

## IDAHO

IDENTITY THEFT RANKING BY STATE: Rank 36, 49.2 Complaints Per 100,000  
Population, 737 Complaints (2007)  
Updated November 30, 2008

**Current Laws:** It is unlawful for any person to obtain or record personal identifying information of another person without the authorization of that person, with the intent that the information be used to obtain, or attempt to obtain, credit, money, goods or services without the consent of that person.

Statute: §18-3126: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310026.K>

“Personal identifying information” means the name, address, telephone number, driver’s license number, Social Security number, place of employment, employee identification number, mother’s maiden name, checking account number, savings account number, financial transaction card number, or personal identification code of an individual person, or any other numbers that can be used to access a person’s financial resources.

Statute: §18-3122: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310022.K>

Violations are a felony, punishable by up to five years in prison and/or a fine of up to \$50,000, if the retail value of the goods obtained or attempted to be obtained exceeds \$300. If the value is under \$300, a violation is a misdemeanor, punishable by up to one year in county jail and/or a fine up to \$1000.

Statute: §18-3128: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310028.K>

It is unlawful for any person to falsely assume or pretend to be a member of the armed forces of the United States or an officer or employee acting under authority of the United States or any department, agency or office thereof or of the state of Idaho or any department, agency or office thereof, and in such pretended character, seek, demand, obtain or attempt to obtain personal identifying information of another person. Violations are a felony.

Statute: §18-3126A: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310026A.K>

**Financial Transaction Cards:** State law prohibits the fraudulent use of financial transaction cards (FTC) or numbers. FTCs include credit and debit cards, and any other instrument issued for the use of the cardholder in obtaining money, goods, services, or anything else of value on credit, or to obtain access to a bank account. Among other things, it is unlawful for any person to do any of the following with the intent to defraud:

- To knowingly obtain or attempt to obtain credit or to purchase or attempt to purchase any goods, property, or service, by the use of any false, fictitious, counterfeit, revoked, expired or fraudulently obtained FTC, by any FTC account number, or by the use of any FTC issued; or
- To make an application for an FTC 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 any indebtedness for the purposes of influencing the issuer to issue an FTC.

Statute: §18-3124: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310024.K>

Violations are a felony, punishable by up to five years in prison and/or a fine of up to \$50,000, if the retail value of the goods obtained or attempted to be obtained exceeds \$300. If the value is under \$300, a violation is a misdemeanor, punishable by up to one year in county jail and/or a fine up to \$1000.

Statute: §18-3128: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310028.K>

It is a felony, punishable by up to five years in prison and/or up to a \$50,000 fine, to acquire an FTC or FTC number from another without the consent of the cardholder or issuer; to receive an FTC or FTC number, with the knowledge that it has been so acquired and with the intent to use it to defraud; or to sell or transfer the FTC or FTC number to another person with the knowledge that it will be used to defraud. It is also a felony to acquire an FTC or FTC number that a person knows to have been lost, mislaid, or delivered under a mistake as to the identity or address of the card holder, and to retain possession with the intent to use to defraud or to sell or transfer to another person with the knowledge that it is to be used to defraud.

Statute: §18-3125: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310025.K>

A person, with intent to defraud, who counterfeits, falsely makes, embosses, or encodes magnetically or electronically any FTC is guilty of forgery, punishable by one to fourteen years in prison. It also prohibits using the FTC or FTC account number or personal identification number (PIN) of a cardholder in the creation of a fictitious or counterfeit credit card sales draft; signing the name of another or a fictitious name to an FTC sales slip or credit draft.

Statute: §18-3123: <http://www3.state.id.us/cgi-bin/newidst?sctid=180310023.K>

**Scanning Devices:** State law prohibits the possession or use of a scanning device or re-encoder that is used to obtain or record encoded information from the magnetic strip of a payment card to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A re-encoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are considered grand theft, and are a felony, punishable by one to fourteen years in prison and/or a fine up to \$5000.

Statute: §18-2415: <http://www3.state.id.us/cgi-bin/newidst?sctid=180240015.K>

## **Victim Assistance:**

**Security Freeze:** State law allows all Idaho consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information. To request a freeze, a consumer must request one in writing to the credit reporting agencies. The credit reporting agency may charge up to \$6 to place or temporarily lift a security freeze. Victims of identity theft will not be charged any fees in connection with the placing, removing, or temporary lifting of a security freeze.

The reporting agency must place the freeze within three business days after receiving the request, and within five days of 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. However, a temporary unlocking must be completed within 15 minutes after the consumer's request is received through an electronic contact method between the hours of 6:00 am and 9:30 pm.

Statute: §28-52-101 through 109: <http://www3.state.id.us/oasis/S1380.html> - [engrhttp://www3.state.id.us/idstat/TOC/28052KTOC.html](http://www3.state.id.us/idstat/TOC/28052KTOC.html)

Office of the Attorney General, Credit Freeze Frequently Asked Questions”  
(<http://www2.state.id.us/ag/consumer/tips/creditreportfreeze.htm>)

**Security Breach:** State law requires businesses operating in the state and state and local government agencies that own or license computerized data that include consumers' personal information to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. A security breach means “the illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information.” If a business or agency becomes aware of a breach of the security of the system, it must conduct a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If so, it must notify consumers in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

Personal information means an Idaho resident's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not redacted: Social Security number; driver's license or Idaho identification card number; or an account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account. Publicly available information is not included.

Notification can be provided to the affected persons by mail, e-mail, or by telephone. If the cost of providing regular notice would exceed \$25,000, the amount of people to be notified exceeds 50,000, or the agency or business does not have sufficient contact information, substitute notice

may be provided. When substitute notice is used, it must consist of all of the following, as applicable: e-mail notice, conspicuous posting on the entity's web site, and notification to statewide media.

Statute: §28-51-105: <http://www3.state.id.us/cgi-bin/newidst?sctid=280510105.K>

---

### **State Resources:**

Office of the Attorney General, "Identity Theft"  
(<http://www2.state.id.us/ag/consumer/identitytheft.htm>)

"Identity Theft Manual" (<http://www2.state.id.us/ag/consumer/tips/IdentityTheft.pdf>)  
This comprehensive document includes prevention tips and information on the steps victims of identity theft should take. It directs victims to: *"File a report with your local police and the police in the community where the theft occurred. Obtain certified copies of the report because you may need it to validate your claims to creditors."*

"Credit Reports" (<http://www2.state.id.us/ag/consumer/tips/creditreports.htm>)

"Identity Theft Letters and Forms"  
([http://www2.state.id.us/ag/consumer/identity\\_theft/identitytheftformsindex.htm](http://www2.state.id.us/ag/consumer/identity_theft/identitytheftformsindex.htm))

This Web page includes links to forms and sample letters to help victims of identity theft:

- "Annual Free Credit Report Request Form"  
([http://www2.state.id.us/ag/consumer/identity\\_theft/AnnualFreeCreditReportRequestForm.pdf](http://www2.state.id.us/ag/consumer/identity_theft/AnnualFreeCreditReportRequestForm.pdf)): *"A form you can mail to the three major consumer credit reporting agencies to obtain your free annual credit report. If your report contains fraudulent or incorrect information, you should report it to the agency and the creditor immediately."*
- "Sample Blocking Letter to Consumer Reporting Company"  
([http://www2.state.id.us/ag/consumer/identity\\_theft/SampleBlockingLetterToCRC.pdf](http://www2.state.id.us/ag/consumer/identity_theft/SampleBlockingLetterToCRC.pdf)): *"An example of a letter you can mail to a consumer credit reporting agency to dispute fraudulent information in your credit file. Make sure you provide the agency with as much information and documentation as possible, including a copy of the police report. Never send original documents to a credit reporting agency."*
- "Sample Dispute Letter for Existing Accounts"  
([http://www2.state.id.us/ag/consumer/identity\\_theft/SampleDisputeLetterForExistingAccounts.pdf](http://www2.state.id.us/ag/consumer/identity_theft/SampleDisputeLetterForExistingAccounts.pdf)): *"An example of a letter you can mail to a creditor to dispute fraudulent charges to or debits from your financial accounts. Make sure you provide the creditor with as much information and documentation as possible, including a copy of the police report. Never send original documents to creditors."*

- Identity Theft Affidavit”  
([http://www2.state.id.us/ag/consumer/identity\\_theft/SampleDisputeLetterForExistingAccounts.pdf](http://www2.state.id.us/ag/consumer/identity_theft/SampleDisputeLetterForExistingAccounts.pdf)): “A form you can mail to consumer credit reporting agencies and creditors to tell them you are an identity theft victim and that you are not responsible for the identity thief’s debts. Follow the instructions carefully so your affidavit is complete. Call the creditor before you mail your affidavit to find out if the creditor requires specific documentation from you or if the creditor requires you to have the affidavit notarized. Never send original documents to credit reporting agencies or creditors.”
- 

## **Legislation:**

### **2008:**

**SB 1380** allows Idaho consumers to freeze access to their credit reports as a way to help prevent fraud and identity theft. A security freeze prohibits, with certain specific exceptions, the credit reporting agency from releasing the consumer’s credit report or any information from it without the express authorization of the consumer. Consumers can temporarily lift or permanently remove the freeze to obtain credit. Credit reporting agencies can charge a fee of up to \$6 to place or temporarily lift a freeze. Identity theft victims may not be charged to place or remove a freeze.

**SB 1357** clarifies the existing identity theft statute to cover situations in which an offender uses a stolen Social Security number or date of birth in conjunction with his/her name or a fictitious name (instead of only the name of the victim) to obtain credit, money, goods or services.

### **2006:**

**SB 1374** requires businesses and state and local government agencies that collect and maintain computerized records containing consumer’s personal information to notify affected consumers if that personal data is compromised in a security breach, putting them at risk for identity theft.

### **2005:**

**SB 1156** amends existing identity theft law to provide that it is unlawful for any person to falsely assume or pretend to be a member of the armed forces of the United States or an officer or employee acting under authority of the United States or the state of Idaho, and in such pretended character, seek, demand, obtain or attempt personal identifying information of another person. Violations are a felony, punishable by up to five years in prison and/or a fine of up to \$50,000.

### **2003:**

**SB 1365** prohibits the possession or use of a scanning device or re-encoder that is used to obtain or record encoded information from the magnetic strip of a payment card to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A re-encoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are considered grand theft, and are a felony, punishable by one to fourteen years in prison and/or a fine up to \$5000.