

UTAH

IDENTITY THEFT RANKING BY STATE: Rank 31, 57.8 Complaints Per 100,000
Population, 1529 Complaints (2007)
Updated December 30, 2008

Current Laws: A person is guilty of identity fraud when that person:

- Obtains personal identifying information of another person whether that person is alive or deceased; and
- Knowingly or intentionally uses, or attempts to use, that information with fraudulent intent, including to obtain, or attempt to obtain, credit, goods, services, any other thing of value, or medical information.

“Personal identifying information” may include name; birth date; address; telephone number; driver’s license number; Social Security number; place of employment; employee identification numbers or other personal identification numbers; mother’s maiden name; electronic identification numbers; electronic signatures; or any other numbers or information that can be used to access a person's financial resources or medical information except for numbers or information that can be prosecuted as financial transaction card offenses under the payment card fraud statutes.

It is not a defense that the person did not know that the personal information belonged to another person. Identity fraud is a second degree felony (punishable by up to 15 years in jail and/or a fine up to \$10,000) if the value of the credit, goods, employment, services, or any other thing of value is more than \$5000, and a third degree felony (punishable by up to five years in jail and/or a fine up to \$5000) if it is less than \$5000. It is also a second degree felony if the fraudulent use of personal identifying information results, directly or indirectly, in bodily injury to another person.

Multiple violations may be aggregated into a single offense, and the degree of the offense is determined by the total value of all credit, goods, services, or any other thing of value used, or attempted to be used, through the multiple violations.

Statute §76-6-1102: http://le.utah.gov/~code/TITLE76/htm/76_06_110200.htm

It is a Class A misdemeanor, punishable by up to a year in prison and/or a fine up to \$2500, to obtain, possess, or help another person obtain false identification documents. However, it becomes a third degree felony if a person obtains, possesses, or helps another person obtain multiple false identification cards.

Statute: §76-6-1105: http://le.utah.gov/~code/TITLE76/htm/76_06_110500.htm

Jurisdiction: Charges can be filed in the home county of a victim, even if the fraud was perpetrated in another Utah county or out of state. Charges can be filed where the victim’s personal identifying information was obtained; where the defendant used or attempted to use the personally identifying information; where the victim of the identity fraud resides or is found; or

if multiple offenses of identity fraud occur in multiple jurisdictions, in any county where the victim's identity was used or obtained, or where the victim resides or is found.

Statute: §76-1-202: http://le.utah.gov/~code/TITLE76/htm/76_01_020200.htm

Phishing: It is a second degree felony to use a computer for any scheme or artifice to obtain a person's sensitive personal identifying information by means of false or fraudulent pretenses, representations, or promises. The punishment does not depend, as it does in most fraud cases, on the amount of money lost. Sensitive personal identifying information includes an individual's Social Security number; driver's license number or other government issued identification number; financial account number or credit or debit card number; password or personal identification number or other identification required to gain access to a financial account or a secure website; automated or electronic signature; unique biometric data; or any other information that can be used to gain access to an individual's financial accounts or to obtain goods or services.

Statute: §76-10-1801(f): http://le.utah.gov/~code/TITLE76/htm/76_10_180100.htm

Payment Cards: It is unlawful for any person to:

- Knowingly, with intent to defraud, obtain or attempt to obtain credit or purchase or attempt to purchase goods, property, or services, by the use of a false, fictitious, altered, counterfeit, revoked, expired, stolen, or fraudulently obtained financial transaction card, by any financial transaction card credit number, personal identification code, or by the use of a financial transaction card not authorized by the issuer or the card holder; or
- Make application for a financial transaction card to an issuer, while knowingly making or causing to be made a false statement or report relative to his name, occupation, financial condition, assets, or to willfully and substantially undervalue or understate any indebtedness for the purposes of influencing the issuer to issue the financial transaction card.

Violations range from a class B misdemeanor to a second degree felony, based on the value of the property, money, or thing obtained or sought to be obtained.

Statute: §76-6-506.2: http://le.utah.gov/~code/TITLE76/htm/76_06_050602.htm

Under state law, it is a third degree felony, punishable by up to five years in prison and/or a fine up to \$5000, to:

- Acquire a financial transaction card from another without the consent of the card holder or the issuer, or, with the knowledge that it has been acquired without consent, and with intent to use it unlawfully;
- Receive a financial transaction card with intent to use it unlawfully;
- Sell or transfer a financial transaction card to another person with knowledge that it will be used unlawfully;
- Acquire a financial transaction card that the person knows was lost, mislaid, or delivered under a mistake as to the identity or address of the card holder; and retains possession with intent to use it unlawfully or sell or transfer it to another person with the knowledge that it will be used unlawfully; or
- Possess, sell, or transfer any information necessary for the use of a financial transaction card, including the credit number of the card, the expiration date of the card, or the personal identification code related to the card, without the consent of the cardholder or the issuer, or

with the knowledge that it has been acquired without consent, and with intent to use the information unlawfully.

Statute: §76-6-506.3: http://le.utah.gov/~code/TITLE76/htm/76_06_050603.htm

Scanning Devices: State law prohibits 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 without the authorization of the authorized user and with the intent 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 third degree felony. Second or subsequent offenses are a second degree felony.

Statute: §76-6-506.7: http://le.utah.gov/~code/TITLE76/htm/76_06_050607.htm

Driver's Licenses: It is a third degree felony, punishable by up to five years in prison, to use a fraudulent driver's license to aid or further efforts to fraudulently obtain goods or services or to aid or further the commission of a violent felony. It is a Class A misdemeanor, punishable by up to one year in jail, for an employee of the Driver License Bureau to knowingly issue a driver license with false or fraudulent information. It is a Class A misdemeanor to knowingly acquire, transfer, or use a false or altered driver license certificate to purchase tobacco or alcohol. It is a Class C misdemeanor to lend or knowingly permit another person to use your license; to use a license that is not yours; to knowingly make a false statement in an application for the license; to knowingly use or acquire a false identification card; or to alter any information on an authentic driver license certificate.

Statute: §53-3-229: http://le.utah.gov/~code/TITLE53/htm/53_03_022900.htm

Disposal of Customer Records: Businesses are required to destroy or arrange for the destruction of records containing personal identifying information before disposing of them. This can be done by shredding, erasing, or modifying the information to make it indecipherable.

Statute: §13-44-201: http://le.utah.gov/~code/TITLE13/htm/13_44_020100.htm

Social Security Numbers: State law prohibits a person from displaying a Social Security number in a manner or location that is likely to be open to public view. It also prevents state or local agencies to employ inmates in any capacity that would allow an inmate access to another person's personal information.

Statute: §13-45-3: http://le.utah.gov/~code/TITLE13/htm/13_45_030100.htm

Victim Assistance:

Restitution: State law requires judges to order defendants convicted of identity theft to make restitution to the victim(s) of the offense or state on the record the reason why the court does not find ordering of restitution to be appropriate. Restitution may include payment for any costs incurred, including attorneys fees, lost wages, and replacement of checks; and the value of the victim's time incurred due to the offense in clearing his/her credit record or credit record or in any civil or administrative proceedings necessary to satisfy or resolve any debt, lien, or other

obligation of the victim arising from the offense, or in attempting to remedy any other intended or actual harm to the victim incurred as a result of the offense.

Statute §76-6-1102: http://le.utah.gov/~code/TITLE76/htm/76_06_110200.htm

Security Freeze: All Utah 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. The credit reporting agency is not allowed to charge a fee to victims for placing, temporarily removing, or removing a security freeze on a credit report. To avoid paying a fee, victims must send a valid copy of a police report or provide the police docket number that documents identity fraud. For all others, a “reasonable fee” will be applied for placing, temporarily lifting a freeze, or removing a security freeze.

The reporting agency must place the freeze within five business days after receiving the request, and within five days after placing the freeze, 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 or within 15 minutes if the request is made through an electronic contact method or by telephone during normal business hours.

Statute: §13-45-101 through 205: http://le.utah.gov/~code/TITLE13/13_45.htm

“Credit Freeze” (<http://idtheft.utah.gov/news/story03/fullStory03.html>)

How To Apply for a Security Freeze:

<http://www.consumersunion.org/pdf/security/securityUT.pdf>

Security Breach: State law requires a person or business that owns or licenses computerized data that includes the personal information of a Utah resident to conduct a reasonable and prompt investigation of any breach of security to determine the likelihood that personal information has been or will be misused as a result of the breach. If, after the investigation is concluded, the business determines that misuse of an individual’s personal information has occurred or is reasonably likely to occur as a result of the breach of security, the business must notify the individual of the breach. A security breach occurs upon “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information.”

Personal information is defined as an person’s first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or the data element is unencrypted and not protected by another method that renders the data unreadable or unusable: Social Security number; financial account number, or credit or debit card number, and any required security code, access code, or password, that would permit access to the person’s account; or driver license number or state identification card number. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Notice must be made in the most expedient time possible without unreasonable delay, considering legitimate investigative needs of law enforcement; after determining the scope of the breach of system security; and after restoring the reasonable integrity of the system. Notification can be provided by mail, e-mail, telephone, or by publishing notice of the breach of system security in a newspaper of general circulation.

Statute: §13-44-202: http://le.utah.gov/~code/TITLE13/htm/13_44_020200.htm

Court Records: In any case in which a person commits identify fraud and uses the personal identifying information obtained to commit a crime in addition to the identity fraud, the court must make appropriate findings in any prosecution of such a crime that the person whose identity was falsely used to commit the crime did not commit the crime.

Statute: §76-6-1104: http://le.utah.gov/~code/TITLE76/htm/76_06_110400.htm

State Resources:

“Identity Theft Reporting Information System” (<http://idtheft.utah.gov/index.html>)
Victims in Utah can report identity theft crimes online through the Attorney General’s Office Identity Theft Reporting Information System: *“This is an official law enforcement web site from which all claims are reported to local, state or federal law enforcement agencies. Reporting a false claim is a crime and violations will be prosecuted to the fullest extent of the law.”*

“Report Identity Theft” (<http://idtheft.utah.gov/reportidtheft/index.html>)

“Education” (<http://idtheft.utah.gov/education/index.html>)

This page contains links to many useful and helpful resources, including fact sheets, sample letters, and information on credit reporting agencies:

- “What is Identity Theft?”
(http://idtheft.utah.gov/education/educationpages/whatisidentitytheft_001.html)
- “Step-By-Step Instructions”
(<http://idtheft.utah.gov/education/StepbyStepInstructions/index.html>)
This page contains information to assist individuals who are victims or suspect they may be victims of identity theft, depending on the situation and type of identity stolen.
- “Detect and Recover from Identity Theft”
(http://idtheft.utah.gov/education/educationpages/detectandrecoverfromidentitytheft_001.html)
- “Prevent Identity Theft”
(http://idtheft.utah.gov/education/educationpages/preventidtheft_001.html)
- “Social Security Number Identity Theft”
(http://idtheft.utah.gov/education/educationpages/requestasocialsecuritystatement_001.html)

Utah Department of Public Safety, “Identity Crime”
(http://publicsafety.utah.gov/investigations/id_theft.html)

“Identity Theft and Criminal Records” (<http://www.des.utah.gov/bci/IDtheft.html>)

“Identity theft is very much a part of our world today, and is growing at an alarming rate. The Bureau of Criminal Identification (BCI) is aware that there are many victims of identity theft and

out staff is willing to help those affected. Following are some steps that need to be taken to begin the process of removing your name or other identifying information from a criminal record at BCI.”

Legislation:

2008:

SB 52 will require judges to order defendants convicted of identity to make restitution to the victim(s) of the offense or state on the record the reason why the court does not find ordering of restitution to be appropriate. Restitution may include payment for any costs incurred, including attorneys fees, lost wages, and replacement of checks; and the value of the victim’s time incurred due to the offense in clearing his/her credit record or credit record or in any civil or administrative proceedings necessary to satisfy or resolve any debt, lien, or other obligation of the victim arising from the offense, or in attempting to remedy any other intended or actual harm to the victim incurred as a result of the offense.

The bill also adds a person’s birth date to the list of personal identifying information in the identity theft statute.

2007:

HB 432 requires the attorney general to maintain an Internet website to assist victims of identity-related crimes. The website will allow an identity theft victim to report the crime and have the crime routed to the appropriate law enforcement agency, and can be expanded to include additional services.

SB 140 provides that it is a second degree felony when a person fraudulently uses personal identifying information and then use results, directly or indirectly, in bodily injury to another person.

SB 15 authorizes the Department of Workforce Services to notify an individual about the suspected misuse of his personal identifying information, which is indicated by a Social Security number (SSN) under which wages are being reported by two or more individuals or that of a person under 16 with reported wages over \$1,000 for a single reporting quarter. The department may also notify the relevant law enforcement agency.

2006:

Under **SB 184**, if a person uses another party’s identifying information with fraudulent intent and to obtain anything of value, it is not a defense that the person did not know that the identifying information belonged to another person.

SB 52 targets phishing crimes, in which the Internet and e-mail is used to steal people’s personal identifying information, especially bank account numbers or other financial information. The tactic typically involves e-mails asking for personal information or directing a user to a mock Web site, which results in the theft of account numbers and passwords. Under the bill, such crimes will be a second degree felony, and will not depend, as it does in most fraud cases, on the

amount of money lost. The enhanced penalty recognizes that even if a person does not actually lose money, the theft of the identity often consumes a lot of time to correct the mistakes or unfreeze accounts.

Under **SB 71**, Utah residents will be allowed to freeze their credit report, which would prevent new accounts from being opened. 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 crooks 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

The bill also provides that a person may not display a Social Security number (SSN) in a manner or location that is likely to be open to public view, and provides for civil penalties for violations. It also prevents state or local agencies to employ inmates in any capacity that would allow an inmate access to another person's personal information.

SB 69 requires businesses maintaining personal information about people to safeguard against its disclosure and notify customers if that information is subject to a system security breach. Notification would be required if the company determines that the misuse of information is highly likely to occur. The notification must be in the most expedient time possible, but it can be delayed if a law enforcement agency determines that it could hurt a criminal investigation.

The bill also requires businesses to implement and maintain reasonable procedures to prevent the unlawful use or disclosure of personal information collected or maintained in the regular course of business. Before disposing of records containing personal information, it also must destroy or arrange for the destruction of the records, either by shredding, erasing, or modifying the information to make it indecipherable. The Attorney General's Office would be able to assess fines of up to \$2,500 per violation or series of violations concerning a specific consumer and no more than \$100,000 for related violations affecting more than one. It can also seek injunctive relief to stop the violations.

2005:

SB 167 targets the producers and users of fake identification cards. The bill sets out criminal penalties for underage people attempting to illegally buy alcohol or tobacco, and makes it a crime to use a fake ID to steal a person's identity. The bill makes it a ticketable offense to have a fake driver license and a class A misdemeanor to use one to get into a bar or buy alcohol or tobacco. A class A misdemeanor could result in a year in jail. A person who uses a fraudulent license to open a line of credit or cash a check could be charged with a third-degree felony, with a potential penalty of five years in prison. A person who uses the license as part of a violent crime could face the same penalty. The bill also targets rogue employees in the Driver License Division who issue illegal IDs.

SB 118 includes using the name and likeness of a deceased person under the identity theft statutes. The bill includes the deceased in legislation that prohibits identity theft, leaving no discrepancy between the living and the dead as far as the crime is involved.

2004:

SB 16 increases penalties for identity theft and makes it a crime to possess identification cards in another's name. Under the bill, identity theft will be a felony, regardless of the value of the credit, goods, services, or any other thing of value obtained. It makes it a class A misdemeanor to possess false identification or help someone obtain one. A third degree felony could be charged if a person has or helps another get multiple fake IDs. The bill also allows felony charges to be filed in the home county of a victim, even if the fraud was perpetrated in another county or out of state.

2003:

SB 42 expands the state's stolen credit card law to make using a stolen credit or debit card number a third-degree felony. It is already a third-degree felony to use a stolen card, but the measure extends the penalty to using just the card's number. This allows felony prosecution of anyone who skims credit card information with the intent to defraud the rightful holder. It criminalizes the use of but does not outlaw personal scanners that can be used to extract or totally remove financial information from the magnetic strip on a credit card.