

CALIFORNIA

IDENTITY THEFT RANKING BY STATE: Rank 2, 120.1 Complaints Per 100,000

Population, 43,892 Complaints (2007)

Updated November 25, 2008

Current Laws: A person who, with the intent to defraud, acquires or retains possession of the personal identifying information of another person can be punished by a fine up to \$1000 and/or up to one year in county jail. Penalties may be increased if a person:

- Has a previous conviction for an identity theft violation; or
- Acquires or retains the personal identifying information of ten or more persons; or
- Obtains personal identifying information of another person and uses that information without the consent of that person for any unlawful purpose, including to obtain or attempt to obtain credit, goods, services, real property, or medical information; or
- With intent to defraud, sells, transfers, or conveys the personal identifying information of another person; or
- With actual knowledge that the personal identifying information of a specific person will be used fraudulently, sells, transfers, or conveys that information.

For these offenses, violations can be either a misdemeanor or a felony (known as a “wobbler” offense) depending upon the prosecutor’s charging decision and the actual punishment imposed by the trial court. As a misdemeanor, identity theft is punishable by up to one year in county jail and/or a fine of up to \$1000. It may also be punishable as a felony by imprisonment in the state prison for a term of 16 months, two years, or three years in state prison, and/or a fine up to \$10,000.

Personal identifying information means any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license, or identification number, social security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the person, address or routing code, telecommunication identifying information or access device, information contained in a birth or death certificate, or credit card number of an individual person, or an equivalent form of identification.

Statute: Penal Code § 530.5: (must scroll down to relevant section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>

Jurisdiction: The jurisdiction for a criminal action for identity theft offenses may be the county where the theft occurred, the county where the information was illegally used, or the the county in which the victim resided at the time the offense was committed. If similar identity theft crimes occur in multiple jurisdictions, any one of those jurisdictions can be used for all of the offenses.

Statute: Penal Code §786(b): (must scroll down to appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=777-795>

Statute of Limitations: To give victims, law enforcement, and prosecutors a reasonable opportunity to discover and identify crimes of identity theft, state law provides that the statute of limitations for the crime begins when the crime was discovered, instead of when it was committed.

Statute: Penal Code §803.5: (must scroll down to appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=799-805>

Government Documents: State law provides that a person who possesses a birth certificate (genuine or counterfeit) with the intent to conceal his/her identity or to represent himself/herself as the person named in the document is guilty of a misdemeanor. It is an alternate misdemeanor-felony offense for a person to manufacture, sell, offer, or transfer a purported birth certificate, where the defendant intends to deceive and knows the document is counterfeit.

Statute: Penal Code §529a: (must scroll down to the appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>

It is a misdemeanor to possess document-making devices with intent to use them to manufacture, alter, or authenticate a deceptive identification document.

Statute: Penal Code §483.5: (must scroll down to appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=470-483.5>

Payment Cards: Any person who acquires or retains possession of access card account information, without the cardholder's or issuer's consent, with the intent to use it fraudulently, is guilty of grand theft. A person who with intent to defraud, acquires or retains an access card, with the intent to use, sell, or transfer the card, is guilty of petty theft. A person who within a twelve-month period, acquires access cards issued in the names of four or more people which he has reason to know were taken or retained fraudulently, is guilty of grand theft.

Statute: Penal Code §484e: (must scroll down to the appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9>

Any person who publishes the number or code of an existing, canceled, revoked, expired or nonexistent access card, personal identification number, computer password, access code, debit card number, bank account number, or the numbering or coding which is employed in the issuance of access cards, with the intent that it be used or with knowledge or reason to believe that it will be used to avoid the payment of any lawful charge, or with intent to defraud or aid another in defrauding, is guilty of a misdemeanor.

Statute: Penal Code §484j: (must scroll down to the appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9>

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 with intent to defraud. Scanning devices are electronic devices that are 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 misdemeanor, punishable by up to one year in jail and/or a fine of up to \$1000.

Statute: Penal Code §502.6: (must scroll down to the appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9>

Under state law, a person or entity that intentionally remotely reads or attempts to remotely read a person's identification document using radio frequency identification (RFID), for the purpose of reading that person's identification document without that person's knowledge and prior consent, will be punished by imprisonment in a county jail for up to one year and/or a fine of up to \$1500. There are exceptions for inadvertent scanning and also permits various emergency medical services and law enforcement agencies to scan without a bearer's permission to identify or assist an unresponsive person, or to solve a crime, as long as a search warrant has been issued.

Text of Legislation: http://www.leginfo.ca.gov/pub/07-08/bill/sen/sb_0001-0050/sb_31_bill_20080930_chaptered.html

Phishing: State law prohibits phishing the act of posing as a legitimate company or government agency in an email, Web page, or other Internet communication in order to trick a recipient into revealing his or her personal information. It makes it unlawful for any person, through the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be an online business without the approval or authority of the online business.

Statute: Business and Professions Code §22948-22948.3: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22948-22948.3>

Spyware: State law prohibits an authorized person from knowingly installing or providing software that performs certain functions, such as taking control of the computer or collecting personally identifiable information. It specifically prevents the collection, through intentionally deceptive means, personally identifiable information, through the use of a keystroke-logger or by extracting it for a purpose unrelated to the purpose of the software or service.

Statute: Business and Professions Code §22947: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22947-22947.6>

Social Security Numbers: California law contains numerous protections for Social Security numbers (SSN). It prohibits businesses, governments, and other entities from publicly displaying or posting an individual's SSN; printing SSNs on ID cards or badges; printing SSNs on documents mailed to customers, unless the law requires it or the document is a form or application; printing SSNs on postcards or any other mailer where its visible without opening an envelope; avoiding legal requirements by encoding or embedding SSNs in cards or documents, such as using a bar code, chip or magnetic strip; requiring people to send SSNs over the Internet, unless the connection is secure or the number is encrypted; and requiring people to use an SSN to log onto a web site, unless a password is also used. Organizations may continue their current practices for using SSNs for existing customers, rather than stopping the practices barred by the new law described above, unless a customer requests otherwise in writing.

Statute: Civil Code §1798.85-1798.86: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.85-1798.86>

Protection of Personal Information: State law requires businesses to use safeguards to ensure the security of personal information, defined as an individual's name, plus his/her Social Security number (SSN), driver's license or state identification number, financial account numbers, and to contractually require third parties to do the same

Statute: Civil Code §1798.81.5: (must scroll down to appropriate section)
<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84>

Change of Address: State law requires a credit card issuer or telephone company that receives a request for a change of address on an account and then within a specified period receives a request for a new credit card or service to notify the consumer at the former address of record.

Statute: Civil Code §1799.1b: (must scroll down to appropriate section)
<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1799.1-1799.1b>

State law requires a credit card issuer that receives an application with a different address in response to a mailed unsolicited offer to verify the change of address.

Statute: Civil Code §1747.06: (must scroll down to appropriate section)
<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1747-1748.7>

Victim Assistance:

Mandatory Police Reports: A person who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over his or her actual residence or place of business, which is required to 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 law enforcement agency where the suspected crime was committed for further investigation of the facts.

Statute: Penal Code §530.6: (must scroll down to relevant section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>

Criminal Identity Theft: A person who reasonably believes that he or she is the victim of identity theft may petition a court for an expedited judicial determination of his or her factual innocence, in cases where the perpetrator of the identity theft was arrested for, cited for, or convicted of a crime under the victim's identity, or where a criminal complaint has been filed against the perpetrator in the victim's name, or where the victim's identity has been mistakenly associated with a record of criminal conviction. If the victim is found factually innocent, the court must issue an order certifying this determination, and may order the name and associated personal identifying information contained in court records, files, and indexes accessible by the public be deleted, sealed, or labeled to show that the data is impersonated and does not reflect the defendant's identity.

Statute: Penal Code §530.6: (must scroll down to relevant section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>

If a person obtains personal identifying information of another person, uses that information to commit a crime in addition to the crime of identity theft, the court records must reflect that the person whose identity was falsely used to commit the crime did not commit the crime.

Statute: Penal Code §530.5: (must scroll down to relevant section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>

The California Department of Justice maintains a registry to assist victims of criminal identity theft, in which a suspect in a criminal investigation identifies himself using the identity of another, innocent person. The registry is available to help victims of identity theft who are wrongly linked to crimes, by providing a centralized place that can be checked by police and other authorized persons to confirm that a person is not wanted by law enforcement and that a mistaken criminal history was created in his name.

Victims who have been charged with a crime committed by another person using his/her stolen identity or those whose identity has been mistakenly associated with a record of criminal conviction can register to enter their name into the Identity Theft Database. In most cases of criminal identity theft, victims must go to court to obtain an order from a judge stating they are "factually innocent" of the crime on their record. Once confirmed, the information is entered in a statewide database and can be used to show others that a he/she was not actually responsible for the crime. The information is available via a toll-free number to the identity theft victim, criminal justice agencies, law enforcement, and other individuals and agencies authorized by the victim to see the information.

Statute: Penal Code § 530.7: (must scroll down to the appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>

"Identity Theft Registry" (<http://ag.ca.gov/idtheft/general.php>)

"How to Use the Identity Theft Registry"

(<http://www.privacyprotection.ca.gov/sheets/cis8englsih.pdf>)

"Petition Forms" (<http://www.privacyprotection.ca.gov/sheets/cis8petition.pdf>)

"Registry Forms" (<http://www.privacyprotection.ca.gov/sheets/cis8registry.pdf>)

Access to Records on Fraudulent Accounts: State law allows identity theft victims or their law enforcement representatives to obtain copies of documents on fraudulent accounts from the financial institution or utility where the accounts were opened. The financial institutions and businesses are required to release to a victim with a police report or to the victim's law enforcement representative information and evidence related to the accounts. This includes information related to the application or account, such as a copy of the unauthorized person's application or application information and a record of transactions or charges associated with the application or account. The requested information must be provided within 10 days of receiving the request at no cost.

Statute: Penal Code §530.8: (must scroll down to appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=528-539>

Civil Code §1748.95: (must scroll down to appropriate section) <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1748.9-1748.14>

Financial Code §4002: (must scroll down to appropriate section) <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=03001-04000&file=4000-4002>

Financial Code §22470: (must scroll down to appropriate section) <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=fin&group=22001-23000&file=22470>

“Requesting Fraudulent Transaction or Account Information”

(http://www.privacyprotection.ca.gov/lawenforcement/le_instructions.htm)

“Identity Theft Victim’s Request for Fraudulent Transaction / Account Information

(<http://www.privacyprotection.ca.gov/lawenforcement/inforequestformpc530.pdf>)

“Instructions for Identity Theft Victims on Requesting Fraudulent Transaction/Account

Information” (<http://www.privacyprotection.ca.gov/lawenforcement/victiminstructions530.pdf>)

Destruction of Records: State law requires businesses to take all reasonable steps to destroy, or arrange for the destruction, of a customer’s records within its custody or control that contain personal information that is no longer to be retained by the business. This can be done by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means. Personal information means any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including, but not limited to his/her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver’s license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit or debit card number, or any other financial information.

Statute: Civil Code §1798.81: (must scroll down to appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84>

Security Freeze: State law allows all 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. Credit reporting agencies may charge \$10 to implement a freeze or to temporarily lift

a freeze for a specific time period or for a specific creditor. Seniors over 65 may be charged no more than \$5, and victims of identity theft may not be charged.

The reporting agency must place the freeze within three business days after receiving the request, and within ten 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.

Statute: Civil Code § 1780.11.2 through 1785.11.6 (must scroll down to relevant section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1785.10-1785.19.5>

Office of Privacy Protection, “How to Freeze Your Credit Files”:

<http://www.privacyprotection.ca.gov/sheets/cis10securityfreeze.pdf>

Security Breach: State law requires state agencies and businesses operating in the state 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 occurs upon “unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity” of personal information. Disclosure must occur to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an authorized person. The disclosure must be made in the most expedient time possible, and without unreasonable delay, consistent with legitimate needs of law enforcement.

Personal information means an individual’s first name or first initial and his/her 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 or redacted: Social Security number; driver’s license or California identification card number; 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; or medical information. Publicly available information is not included.

Notification can be provided to the affected persons 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 entity or business 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: Civil Code §1798.82: (must scroll down to appropriate section)

<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84>

“What to Do If Your Personal Information is Compromised”

<http://www.privacyprotection.ca.gov/financial/sbfs021205.pdf>

Security breach notification laws and procedures also apply to electronic medical or health information. California residents must be notified when their unencrypted medical histories, information on mental or physical conditions, medical treatments and diagnoses, insurance policy or subscriber number, insurance applications, claims history, or appeals are breached.

Statute: Civil Code §56.06: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=56-56.07>

Prohibition Against Debt Collectors: State law prohibits debt collectors from pursuing collection of a debt when an alleged debtor provides a police report of identity theft and other information on his status as an identity theft victim. The bill also helps identity theft victims clear up their records by requiring debt collectors who cease collection activities to notify the creditors and consumer credit reporting agencies to which the collector previously provided adverse information.

Statute: Civil Code §1788.18: (must scroll down to appropriate section)
<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1788.10-1788.18>

In addition, state law gives identity theft victims the right to bring an action against a claimant who is seeking payment on a debt not owed by the identity theft victim. The victim may seek an injunction against the claimant, plus actual damages, costs, a civil penalty, and other relief.

Statute: Civil Code §1798.92-1798.97: <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.92-1798.97>

Free Credit Reports: State law provides that an identity theft victim who provides the credit bureau with a copy of a police report is entitled to twelve free credit reports, one per month, in the twelve months from the date of the police report.

Statute: Civil Code §1785.15.3: (must scroll down to the appropriate section)
<http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1785.10-1785.19.5>

State Resources:

Office of the Attorney General, “Identity Theft” (<http://ag.ca.gov/idtheft/>)

“Tips for Victims” (<http://ag.ca.gov/idtheft/tips.php>)

This site directs victims to: *“File a Report with Local Police of Police Where Identity Theft Occurred: Get a copy of the police report and retain for your records. Credit card companies and financial institutions may require you to show a copy of this report to verify the crime. Keep the phone number of your investigator and provide it to creditors and others who require verification of your case.”*

Office of Privacy Protection, “Identity Theft”
(http://www.oispp.ca.gov/consumer_privacy/identitytheft.asp)

“Top Ten Tips for Identity Theft Protection”

(http://www.oispp.ca.gov/consumer_privacy/consumer/documents/html/cis1english.asp)

“Identity Theft Victim Checklist”

(http://www.oispp.ca.gov/consumer_privacy/consumer/documents/html/cis3english.asp)

This document directs victims to: “Report the Crime to the Police: Under California law, you can report identity theft to your local police department. Ask the police to issue a police report of identity theft. Give the police as much information on the theft as possible. One way to do this is to provide copies of your credit reports showing the items related to identity theft. Black out other items not related to identity theft. Give the police any new evidence you collect to add to your report. Be sure to get a copy of your police report. You will need to give copies to creditors and the credit bureaus.”

It also informs victims that: *“When you file your police report of identity theft, the officer may give you forms to use to request account information from credit grantors, utilities or cell phone service companies. If the officer does not do this, you can use the form available from the Office of Privacy Protection in Consumer Information Sheet 3A, “Requesting Information on Fraudulent Accounts.” When you write to creditors where the thief opened or applied for accounts, send copies of the forms, along with copies of the police report. Give the information you receive from creditors to the officer investigating your case.”*

“Requesting Information on Fraudulent Accounts: A Guide for Identity Theft Victims”

(<http://www.privacyprotection.ca.gov/sheets/cis3aenglish.pdf>)

This document includes the appropriate form for requesting a copy of application and business transaction records relating to fraudulent transactions or accounts opened or applied for using an identity theft victim’s name and directions for its use.

“Your Social Security Number: Controlling the Key to Identity Theft”

(http://www.oispp.ca.gov/consumer_privacy/consumer/documents/html/cis3aenglish.asp)

“When Your Child’s Identity is Stolen”

(http://www.oispp.ca.gov/consumer_privacy/consumer/documents/html/cis3benglish.asp)

“Identity Theft and the Deceased”

(http://www.oispp.ca.gov/consumer_privacy/consumer/documents/html/cis3cenglish.asp)

“Information for Law Enforcement”

(http://www.oispp.ca.gov/consumer_privacy/law_enforcement/)

“The links below give law enforcement officers materials they can use to help victims of identity theft. The Victim Checklist and the Affidavit can be given to victims to use as they take all the steps necessary to clear up their records. “How to Use the California Identity Theft Registry” (with its related forms) can be given to victims who have a criminal record created in their name by an identity thief. In addition, Penal Code section 530.8 makes it possible for identity theft victims or their law enforcement representatives to get copies of documents on fraudulent accounts from the financial institution or utility where the accounts were opened. The link for Requesting Fraudulent Account Information leads to forms to use for requesting the information.

Officers may direct victims who need additional assistance in clearing up their records to the Office of Privacy Protection's Web site and toll-free number, 866-785-9663."

- Identity Theft Victim Checklist (http://www.oispp.ca.gov/consumer_privacy/consumer/documents/html/cis3english.asp)
- Identity Theft Affidavit (<http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>)
- Identity Theft Affidavit in Spanish (<http://www.ftc.gov/bcp/online/spanish/credit/s-affidavit.pdf>)
- Requesting Fraudulent Transaction or Account Information (http://www.oispp.ca.gov/consumer_privacy/law_enforcement/instructions.asp)
 - "Identity Theft Victim's Request for Fraudulent Transaction / Account Information" (http://www.oispp.ca.gov/consumer_privacy/law_enforcement/documents/pdf/inforequestformpc530.pdf)
 - "Instructions for Identity Theft Victims on Requesting Fraudulent Transaction/Account Information" (http://www.oispp.ca.gov/consumer_privacy/law_enforcement/documents/pdf/victiminstructions530.pdf)
- "How to Use the California Identity Theft Registry – A Guide for Victims of "Criminal" Identity Theft" (http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis8english.pdf)
 - Petition Form (http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis8petition.pdf)
 - Registry Forms (http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis8registry.pdf)

Division of Motor Vehicles, "Have You Been A Victim of Identity Theft?" (http://www.dmv.ca.gov/pubs/brochures/fast_facts/ffd124.htm)

Legislation:

2008:

AB 372 makes changes to the state's law that allows consumers to place freezes on their credit files. The bill caps fees at \$10, down from \$12, and lowers the maximum cost to seniors 65 or over to \$5. It also requires the credit reporting agencies to accept requests by regular mail, instead of only by certified mail, and requires agencies to comply for requests within three business days, down from five business days.

SB 612 allows prosecutors to charge people with identity theft in the jurisdictions where the victims live. Previously, prosecutions could only take place where the crime occurred, usually in the jurisdiction of the perpetrators' residence.

SB 31 makes it illegal to surreptitiously read personal information stored on radio frequency identification (RFID) tags without an owner's knowledge and permission. Violators would be punished by imprisonment in a county jail for up to one year, and/or a fine up to \$1500. The bill makes exceptions for inadvertent scanning and also permits various emergency medical services and law enforcement agencies to scan without a bearer's permission to identify or assist an

unresponsive person, or to solve a crime, as long as a search warrant has been issued. The use of RFID technology has become more widespread to encode information on identification documents, such as driver's licenses, passports, health insurance cards, and other ID cards.

2007:

Under **AB 1298**, California residents must be notified when their electronic medical information or health information has been exposed. Specifically, it expands the state's data breach notification law to include unencrypted medical histories, information on mental or physical conditions, and medical treatments and diagnoses. It also covers unencrypted insurance policy or subscriber number, any applications for insurance, claims histories and appeals. The law also prevents any company that holds electronic personal health records from disclosing that information without consent. The exposed information must include a California resident's name to require notification, but does not need to include Social Security numbers. The law applies to state agencies and any company that does business with Californians, even if its headquarters are not in the state. The data breach law previously covered only financial information.

AB 1168 requires the Secretary of State and all county recorders to truncate Social Security numbers (SSNs) in records they hold so that no more than the last four digits are displayed to the public. In addition, the Franchise Tax Board will be required to truncate SSNs on lien abstracts that it files as public documents. It also requires universities and colleges to truncate SSNs in their electronic student and employee records, and allows the Secretary of State's office to stop certain financial documents from being filed if they contain more than the last four digits of a SSN.

Governor Arnold Schwarzenegger vetoed a bill (**AB 779**) that would have increased the state's data protection standards. The bill would have required retailers in California who failed to follow accepted security guidelines to reimburse credit unions and banks for the costs associated with alerting customers and reissuing cards after a data breach. It would also have prohibited merchants from storing specific types of authentication data taken from the magnetic stripe on the back of credit and debit cards. In addition, the bill would have required all entities accepting payment card transactions to use strong encryption routines and access controls while storing and transmitting data such as card verification values and personal identification numbers. Retailers also would have been forced to disclose more details about breaches, including a description of the categories of personal data that might have been compromised. Gov. Schwarzenegger objected to the broad scope of the law and argued that compliance would be excessively costly and burdensome for small businesses. He also argued that the industry is better equipped than lawmakers to evaluate the need for higher standards.

2006:

AB 2886 seeks to crack down on criminals who possess stolen personal information that they then use to commit large-scale identity theft. The legislation increases penalties for repeat offenders and possessing the data of ten or more persons used for trafficking and financial fraud. The bill also makes mail theft a misdemeanor offense on the state level. The legislation proportionately sentences repeat offenders and increases penalties for identity theft by punishing the crime as a felony in some cases. The mail-theft provisions help alleviate the United States

Postal Inspection Service's caseload by granting authority to California law enforcement to investigate and prosecute cases involving mail theft.

To help law enforcement agencies spot identity theft trends and more effectively combat the growing crime, **SB 1390** requires the California Department of Justice to publish data regarding identity theft arrests in its annual report of crime statistics. Separating out identity theft arrest information will create more accurate criminal justice statistical data.

2005:

AB 1566 increases the penalty for identity theft crimes if the victim is a member of the armed forces, reserves, or National Guard, who has been called to active duty and is deployed to a location outside of the state. Violations are punished by one year in county jail and/or a fine up to \$1500.

SB 355 targets phishing, the act of posing as a legitimate company or government agency in an email, Web page, or other Internet communication in order to trick a recipient into revealing his or her personal information. The bill makes it unlawful for any person, through the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be an online business without the approval or authority of the online business.

2003:

The Legislature passed several bills to give victims of identity theft greater protections.

- **AB 610** will require creditors to take reasonable steps to verify a consumer's first and last name as well as their social security number when inconsistent information is discovered on their credit report. The bill is designed to protect consumers from identity theft stemming from unverified inconsistent personal information on credit reports.
- **AB 763** bans a person or business from sending an envelope or postcard that displays all or part of a Social Security number
- **AB 1105** gives identity theft victims more access and time under legal statutes to discover and research identity theft crimes against them. The bill prohibits the statute of limitations for identity theft cases from beginning until the crime has been discovered and does not expire until four years after the date of discovery. Due to the nature of the crime, it is not uncommon for an identity theft victim to be unaware of the crime until after it has been committed.
- **AB 1772** allows an identity theft victim to obtain information on unauthorized mail receipts, forwarding addresses, rental applications and evidence of accounts fraudulently made in their name. Under the existing law, an identity thief can fraudulently use a victim's name to create confidential business accounts and complete application forms. This bill would permit victims of identity theft to obtain this confidential information to prevent the continuation of the crime.
- **AB 1773** allows law enforcement to get a search warrant from a local magistrate, instead of waiting for a foreign jurisdictional judge, when the warrant is related to an identity theft case and the victim lives in the same county as the issuing court.
- **AB 1294** requires debt collectors to stop trying to collect debts from debtors who provide a police report showing that they are a victim of identity theft.

- **SB 25** seeks to prevent identity theft by reducing the exposure of consumers' Social Security Numbers to identity thieves and requiring credit issuers to verify the identity of the applicant if the credit report contains a security alert. The bill enhances protections against identity theft by barring state agencies, including colleges and universities, from using Social Security numbers in ID cards and other public documents. It also forces credit bureaus to honor fraud alerts placed by consumers who suspect they are victims of identity theft.
- **SB 125** allows identity theft victims and law enforcement officers to obtain copies of applications and application information submitted by the identity thief to various creditors and agencies without having to submit a subpoena. It also eases the ability of victims to restore their identities and strengthens law enforcement officials' ability to prosecute identity thieves.
- **SB 602** requires credit reporting agencies to notify consumers before the expiration of credit report security alerts, which are placed by people who think they may have been victims of identity theft. The law also restricts bars and other businesses from electronically swiping driver's licenses to collect encoded data.
- **SB 684** allows people who suspect they are identity theft victims to get more information about unauthorized changes to existing accounts and new applications for credit.
- **SB 752** allows identity theft victims who are accused of crimes to clear their names through comparison thumbprints of victim and thief.

2002:

The Legislature passed numerous bills to deal with the growing problem of identity theft and fraud. These include:

- **AB 1155** authorizes courts to impose a fine of \$25,000 on an individual who is convicted of a felony for conspiring to commit identity theft. This bill also makes it a misdemeanor for any person to obtain, or assist another person in obtaining a driver's license, identification card, vehicle registration certificate, or other official document issued by the Department of Motor Vehicles to which that person is not entitled. This bill emanates from a recommendation adopted early in 2001 by DMV's task force on identity theft. The task force found that it is difficult under current law to prosecute DMV employees who assist identity thieves in obtaining driver's licenses in the name of other individuals.
- **SB 1254** makes it a misdemeanor to acquire and possess another person's specified identifying information and expands the definition of identity theft. This bill will also make various changes to current law regarding release of information to identity theft victims.
- **AB 1773** allows a district attorney to prosecute a person for identity theft offense in the county where the information was taken, or in the county where the information was used for illegal purpose. Supporters argue that since identity theft crimes can occur simultaneously in dozens of counties within the state, allowing these crimes to be joined and prosecuted in a single county will greatly enhance the prosecution of these crimes.
- **SB 1239** requires credit-reporting agencies to give identity theft victims the right to block fraudulent information and get a free copy of their credit reports once a month for a year in order to monitor their financial information.
- **AB 1219** ensures that the burden for rectifying crimes of identity theft is not solely the victim's. The law allows a court or prosecuting attorney to move for an expedited judicial determination of factual innocence for a victim. The bill also allows the court to order the removal of the victim's name from court records and files. Once a victim of identity theft has

been wrongly accused, cited for or convicted of a crime, it is a long and tedious process to correct.

- **SB 1386** requires state agencies and businesses that maintain computerized data to disclose any breach of security that includes personal information. It requires that consumers be notified if their personal or financial information was accessed by unauthorized individuals. This gives consumers notice that unauthorized individuals have acquired their personal and/or financial information, thereby giving them the opportunity to take proactive steps to ensure that they do not become victims of identity theft.