

## WASHINGTON

IDENTITY THEFT RANKING BY STATE: Rank 13, 76.4 Complaints Per 100,000

Population, 4942 Complaints (2007)

Updated January 11, 2009

**Current Laws:** Washington's identity theft law states that no person may knowingly obtain, possess, use, or transfer a means of identification or financial information of another person, living or dead, with the intent to commit, or to aid or abet, any crime.

“Means of identification” means information or an item that is not describing finances or credit but is personal to or identifiable with an individual or other person, including:

- A current or former name of the person, telephone number, an electronic address, or identifier of the individual or a member of his or her family, including the ancestor of the person;
- Information relating to a change in name, address, telephone number, or electronic address or identifier of the individual or his or her family;
- Social Security, driver's license, or tax identification number of the individual or a member of his or her family; or
- Other information that could be used to identify the person, including unique biometric data.

“Financial information” means any of the following information identifiable to the individual that concerns the amount and conditions of an individual's assets, liabilities, or credit:

- Account numbers and balances;
- Transactional information concerning an account; and
- Codes, passwords, Social Security numbers, tax identification numbers, driver's license or permit numbers, state identicaid numbers issued by the Department of Licensing, and other information held for the purpose of account access or transaction initiation.

A violation when the accused or an accomplice uses the victim's means of identification or financial information and obtains an aggregate total of credit, money, goods, services, or anything else of value in excess of \$1500 in value is a class B felony, punishable by up to ten years in prison and/or a fine up to \$20,000. Losses below \$1500 are a class C felony, punishable by up to five years in prison and/or a fine of up to \$10,000. Upon conviction, the law allows courts to issue an order a victim can use to correct public records tainted by identity theft.

These provisions do not apply to any person who obtains another person's driver's license or other form of identification for the sole purpose of misrepresenting his or her age.

Statute: §9.35.020: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9.35.020>

The relevant unit of prosecution for identity theft is an unlawful use of a means of identification or financial information. A defendant may be prosecuted and punished separately for every instance the defendant unlawfully obtains, possesses, transfers, or uses the means of

identification or financial information, unless the instances constitute the same criminal conduct. Whenever any series of transactions involving a single person's identification or financial information would, when considered separately, constitute identity theft in the second degree because of value, and the series of transactions are part of a common scheme or plan, the transactions may be aggregated for purposes of determining the degree of identity theft involved. If a person commits another crime during the commission of identity theft, the defendant may be prosecuted and punished separately for the other crime as well as for the identity theft.

Statute: §9.35.001: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9.35.001>

**Jurisdiction:** Identity theft crimes are considered to have been committed in any locality where the person whose means of identification or financial information was appropriated resides, or in which any part of the offense took place, regardless of whether the defendant was ever actually in that locality.

Statute: §9.35.020: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9.35.020>

**Financial Information:** It is a class C felony for any person to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, financial information from a financial information repository, financial services provider, merchant, corporation, trust, partnership, or unincorporated association:

- By knowingly making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial information repository with the intent to deceive the person into relying on that statement or representation for purposes of releasing the financial information;
- By knowingly making a false, fictitious, or fraudulent statement or representation to a customer of a financial information repository, financial services provider, merchant, corporation, trust, partnership, or unincorporated association with the intent to deceive the customer into releasing financial information or authorizing the release of such information;
- By knowingly providing any document to an officer, employee, or agent of a financial information repository, financial services provider, merchant, corporation, trust, partnership, or unincorporated association, knowing that the document is forged, counterfeit, lost, or stolen; was fraudulently obtained; or contains a false, fictitious, or fraudulent statement or representation, if the document is provided with the intent to deceive the officer, employee, or agent to release the financial information.

In addition to criminal penalties, violators are also liable for \$500 or actual damages, whichever is greater, and reasonable attorneys' fees.

Statute: §9.35.010: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9.35.010>

**Phishing:** The state prohibits "phishing" scams, in which identity thieves try to trick consumers out of personal information by sending e-mails that appear to come from a business, such as a bank. It is a violation for a person to take any action to induce a person to provide personally identifying information by means of a web page, electronic mail message, or otherwise using the internet by representing oneself, either directly or by implication, to be another person, without the authority or approval of such other person.

“Personally identifying information” means an individual’s: Social Security number; driver’s license number; bank account number; credit or debit card number; personal identification number; automated or electronic signature; unique biometric data; account passwords; or any other piece of information that can be used to access an individual's financial accounts or to obtain goods or services.

Businesses affected by such fraud can bring a civil action in Superior Court to seek up to \$5,000 or actual damages. An individual may recover up to \$500 or actual damages, whichever is greater. Courts may increase the damages up to three times for repeat offenders.

Statute: §19.190.080:

<http://apps.leg.wa.gov/RCW/default.aspx?cite=19.190&full=true#19.190.080>

**Spyware:** State law prohibits the use of spyware, software that surreptitiously monitors a computer user’s actions. It is illegal for anyone to transmit software to another computer without the owner’s knowledge or to falsely entice someone to download software, or for an unauthorized person to install software that would take control of a computer’s computer, modify its security settings, collect the user’s personal identification information, interfere with its removal, or otherwise deceive the authorized user. State law also prohibits:

- disabling the ability of anti-spyware or anti-virus software to update automatically, if the disabling is done through intentionally deceptive means;
- using the owner or operator's computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer or person, including, but not limited to, launching a denial of service attack;
- transmitting or relaying commercial e-mail or a computer virus from the owner or operator's computer if initiated by a person other than the owner or operator;
- modifying toolbars or buttons of the owner or operator's Internet browser used to access and navigate the Internet, if the disabling is done through deceptive means; and
- inducing an owner to install software by displaying a pop-up, web page, or other message whose source is misrepresented.

Violators can be fined actual damages or up to \$100,000, whichever is greater. The court may increase those damages by threefold for repeat offenders, up to a maximum of \$2 million. These prohibitions also apply to those persons who know or consciously avoid knowing that their services are being used to procure or transmit spyware.

Statute: §19.270: <http://apps.leg.wa.gov/RCW/default.aspx?cite=19.270>

**Drivers’ Licenses:** It is a misdemeanor for a person to:

- Display or have in his possession any fictitious or fraudulently altered driver’s license or identicard;
- Lend his driver’s license or identicard to any other person or knowingly permit the use thereof by another;
- Display or represent as one’s own any driver’s license or identicard not issued to him;
- Use a false or fictitious name in any application for a driver’s license or identicard or to knowingly make a false statement or to knowingly conceal a material fact or otherwise commit a fraud in any such application; or
- Permit any unlawful use of a driver’s license or identicard issued to him or her.

It is a class C felony for any person to sell or deliver a stolen driver's license or identicard. It is also unlawful for any person to manufacture, sell, or deliver a forged, fictitious, counterfeit, fraudulently altered, or unlawfully issued driver's license or identicard, or to manufacture, sell, or deliver a blank driver's license or identicard except under the direction of the department of motor vehicles. A violation is a class C felony if committed for financial gain or with intent to commit forgery, theft, or identity theft.

For people under 21, making up to four fake drivers' licenses is a misdemeanor if done for the sole purpose of age misrepresentation.

Statute: §46.20.0921: <http://apps.leg.wa.gov/RCW/default.aspx?cite=46.20.0921>

State law also makes it a class C felony for a person to use radio waves to intentionally possess, read, or capture remotely, information on another person's enhanced driver's license without the person's express knowledge and consent. The enhanced licenses, which can be used in place of a passport to cross land and sea borders between the U.S., Canada, and Mexico, include a radio frequency identification chip or similar technology, which could lead to theft of the identity contained within them.

Statute: §9A.58: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9A.58>

**Payment Instruments:** A person is guilty of unlawful production of payment instruments if he or she prints or produces a check or other payment instrument in the name of a person or entity, or with the routing number or account number of a person or entity, without the permission of the person or entity to manufacture or reproduce such payment instrument with such name, routing number, or account number. A "payment instrument" means a check, draft, money order, traveler's check, or other instrument for the transmission or payment of money or its equivalent value, whether or not negotiable, but does not include a credit card voucher, letter of credit, or instrument that is redeemable by the issuer in goods or services.

A person is guilty of unlawful possession of payment instruments if he or she possesses two or more checks or other payment instruments, alone or in combination:

- In the name of a person or entity, or with the routing number or account number of a person or entity, without the permission of the person or entity to possess such payment instrument, and with intent either to deprive the person of possession of such payment instrument or to commit theft, forgery, or identity theft; or
- In the name of a fictitious person or entity, or with a fictitious routing number or account number of a person or entity, with intent to use the payment instruments to commit theft, forgery, or identity theft.

A person is guilty of unlawful possession of a personal identification device if the person possesses a personal identification device with intent to use such device to commit theft, forgery, or identity theft. "Personal identification device" includes any machine or instrument whose purpose is to manufacture or print any driver's license or identification card issued by any state or the federal government, or any employee identification issued by any employer, public or private, including but not limited to badges and identification cards, or any credit or debit card.

A person is guilty of unlawful possession of fictitious identification if the person possesses a personal identification card with a fictitious person's identification with intent to use such identification card to commit theft, forgery, or identity theft, when the possession does not amount to a violation of the identity theft statute.

A person is guilty of unlawful possession of instruments of financial fraud if the person possesses a check-making machine, equipment, or software, with intent to use or distribute checks for purposes of defrauding an account holder, business, financial institution, or any other person or organization.

All violations are a class C felony.

Statute: §9A.56.320: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9A.56.320>

**Scanning Devices:** State law prohibits the possession and 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 a payment card. A re-encoder is an electronic device that places encoded information from a payment card onto a different card. Violations are a class C felony, and subsequent violations are a class B felony.

Statute: §9A.56.290: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9A.56.290>

**Destruction of Records:** State law requires businesses to take all reasonable steps to destroy, or arrange for the destruction of personal financial and health information and personal identification numbers issued by government entities. If information is not disposed of in accordance with the law, businesses may be subject to civil liability if an individual is harmed by their failure.

“Personal financial” and “health information” mean information that is identifiable to an individual and that is commonly used for financial or health care purposes, including account numbers, access codes or passwords, information gathered for account security purposes, credit card numbers, information held for the purpose of account access or transaction initiation, or information that relates to medical history or status. “Personal identification number issued by a government entity” means a tax identification number, Social Security number, driver’s license or permit number, state identification card number issued by the department of licensing, or any other number or code issued by a government entity for the purpose of personal identification that is protected and is not available to the public under any circumstances.

Statute: §19.215: <http://apps.leg.wa.gov/RCW/default.aspx?cite=19.215&full=true>

## **Victim Assistance:**

**Mandatory Police Reports:** A person who has learned or reasonably suspects that his or her financial information or means of identification has been unlawfully obtained, used by, or disclosed to another, may file an incident report with a law enforcement agency, by contacting the agency that has jurisdiction over his or her actual residence, place of business, or place where the crime occurred. The agency must create a police incident report of the matter and provide the complainant with a copy of that report. The law enforcement agency may refer the incident to another law enforcement agency, and the law does not require the law enforcement agency to investigate the reports of identity theft. In addition, identity theft incident reports are not required to be counted as an open case for purposes of compiling open case statistics.

Statute: § 9.35.050: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9.35.050>

**Civil Damages:** People convicted of identity theft are responsible for civil damages to the victim of \$1000 or actual damages, whichever is greater, including costs to repair the victim's credit record and reasonable attorneys' fees.

Statute: §19.182.160: <http://apps.leg.wa.gov/RCW/default.aspx?cite=19.182.160>

**Credit Blocks:** Within 30 days of receipt of proof of the consumer's identification and a copy of a police report filed by the consumer, evidencing the consumer's claim to be a victim of a identity theft, a consumer reporting agency must permanently block reporting any information the consumer identifies on his or her consumer report is a result of the identity theft violation so that the information cannot be reported. The consumer reporting agency must promptly notify the furnisher of the information that a police report has been filed, that a block has been requested, and the effective date of the block.

Statute: §19.182.160: <http://apps.leg.wa.gov/RCW/default.aspx?cite=19.182.160>

**Security Breaches:** State law requires state agencies and any person or business that conducts business in the state and that owns or licenses computerized data that includes personal information to disclose any breach of security of the system to any resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. A security breach occurs upon "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information" maintained by the person, business, or agency. Notification is not required for a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.

Personal information is defined as an individual'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 encrypted: Social Security number; driver's license number or Washington identification card number; or an account number or credit or debit card number, in combination with any required security code, access code, or password, that would permit access to an individual's financial account. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notification can be provided by mail or e-mail. If the cost of providing regular notice would exceed \$250,000, the amount of people to be notified exceeds 500,000, or the business or agency 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 business or agency's web site, and notification to major statewide media.

Statute: Businesses: §19.255.010: <http://apps.leg.wa.gov/RCW/default.aspx?cite=19.255.010>  
Government Agencies: §42.56.590: <http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590>

**Security Freeze:** All Washington 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. Currently, only victims of identity theft and a person who has been notified of a security breach of his unencrypted personal information are permitted to place such a freeze on their accounts.

To request a freeze, a consumer must request one in writing by certified mail. Consumer reporting agencies may charge a fee of \$10 to place or temporarily lift a security freeze. However, victims of identity theft with a report of alleged identity theft fraud or a person 65 years of age or older may not be charged.

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. However, if an agency has developed procedures involving the use of telephone, fax, Internet, or other electronic media to receive and process a request from a consumer to temporarily lift a security freeze, it must be completed within 15 minutes if submitted through the electronic contact method during normal business hours.

Statute: §19.182.170: <http://apps.leg.wa.gov/RCW/default.aspx?cite=19.182.170>

For More Information: <http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/SecurityFreeze.aspx>

**Fraudulent Transactions:** State law requires businesses to provide victims, upon request, with information about fraudulent transactions made in their names. Businesses may require proof of identity and may charge a fee for the reasonable cost of providing the requested information. Businesses that refuse to provide information may be required to pay damages and a \$1,000 penalty for willful violations.

Statute: §9.35.040: <http://apps.leg.wa.gov/RCW/default.aspx?cite=9.35.040>

**Prohibitions Against Debt Collectors:** State law prohibits collection agencies from calling identity theft victims multiple times once they have been notified that a series of checks have been stolen or misappropriated.

Statute: §19.16.250(20): <http://apps.leg.wa.gov/RCW/default.aspx?cite=19.16.250>

---

### **State Resources:**

Office of the Attorney General, “Identity Theft and Privacy”  
(<http://www.atg.wa.gov/ConsumerIssues/ID-Privacy.aspx>)

“Identity Theft” (<http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/IdentityTheft.aspx>)

This page provides information for victims of identity theft, including steps they should take. It directs victims to: “**Step 3: Report the ID theft to the police or sheriff in the area where you live. ID theft is a felony, and charges may be filed against the thief in the county where you live. Ask the police to make a police report and give you a copy. You will need this to help correct your credit rating.**”

- “Tips for Identity Theft / Privacy” (<http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/Tips.aspx>)
- “ID Theft Brochure for Consumers”  
([http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding\\_Consumers/Brochures/pf\\_consumer\\_id\\_theft.pdf](http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding_Consumers/Brochures/pf_consumer_id_theft.pdf))
- “Information for Businesses” (<http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/Businesses.aspx>)
- “Protecting Personal Information: A Guide for Business”  
([http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding\\_Consumers/Consumer\\_Issues\\_A-Z/Identity\\_Theft\\_%28Privacy%29/ID%20Theft%20co\\_brand\\_business\\_booklet.pdf](http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding_Consumers/Consumer_Issues_A-Z/Identity_Theft_%28Privacy%29/ID%20Theft%20co_brand_business_booklet.pdf))
- “Security Freeze and Fraud Alert” (<http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/SecurityFreeze.aspx>)
- “Phishing” (<http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/Phishing.aspx>)
- “Dumpster Diving” (<http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/DumpsterDiving.aspx>)

“Department of Financial Institutions”

([http://dfi.wa.gov/consumers/education/identity\\_theft.htm](http://dfi.wa.gov/consumers/education/identity_theft.htm))

This site includes helpful information for consumers, including:

- “Avoid Identity Theft”  
([http://dfi.wa.gov/consumers/education/identity\\_theft/avoid\\_identity\\_theft.htm](http://dfi.wa.gov/consumers/education/identity_theft/avoid_identity_theft.htm))
  - “What To Do If Your Identity Has Been Stolen”  
([http://dfi.wa.gov/consumers/education/identity\\_theft/what\\_to\\_do\\_stolen.htm](http://dfi.wa.gov/consumers/education/identity_theft/what_to_do_stolen.htm))  
This page directs victims to: “*File a report with your local police. Get a copy of the police report, so you have proof of the crime.*”
  - “What To Do If You Lose Your Wallet or Purse?”  
([http://dfi.wa.gov/consumers/education/identity\\_theft/if\\_you\\_lose.htm](http://dfi.wa.gov/consumers/education/identity_theft/if_you_lose.htm))
-

## **Legislation:**

### **2008:**

**SB 5878** requires law enforcement to take a police report from victims of identity theft and provide the complainant with a copy of the report. In order for victims to exercise certain state and federal rights, it is necessary for the victim to obtain a police report. For example, a consumer must have a police report to freeze their credit, place long-term fraud alerts, and to obtain records of fraudulent accounts from merchants. The bill also allows prosecutors to bring separate charges against an accused identity thief for each use of an individual's information.

**HB 2637** seeks to promote identity theft prosecutions by allowing records provided by out-of-state businesses to be authenticated by affidavit, rather than in person, in criminal cases to reduce time and expense in bringing identity theft prosecutions.

**HB 2729** seeks to protect the state's new enhanced drivers' licenses that can be used in place of a passport to cross land and sea borders between the U.S., Canada, and Mexico. These enhanced licenses include a radio frequency identification chip or similar technology, which could lead to theft of the identity contained within them. Under the law, it is now a class C felony if he uses radio waves to intentionally possess, read, or capture remotely, information on another person's enhanced driver's license without that person's express knowledge and consent.

**SB 2879** expands the state's anti-spyware laws to prohibit the following computer activities:

- disabling the ability of anti-spyware or anti-virus software to update automatically, if the disabling is done through intentionally deceptive means;
- using the owner or operator's computer as part of an activity performed by a group of computers for the purpose of causing damage to another computer or person, including, but not limited to, launching a denial of service attack;
- transmitting or relaying commercial e-mail or a computer virus from the owner or operator's computer if initiated by a person other than the owner or operator;
- modifying toolbars or buttons of the owner or operator's Internet browser used to access and navigate the Internet, if the disabling is done through deceptive means; and
- inducing an owner to install software by displaying a pop-up, web page, or other message whose source is misrepresented.

### **2007:**

**SB 5826** will allow Washington 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. Previously, only victims of identity theft could place such a freeze.

**2006:**

**HB 1966** provides for increased prosecutions for identity theft by categorizing identity theft in the first and second degrees as “crimes against persons” instead of “crimes against property.” As a “crime against persons,” people convicted of identity theft cannot clear their records, can be subject to community placements or community custody, and cannot qualify for up to 50% earned release time for good conduct.

**2005:**

**SB 6043** requires businesses to notify a consumer if his personal information was acquired as a result of a security system breach. However, the bill was amended to allow companies to decide whether to notify customers when their data are stolen. If the companies consider it a “technical breach” that does not seem reasonably likely to subject customers to criminal activity, they are not required to tell consumers.

**SB 5418** gives consumers who receive notice of a security breach, as well as those who have become victims of identity theft, the right to put a security freeze on their credit file to prevent new accounts from being opened in their name. Such a freeze allows the consumer to prevent anyone from looking at his or her credit reporting file for purposes of granting credit unless the consumer specifically chooses to let a particular business access the information. When applying for credit, the consumer can lift the freeze for particular companies.

**SB 5939** requires police departments to provide victims with police or incident reports, allowing victims to work with credit-reporting agencies to clean up fraudulent accounts and place a fraud alert or security freeze on their file. The law does not require a law enforcement agency to investigate each report.

**HB 1012** targets the use of spyware, software that surreptitiously monitors a computer user’s actions. The bill makes it illegal for anyone to transmit software to another computer without the owner’s knowledge or to falsely entice someone to download software. It prohibits an unauthorized person from installing software that would take control of a computer’s computer, modify its security settings, collect the user’s personal identification information, interfere with its removal, or otherwise deceive the authorized user. Violators can be fined actual damages or up to \$100,000, whichever is greater. The court may increase those damages by threefold for repeat offenders, up to a maximum of \$2 million.

**HB 1888** amends the state’s anti-spam statute to specifically prohibit “phishing” scams, in which identity thieves try to trick consumers out of personal information by sending e-mails that appear to come from a business, such as a bank. The bill makes it illegal for a person to misrepresent his or her identity in order to solicit information online. Businesses affected by such fraud can bring a civil action in Superior Court to seek up to \$5,000 or actual damages. An individual may recover up to \$500 or actual damages, whichever is greater. Courts may increase the damages up to three times for repeat offenders.

### **2003:**

The Legislature passed several bills designed to cut down on identity theft and fraud:

- **SB 5716** toughens the penalties for making or selling phony driver's licenses. Under the bill, dealing in fake licenses for criminal purposes will be a Class C felony. For people under 21, making up to four fake drivers' licenses will be a misdemeanor if done for the sole purpose of age misrepresentation.
- **SB 5719** makes it a felony to possess or use credit card scanners, small, cell-phone-sized devices that record the information on a credit or ATM card. It also criminalizes the use of a re-encoder to place information encoded on a credit or debit card onto a different card.
- **SB 5720** allows merchants to ask for identification for a credit card transaction. While the bill does not require merchants to do so, it declares null and void merchant agreements used by some credit card companies, including Visa and MasterCard, which prohibit stores from asking for additional identification.
- **HB 1844** criminalizes the possession or manufacture of tools used in financial fraud, such as blank ATM or credit cards, blank checks or multiple fake IDs.

### **2001:**

**SB 5449** stiffens penalties for identity theft and makes it easier for victims to obtain information needed to reestablish their identity and deal with their creditors. The law doubles the maximum sentence for identity theft to 10 years in prison and up to \$20,000 in fines in cases involving more than \$1,500. It also makes identity theft a crime under the Racketeer Influenced and Corrupt Organizations (RICO) Act, which could enhance the penalties even more.

The law provides victims with some tools they can use to clear up their own names and credit histories, regardless what happens with any criminal prosecution:

- Requires merchants and other businesses to provide identity theft victims information about fraudulent transactions made in their name. Businesses that refuse to do so could be forced to pay damages and a \$1,000 penalty.
- Allows victims to block tainted credit reports by filing police reports with credit reporting agencies.
- Makes it easier for identity theft victims to testify by requiring prosecutors to try cases in the county where the victim resides, rather than where the defendants are arrested and charged.
- Allows victims to get court documents that help them correct their credit history if identity thieves are convicted.
- Provides that a collection agency may not call victims more than one time in 180 days in order to collect on debts created because of an identity theft.