

**COLORADO**

IDENTITY THEFT RANKING BY STATE: Rank 8, 89.0 Complaints Per 100,000 Population, 4328 Complaints (2007)

Updated November 28, 2008

**Current Laws:** A person commits identity theft if he or she:

- Knowingly possesses or uses the personal identifying information, financial identifying information, or financial device (credit card, check, debit card, etc.) of another without permission to obtain cash, credit, property, services, or any other thing of value.
- Falsely makes, completes, or alters a document or financial device containing any personal identifying information of another person, with the intent to defraud.
- Knowingly possess the personal identifying information of another person to apply for credit.
- Knowingly uses or possesses the personal identifying information of another without permission or lawful authority to obtain a government-issued document.
- Attempts, conspires with another, or solicits another to commit any of these acts.

“Identifying information” is defined as information that, alone or in conjunction with other information, identifies an individual, including but not limited to such individual’s:

- Name, address, or birth date.
- Telephone, Social Security, taxpayer identification, driver's license, identification card, alien registration, government passport, or checking, savings, or deposit account number.
- Biometric data, defined as data, such as fingerprints, voice prints, or retina and iris prints, that capture, represent, or enable the reproduction of the unique physical attributes of an individual.
- Unique electronic identification device or telecommunication identifying device, meaning a number, or magnetic or electronic device that enables the holder to use telecommunications technology to access an account; obtain money, goods, or services; or transfer funds.

Identity theft is a class 4 felony, punishable by two to six years in prison and/or a fine of \$2000 to \$500,000. However, the court may sentence the defendant to a term of imprisonment twice the presumptive range if the defendant is convicted of identity theft; and has a prior conviction for an identity theft violation.

Statute: §18-5-902:

<http://www.michie.com/colorado/lpext.dll/cocode/2c8c9/2f302/2f688/2f6a9?f=templates&fn=document-frame.htm&2.0>

It is a class 5 felony to possess identity theft tools, including any equipment adapted, designed, or commonly used for committing or facilitating the commission of identity theft, with the intent of using the tools to commit the crime.

Statute: §18.5.905:

<http://www.michie.com/colorado/lpext.dll/cocode/2c8c9/2f302/2f688/2f6cd?f=templates&fn=document-frame.htm&2.0>

It is a class 5 felony to gather identity information by deception. This offense occurs if a person knowingly makes or conveys a materially false statement, without permission or lawful authority, with the intent to obtain, record, or access the personal identifying information of another.

Statute: §18-5-904:

<http://www.michie.com/colorado/lpext.dll/cocode/2c8c9/2f302/2f688/2f6c7?f=templates&fn=document-frame.htm&2.0>

**Jurisdiction:** Identity theft may be prosecuted in any county where the prohibited act was committed, or in any county where the victim resides during part or all of the offense.

Statute: §18-1-202:

<http://www.michie.com/colorado/lpext.dll/cocode/2c8c9/2c8f0/2c9f3/2ca0e?f=templates&fn=document-frame.htm&2.0>

**Payment Cards:** A person commits criminal possession of a financial device if the person has in his or her possession or under his or her control any financial device that the person knows, or reasonably should know, to be lost, stolen, or delivered under mistake as to the identity or address of the account holder.

“Financial transaction device” means any instrument or device whether known as a credit card, banking card, debit card, electronic fund transfer card, or guaranteed check card, or account number representing a financial account or affecting the financial interest, standing, or obligation of or to the account holder, that can be used to obtain cash, goods, property, or services or to make financial payments.

Criminal possession of one financial device is a class 1 misdemeanor, punishable by six to eighteen months in prison and/or a fine of \$500 to \$5000. Possession of two or more financial devices is a class 6 felony, punishable by one year to eighteen months in prison and/or a fine of \$1000 to \$100,000. Possession of four or more, of which at least two are issued to different account holders, is a class 5 felony, punishable by one to three years in prison and/or a fine of \$1000 to \$100,000.

Statute: §18-5-903:

<http://www.michie.com/colorado/lpext.dll/cocode/2c8c9/2f302/2f688/2f6b8?fn=document-frame.htm&f=templates&2.0#>

A person commits unauthorized use of a financial transaction device if he uses such device for the purpose of obtaining cash, credit, property, or services or for making financial payment, with intent to defraud, and with notice that either the financial transaction device has expired, has been revoked, or has been cancelled; or for any reason his use of the financial transaction device is unauthorized either by the issuer thereof or by the account holder.

Unauthorized use of a financial transaction device is:

- A class 1 petty offense, punishable by up to six months in jail and/or a fine up to \$500, if the value of the cash, credit, property, or services obtained or of the financial payments made is less than \$100.

- A class 2 misdemeanor, punishable by three to twelve months in prison and/or a fine of \$250 to \$1000, if the value of the cash, credit, property, or services obtained or of the financial payments made is \$100 or more but less than \$500.
- A class 5 felony if the value of the cash, credit, property, or services obtained or of the financial payments made is \$500 or more but less than \$15,000;
- A class 3 felony if the value of the cash, credit, property, or services obtained or of the financial payments made is \$15,000 dollars or more. Violations are punishable by four to twelve years in prison and/or a fine of between \$3000 and \$7500.

The value of the cash, credit, property, or services obtained and the financial payments made shall be the total value of the cash, credit, property, or services obtained or financial payments made by unauthorized use of a single financial transaction device within a six-month period from the date of the first unauthorized use.

Statute: §18-5-702:

<http://www.michie.com/colorado/lpext.dll/cocode/2c8c9/2f302/2f608/2f616?fn=document-frame.htm&f=templates&2.0#>

**Change of Address:** State law requires a credit card issuer that receives an application with a different address in response to a mailed unsolicited offer to verify that the consumer accepting the offer is the same consumer to whom the offer was sent.

Statute: §5-3.7-101:

<http://www.michie.com/colorado/lpext.dll/cocode/89e5/89fb/8fdc/8fdf?fn=document-frame.htm&f=templates&2.0#>

**Social Security Numbers:** It is against state law for a person or entity to:

- Publicly post or publicly display (intentionally communicate or otherwise make available to the general public) in any manner an individual's Social Security number (SSN);
- Print an individual's SSN on any card required for the individual to access products or services provided by the person or entity;
- Require an individual to transmit his or her SSN over the Internet, unless the connection is secure or the social security number is encrypted;
- Require an individual to use his or her SSN to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet web site; and
- Print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires, permits, or authorizes the SSN to be on the document to be mailed.

Social Security numbers may be included in applications and forms sent by mail, including documents 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 SSN. A Social Security number that is permitted to be mailed may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

However, if a business had previously used an individual's SSN in a manner inconsistent with these provisions prior to January 1, 2007, it may continue using the SSN if the following conditions are met:

- The use of the SSN must be continuous. If its use is stopped for any reason, the provisions will apply.
- The individual is provided an annual disclosure that informs him/her that he/she has the right to stop the use of his or her Social Security number in a manner prohibited by the law.
- A written request by an individual to stop the use of his or her Social Security number is implemented within 30 days of the receipt of the request. There may not be a fee or charge for implementing the request.
- The business does not deny services to an individual because the individual makes a written request pursuant to this subsection.

Statute: §6-1-715:

[http://www.michie.com/colorado/lpext.dll/cocode/96d8/96fa/96fc/9a97/9bab?f=templates&fn=document-frame.htm&2.0#JD\\_6-1-715](http://www.michie.com/colorado/lpext.dll/cocode/96d8/96fa/96fc/9a97/9bab?f=templates&fn=document-frame.htm&2.0#JD_6-1-715)

State law prohibits a public entity (state or local agency) from issuing a license, permit, pass, or certificate that contains the holder's Social Security number, unless the issuing authority determines inclusion of the Social Security number is necessary to further the purpose of the license, pass, or certificate or inclusion is required by federal or state law. It also prohibits government agencies from requesting a person's Social Security number over the phone, Internet, or via mail unless the public entity determines receiving the Social Security number is required by federal law or is essential to the provision of services by the public entity.

Statute: §24-72.3-102:

<http://www.michie.com/colorado/lpext.dll/cocode/3a214/41155/41530/4153a?f=templates&fn=document-frame.htm&q=24-72.3-102&x=Advanced&2.0>

**Disposal of Records:** State law requires public and private entities that use documents during the course of business that contain personal identifying information to develop a policy for the destruction or proper disposal of paper documents containing personal identifying information.

“Personal identifying information” includes a Social Security number; personal identification number; password; pass code; official state or government-issued driver's license or identification card number; government passport number; biometric data; employer, student, or military identification number; or financial transaction device.

Statute: §6-1-713:

<http://www.michie.com/colorado/lpext.dll/cocode/96d8/96fa/96fc/9a97/9b97?fn=document-frame.htm&f=templates&2.0#>

### **Victim Assistance:**

**Mandatory Police Reports:** A person who knows or reasonably suspects that his or her identifying information has been unlawfully used by another person may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over the victim's residence or over the place where a crime was committed. The agency must take a police report of the matter, provide the complainant with a copy of that report, and begin

an investigation of the facts. If the suspected crime was committed in a different jurisdiction, the local law enforcement agency may refer the matter to the agency where the suspected crime was committed for investigation of the facts.

Statute: §16-5-103:

<http://www.michie.com/colorado/lpext.dll/cocode/28d4c/28d7c/2965c/29676/29694?fn=document-frame.htm&f=templates&2.0#>

**Restitution:** Victims of identity theft can file a private civil right of action against the perpetrator who committed the crime, regardless of whether the perpetrator was convicted of the crime. The victim is entitled to actual damages, including but not limited to damage to reputation or credit rating, punitive damages, and attorneys fees and costs.

Statute: §13-21-122:

<http://www.michie.com/colorado/lpext.dll/cocode/20396/2182e/21a18/21a1a/21a8a/21f78?f=templates&fn=document-frame.htm&q=13-21-122&x=Advanced&2.0>

**Security Breach:** State law requires an individual or a commercial entity that conducts business in Colorado that owns or licenses computerized data that includes personal information about a state resident that becomes aware of a breach of the security of the system to conduct a prompt investigation to determine the likelihood that personal information has been or will be misused. A security breach occurs upon “unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity.” It must then provide notice as soon as possible to the affected residents unless the investigation determines that the misuse of information has not occurred and is not reasonably likely to occur.

Personal information is defined as an Colorado resident’s first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unreadable: Social Security number, driver's license number or identification card number, account number, or credit or debit card number, in combination with any require security code, access code, or password that would permit access to a resident’s financial account. It does not include publicly available information.

Disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. If the breach affects more than 1,000 people, the entity must also notify the consumer reporting agencies.

Notification can be provided to the affected persons by mail, e-mail, or telephone. If the cost of providing regular notice would exceed \$250,000, the amount of people to be notified exceeds 250,000, or the information broker or data collector does not have sufficient contact information to provide written or electronic notice, substitute notice may be provided. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the entity’s web site, and notification to major statewide media.

Statute: § 6-1-716:

<http://www.michie.com/colorado/lpext.dll/cocode/96d8/96fa/96fc/9a97/9bbe?fn=document-frame.htm&f=templates&2.0#>

**Security Freezes:** All Colorado 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. Consumer reporting agencies may not charge a fee to implement the freeze. However, for each temporary lifting for a period of time or for permanent removal there is a \$10 fee. There is a \$12 fee for lifting the security freeze on a specific party.

The reporting agency must place the freeze within five business days after receiving the request, and within ten days, must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time. Requests for a temporary unlocking of the freeze must be completed within three business days.

Statute: §12-14.3-106.6:

[http://www.michie.com/colorado/lpext.dll/cocode/18a40/18aa6/1a1a3/1a25b?fn=document-frame.htm&2.0#JD\\_12-143-1066](http://www.michie.com/colorado/lpext.dll/cocode/18a40/18aa6/1a1a3/1a25b?fn=document-frame.htm&2.0#JD_12-143-1066)

For More Information: <http://www.ago.state.co.us/idtheft/securityfreeze.cfm>

How To Place A Security Freeze in Colorado:

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

**Credit Report Blocking:** People who believe that they are identity theft victims can ask most credit rating agencies to block and not report information appearing on their credit reports as a result of the crime. Within thirty days after receiving the request and the receipt of a police report or court order, the agency must stop reporting any information that resulted from the crime. The agency must also promptly notify the person or business that furnished the information of the police report and the effective date of the block. A credit rating agency may decline to block or rescind a block if it has a good faith belief that the consumer misrepresented the facts in the request for a block; agrees that information, or portions of it, was blocked in error; or knew or should have known that he received goods, services, or money as a result of blocked transactions. The agency must give consumers prompt written notice of their decision not to block or to rescind a block on information.

Statute: §12-14.3-106.5:

<http://www.michie.com/colorado/lpext.dll/cocode/18a40/18aa6/1a1a3/1a248?fn=document-frame.htm&f=templates&2.0#>

**Criminal Identity Theft:** State law provides for a process by which victims of criminal identity theft, defined as a person whose identifying information has been mistakenly associated with an arrest, summons, summons and complaint, felony complaint, information, indictment, or conviction, may clear their names. If a criminal charge is not pending, a victim of identity theft may, with notice to the prosecutor, petition the court with jurisdiction over the arrest, summons,

summons and complaint, felony complaint, information, indictment, or conviction to judicially determine the person's factual innocence. Alternatively, the court, on its own motion, may make such a determination in the case. If a criminal charge is pending, the prosecuting attorney may request the court to make such a determination. If the court determines that there is no reasonable cause to believe that a victim of identity theft committed the offense for which the victim's identity has been mistakenly associated, the court will find the victim factually innocent of that offense. If the victim is found factually innocent, the court will issue an order certifying this determination. After the court has determined that a person is factually innocent, the court may order the name and associated identifying information contained in court records, files, or a criminal justice record to be labeled to show that the information is not accurate and does not reflect the perpetrator's identity because the victim of identity theft was impersonated.

Statute: §16-5-103:

<http://www.michie.com/colorado/lpext.dll/cocode/28d4c/28d7c/2965c/29676/29694?fn=document-frame.htm&f=templates&2.0#>

---

### **State Resources:**

Office of the Attorney General: "I.D. Theft" (<http://www.ago.state.co.us/idtheft/IDTheft.cfm>)

Office of the Attorney General: "What Should I Do If I Become A Victim of Identity Theft?" (<http://www.ago.state.co.us/idtheft/victim.cfm>):

This document directs victims to: "*File a report with your local law enforcement agency. Obtaining that report will help you in dealing with your banks, creditors, and the major credit reporting bureaus.*"

Office of the Attorney General: "Identity Theft Repair Kit" (<http://www.ago.state.co.us/idtheft/idtrk.pdf>)

This comprehensive document contains an extensive checklist of steps that identity theft victim should take, including filing a report with local law enforcement: "*FILE A REPORT WITH YOUR LOCAL LAW ENFORCEMENT AGENCY. Obtaining that report will help you in dealing with your banks, creditors, and the major credit reporting bureaus.*"

*CRIMINAL VIOLATIONS: If an identity thief has impersonated you when they were arrested or cited for a crime, there are things you can do to correct your record First of all, to prevent being wrongfully arrested, carry copies of documents showing that you are a victim of identity theft even if you do not know that criminal violations have been attributed to your name. If they have, contact the law enforcement agency (police or sheriff's department) that arrested the identity thief. Or if there is a warrant for arrest out for the impersonator, contact the court agency that issued it. You may also want to get a lawyer to help you."*

"What Can Law Enforcement Do To Help Victims of Identity Theft" (<http://www.ago.state.co.us/idtheft/lehhelp.cfm>)

This document for law enforcement agencies explains what they can do to help victims of identity theft: "*Colorado law enforcement agencies can greatly assist victims of identity theft by taking police reports of all allegations of identity theft. Even where there is some question*"

*whether the theft of a person's identity occurred in a particular jurisdiction, a police report of such a theft empowers the victim in dealing with their banks and creditors. More importantly, under Colorado law, a victim can stop the reporting of negative credit information caused by the identity theft by filing the police report with the credit reporting bureaus. **DO NOT REFUSE A VICTIM A POLICE REPORT** even if you have no ability to investigate the crime further."*

The document also includes information on resources available at the national level to assist local law enforcement in combating identity theft, including the Federal Trade Commission's Sentinel ID Theft Clearinghouse ([www.ftc.gov/sentinel](http://www.ftc.gov/sentinel)) and training offered through the National White Collar Crime Center (NW3C) ([www.nw3c.org](http://www.nw3c.org)). It also provides a list of state and federal resources to which victims should be directed, including the sites from the Attorney General's office listed above.

"Can I Prevent Identity Theft?" (<http://www.ago.state.co.us/idtheft/prevention.cfm>)

"Phishing, Pharming, and other Pastoral Pursuits"  
(<http://www.ago.state.co.us/idtheft/PhishPharm.cfm>)

Colorado Bureau of Investigation: "Identity Theft / Mistaken Identity"  
([http://cbi.state.co.us/id/identity\\_theft.cfm](http://cbi.state.co.us/id/identity_theft.cfm)).

This site provides information on how victims of identity theft or criminal impersonation can challenge information on a criminal history record.

- "What Should I Do If I Become a Victim of Identity Theft"  
([http://cbi.state.co.us/idtheft/contents\\_victims.cfm](http://cbi.state.co.us/idtheft/contents_victims.cfm))

This page directs victims to "file a report with your local law enforcement agency. Obtaining that report will help you in dealing with your banks, creditors, and credit reporting agencies. By Colorado Law, your local law enforcement is required to make a report per [§ CRS 16-5-103 paragraph \(3\) three](#)."

---

## **Legislation:**

### **2006:**

**HB 1156** protects Social Security numbers (SSN) by prohibiting an individual or entity from publicly posting or displaying an individual's SSN; printing a SSN on any card required for the individual to access products or services; require an individual to transmit his SSN over the Internet, unless the connection is secure or the SSN is encrypted; require an individual to use his SSN to access a website, unless a password, PIN, or other authentication device is also required; or printing an SSN on any materials that are mailed to the individual, unless required or authorized by state or federal law. If a document with a SSN is mailed, the SSN may not be printed on a postcard or other mailer not requiring an envelope, or be visible on the envelope or without the envelope having been opened.

If a business had previously used an individual's SSN in a manner inconsistent with these provisions prior to January 1, 2007, it may continue using the SSN if the following conditions are met:

- The use of the SSN must be continuous. If its use is stopped for any reason, the provisions will apply.
- The individual is provided an annual disclosure that informs him/her that he/she has the right to stop the use of his or her Social Security number in a manner prohibited by the law.
- A written request by an individual to stop the use of his or her Social Security number is implemented within 30 days of the receipt of the request. There may not be a fee or charge for implementing the request.
- The business does not deny services to an individual because the individual makes a written request pursuant to this subsection.

**HB 1326** makes identity theft a Class 4 felony, punishable by up to six years in prison. Previously, there was no specific crime of identity theft under state law. A person commits identity theft if he or she possesses the personal information of another person with the intent to use it to obtain cash, credit or some other thing of value. The bill specifies other conditions that constitute identity theft. In addition, the bill increases the penalty for the unlawful gathering of personal information from a Class 1 misdemeanor to a Class 5 felony and creates a new Class 5 felony for the possession of identity theft tools.

**HB 1119** requires companies to inform consumers whose personal identifying information has been compromised as a result of a breach in data security. The law requires businesses to conduct, in good faith, a reasonable and prompt investigation into a security breach, and unless it determines that misuse of the personal information has not occurred and is not reasonably likely to occur, it must to notify the individual in the most expedient time possible and without unreasonable delay.

**2005:**

**SB 137** allows all Colorado consumers 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. Consumer reporting agencies may not charge a fee to implement the freeze. However, for each temporary lifting for a period of time or for permanent removal there is a \$10 fee. There is a \$12 fee for lifting the security freeze on a specific party.

**HB 1347** makes it a class 1 misdemeanor to use a false identity to gain the personal identifying information of another person over the Internet, over the phone, or by any other electronic medium.

**2004:**

**HB 1134** helps identity victims put their credit back together. It allows victims to report such crimes to police and require that officials forward the report to law enforcement in the jurisdiction where the crime took place. It also allows an identity theft victim to go before a judge and ask the judge to declare the victim factually innocent.

**HB 1274** will allow victims to collect damages for harm to their credit. The bill also requires credit card companies that offer and receive an acceptance of their card by mail to verify the identity and address of the applicant.

**HB 1311** prohibits the display of a person's social security number on a license, pass, or certificate issued by a public entity, unless it is necessary to further the purpose of the pass or required by state or federal law. It also prohibits a public entity from requesting a person's social security number over the phone, via the Internet, or by mail unless it is required by federal law or is essential to the public entity's service. In addition, it requires public and private entities to develop a policy for disposal of documents containing personal identifying information. It also makes it a class 1 misdemeanor to possess another's personal identifying information with the intent to use the information, or to aid or permit another to use the information, to unlawfully gain a benefit or to injure or defraud another.

**2002:**

**HB 1258** adds protections for victims of identity theft by requiring credit bureaus to block fraudulent information that appears on credit reports. Under the bill, victims would, after filing a police report, provide a copy of the police report to consumer reporting agencies. The agencies would have 30 days to block the bogus information from the victim's credit report. They also would have to notify any businesses where the card was used that a police report exists alleging identity theft. The law also allows courts to correct public records stemming from identity fraud as part of their restitution orders during sentencing of identity thieves.