score within 10 business days of receiving a written request from that consumer. It further requires the agency to send confirmation 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 \$5 to place, remove, or lift a security freeze.

If a freeze is in place, the law prohibits a consumer reporting agency from changing a consumer's name, date of birth, Social Security number or address in the report without sending a written confirmation of the change within 30 days after the change is posted to the consumer's file.

There are several agencies and groups that may continue to access a credit report or score, even if it has been frozen by the consumer. These exceptions include state agencies, including the Department of Revenue, Department of Health Services, Department of Transportation, the Administrative Office of the Courts, Child Protective Services and any state or local agency, law enforcement agency, trial court or private collection agency acting pursuant to a court order.

The law also provides guidelines for consumers to remove or temporarily lift a freeze on a report. A frozen report would most likely result in a legitimate application for credit by the consumer to be denied by a third party, so the consumer may want to remove or temporarily lift the freeze in the future. A freeze must be removed or lifted within three business days of

²⁶ A.R.S. § 18-502

²⁷ A.R.S. § 18-503

²⁸ A.R.S. § 18-504

²⁹ A.R.S. § 44-1372.01

³⁰ A.R.S. § 44-1372.05

the reporting agency receiving the request by mail, and within 15 minutes (with some exceptions) when the request is received by telephone, Internet or other electronic contact method. Any violation of a security freeze requirement by a consumer reporting agency is classified as consumer fraud and is subject to enforcement through private action and the Attorney General through injunctive relief.³¹

Security Freeze for Minors and Incapacitated Persons

According to the National Conference of State Legislatures (NCSL), identity theft crimes involving minors have become more prevalent in recent years. A 2011 Carnegie Mellon University survey found that minors are 51 times more likely to become targets of identity theft than adults. As a result, at least 22 states, including Arizona, have enacted laws authorizing security freezes for minors and incapacitated persons for whom a guardian or conservator has been appointed.

Arizona's law, effective January 1, 2016, allows a security freeze to be placed on a protected person's record or credit report, provided that certain requirements are met. A protected person is someone who is: 1) under 16 years of age at the time a request for the placement of a security freeze is made; or 2) an incapacitated person or a protected person for whom a guardian or conservator has been appointed.

Under the law, a consumer reporting agency is prohibited from charging more than \$5 for each placement, or removal of a security freeze on a protected person's record or credit report. No fee may be charged if either of the following occurs: 1) the protected person's representative provides a copy of a police report to the consumer reporting agency alleging that the protected person has been a victim of identity theft; or 2) the request for the placement or removal of a security freeze is for a protected person who is under 16 years of age at the time the request is made and the agency has a credit report pertaining to that protected person.³²

ADDITIONAL RESOURCES

- Arizona Attorney General
<https://www.azag.gov/identity-theft>
- Arizona Criminal Justice Commission
http://www.azcjc.gov/acjc.web/pubs/home/azcvfs_finalreport_final.pdf
- Consumer Credit Statutes: Arizona Revised Statutes, Title 44, Chapter 11, Article 6
- Federal Trade Commission
www.ftc.gov/bcp/edu/microsites/idtheft/
- FTC, Consumer Sentinel Network
<https://www.ftc.gov/enforcement/consumer-sentinel-network>
- FTC, National Do Not Call Registry
<https://www.donotcall.gov/>
- FTC, OnGuardOnline.gov
<http://www.onguardonline.gov/>
- U.S. Bureau of Justice Statistics
<http://www.bjs.gov/index.cfm?ty=tp&tid=42>
- U.S. Department of Justice
<http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud>
- U.S. Social Security Administration
<http://oig.ssa.gov/report-fraud-waste-or-abuse/what-cant-oig-investigate/identity-theft>
- Equifax
http://www.equifax.com/home/en_us
- Experian
<http://www.experian.com/>
- TransUnion
<http://www.transunion.com/>
- Free annual credit report from each company
<https://www.annualcreditreport.com/index.action>

³¹ A.R.S. § 44-1698

³² A.R.S. § 44-1698.02