



# California Identity Theft Laws and Application Security

## AB 1950, SB 1386 and Beyond

*Cenzic developed this white paper with the assistance of  
Infoliance, Inc. [www.infoliance.com](http://www.infoliance.com)*

*Nothing in this white paper is intended as legal advice. Please consult  
legal counsel if you have legal questions.*



## Table of Contents

Executive Summary .....	3
Rising Public Anxiety About Identity Theft .....	3
The California Legislature Steps In.....	4
SB 1386: Security Breach Notification.....	5
Who Is Covered? .....	5
What Information Is Covered? .....	5
What Is Required?.....	5
What Triggers the Notification Requirement?.....	6
Remedies.....	6
Direct and Indirect Compliance .....	6
AB 1950: Protection of Personal Information.....	6
Who Is Covered? .....	6
What Information Is Covered? .....	7
What Is Required?.....	7
Remedies.....	7
Identity Theft Laws beyond California.....	8
The Application Security Link in the Compliance Chain .....	8
Cenzic’s Application Security Solutions for Assisting in Identity Theft Law Compliance .....	9
About Cenzic .....	10
California Identity Theft Law Compliance Chart.....	11
Appendix .....	14
Section 1798.29 .....	14
Section 1798.81.5 .....	15
Section 1798.82 .....	16
Section 1798.84 .....	17
Footnotes.....	18



## Executive Summary

An April 2002 security breach at California's Stephen P. Teale Data Center triggered public outrage. It eventually led to California's security breach notification law called SB 1386. SB 1386 calls for notification of California residents following some kinds of security breaches. On January 1, 2005, California legislation called AB 1950 went into effect. It requires businesses to protect certain "personal information." A steady wave of security breaches involving the theft or loss of personal information in 2005 underscores the vulnerability of personal information to hackers seeking identity theft targets. It is likely that incident response costs, legal fees, and the losses from tarnished reputations imposed enormous costs on the organizations falling prey to these security breaches.

AB 1950 addresses companies owning or licensing certain personal information about California residents. These companies must implement reasonable security procedures and practices to prevent the unauthorized access, destruction, use, modification, or disclosure of that personal information. SB 1386 requires businesses and state agencies to notify California residences of breaches in the security of certain "personal information" in computerized records. Other states have enacted legislation similar to SB 1386. Federal legislation is pending in Congress.

Application security and automated tools to assess application security vulnerabilities protect computerized information accessible through online applications (Cloud, Mobile and Web apps that connect to back-end systems). Accordingly, application security tools are crucial for preventing unauthorized access, destruction, use, modification, or disclosure of personal information available through online applications, as required by AB 1950. Cenzic's application security solutions helps companies comply with AB 1950, because companies can use automated processes to assess risk, check for vulnerabilities, test code and controls during software development for the purpose of preventing unauthorized access, destruction, use, modification, or disclosure of personal information. Also, companies that successfully prevent security breaches have no breaches to report under SB 1386 or similar laws. And Cenzic's application security solutions are a key tool to preventing breaches from occurring.

## Rising Public Anxiety About Identity Theft

On April 5, 2002, hackers exploited vulnerabilities in a server holding a database of personnel information on California's 265,000 state employees. The victims included then-Governor Grey Davis and 120 state legislators. The security breach at California's Stephen P. Teale Data Center in Rancho Cordova compromised names, Social Security numbers, and payroll information. Public outrage soon followed the May 24, 2002 public disclosure of the breach. For almost two months, the State failed to discover the breach in a timely fashion and tell the affected employees.

The fallout from the public clamoring for legislative protection, likely bolstered by the personal impact on state legislators, led to the enactment of a new type of law. California's legislature enacted a security breach notification law known as SB 1386. As described in more detail in the next section, SB 1386 requires businesses to notify California residents of a breach in the security of certain kinds of personal information.

Over time, the Teale Data Center breach has proven to be only the first of many publicly announced high-profile security breaches of personal information. The latest wave of notices started in February 2005 with the announcement from information broker ChoicePoint. ChoicePoint sold personal information to identity thieves posing as legitimate customers of its information services.

The ChoicePoint breaches, and similar breaches affecting LexisNexis, involved imposters using a "social engineering" attack to obtain legitimate credentials to access databases. Other recent incidents arose from the physical loss of backup tapes holding customer information<sup>1</sup>. Other breaches, however, have involved hackers gaining unauthorized access to applications and information. Examples include:

- DSW Shoe Warehouse (hackers obtained unauthorized access to database of credit card numbers and checking information)
- Tufts University (compromise of an outside server containing personal information)



- HSBC North America/Polo Ralph Lauren (reissue of credit cards became necessary following unauthorized access to Polo credit card transactional information due to software vulnerability)
- University of California, San Diego (a hacker gained unauthorized access to databases containing names, Social Security numbers, and driver's licenses)
- Stanford University (hacker gained access to network and database containing names and Social Security numbers)
- CardSystems Solutions Inc. (hackers penetrated the network and gained unauthorized access to cardholder names, account numbers, expiration dates, and card codes)

The increasing frequency of announcements of high-profile security breaches is likely the result of SB 1386 and similar laws requiring companies to notify customers when their private information is compromised. Companies experiencing and announcing these breaches may have a direct reporting requirement under SB 1386. They may also have disclosed breaches, as in the case of ChoicePoint, because they felt or anticipated pressure from state attorneys general to disclose breaches to affected residents of their states, even in the absence of breach notification legislation.

As with the Teale Data Center announcement in California, the result of these increasingly frequent security breach announcements has been nationwide demand (and legislator sympathy) for new laws to protect the public. Legislatures have enacted breach notification laws in almost 20 states and over ten more state legislatures are considering it. At the federal level, a number of competing breach notification bills have been introduced.

The impact of public outrage may extend far beyond legislative action, though. Companies experiencing breaches face hefty costs involved in responding to the breaches, such as investigation costs, remediation, and legal fees. Less easy to measure, but a real concern for the bottom line, is the loss of reputation from a breach. Some customers may not want to do businesses with companies they perceive as having careless security practices. The loss of revenue from these customers will affect the company's health. In the case of CardSystems, the loss of Visa and Amex as customers may well drive the company into bankruptcy<sup>2</sup>. Finally, public anger sometimes turns to lawsuits, as shown by the class action complaints filed against ChoicePoint and CardSystems. The cost of lawsuits in legal fees, along with the associated disruption to the business, will be significant for these companies.

## The California Legislature Steps In

Throughout recent decades, California has proven to be on the forefront of many trends in the law. The areas of privacy and identity theft are prominent examples. Following the incident at the Teale Data Center, the California legislature enacted SB 1386, and then-Governor Grey Davis signed the bill in September 2002. SB 1386 became effective on July 1, 2003 and was the first significant breach notification law in the country. In 2005, following ChoicePoint and other highly publicized security breaches, SB 1386 became the inspiration for almost 20 other state laws and federal bills.

The California Legislation, however, did not stop with security breach notification. Significantly, breach notification laws do not by themselves require companies to do anything to protect personal information. They merely require reporting a breach after the fact to affected residents if a breach takes place. Thus, breach notification laws arguably leave a loophole: they do nothing to prevent the breaches from occurring in the first place.

Perhaps because of this perceived gap, the California legislature followed SB 1386 with legislation directed at the care of personal information to prevent breaches. Signed by Governor Schwarzenegger in September 2004, the new legislation known as AB 1950 became effective on January 1, 2005. Unlike SB 1386, AB 1950 does require companies to prevent breaches from occurring.



Like SB 1386, AB 1950 sets a new trend. AB 1950 was the first law in the United States that required companies to adopt information security practices where coverage is not specific to particular industries or sectors. Before AB 1950, information security legislative focused on specific sectors, such as government, financial services, and health care. If SB 1386 is any indication, AB 1950 may serve as a model for future legislation in other states.<sup>3</sup>

The remainder of this Section discusses SB 1386 and AB 1950, and describes what they say and require. Subsection (a) focuses on SB 1386 and its requirements. Subsection (b) follows with a discussion of AB 1950. The remaining Sections describe examples of the types of security controls and safeguards these laws require.

## SB 1386: Security Breach Notification

The SB 1386 legislation, which became three sections of the California Civil Code, calls for notification following security breaches. One section covers California state agencies.<sup>4</sup> Another section covers businesses conducting business in California.<sup>5</sup> The third section discusses remedies for violations of the law.<sup>6</sup>

### Who is covered?

A copy of the Civil Code sections enacted by SB 1386 appears in the Appendix.

In particular, SB 1386 covers any person or business that conducts business in California owning or licensing computerized data comprising “personal information” as defined in the law.<sup>7</sup> The law does not say what constitutes “conducting business” in California, although courts interpreting the law may apply traditional legal concepts by analogy.

For instance, the Corporations Code says that foreign corporations cannot “transact intrastate business” in California until they first obtain a certificate of qualification.<sup>8</sup> For this purpose, “transacting business” means “entering into repeated and successive transactions” of business in California, “other than interstate or foreign commerce.”<sup>9</sup> Although no reported court cases have interpreted SB 1386’s “conducts business” language, a court may very well of California need to be concerned about compliance with SB 1386.

SB 1386 also covers state agencies, as well as persons and businesses. Covered agencies are those that own or license computerized data that include “personal information.”<sup>10</sup>

Also, note that SB 1386 only applies to organizations owning or licensing personal information in computerized form. Breaches involving paper records do not trigger SB 1386 obligations. Nonetheless, pending legislation would extend breach notification requirements to businesses holding paper records derived from computerized records.

### What Information Is Covered?

SB 1386 addresses unencrypted “personal information.” “Personal information” means a first and last name or first initial and last name in combination with one of the following:

- Social Security number.
- Driver’s license or California Identification Card number.
- Account number, credit card number, or debit card number in combination with a security code allowing access to a financial account.<sup>11</sup>

Information is “personal information” when either the name or one of the above data elements is unencrypted. SB 1386, however, excludes from “personal information” any publicly available federal, state, or local government records.<sup>12</sup>

### What Is Required?

SB 1386 requires a covered business or state agency to notify California residents affected by a security breach of their unencrypted personal information. The duty is to make the disclosure “in the most expedient time possible” and “without unreasonable delay.”<sup>13</sup> The notification may be



delayed if a law enforcement agency determines that it would impede a criminal investigation, but notification must occur after it would not compromise an investigation.<sup>14</sup> A business or agency can also delay notification “to determine the scope of the breach” and “restore the reasonable integrity” of its systems.<sup>15</sup>

Notice must be given in writing, via electronic notice under the federal E-Sign Act, or using certain methods of substitute notice if notice would be burdensome in terms of cost (more than \$250,000), number of recipients (more than 500,000), or the lack of available contact information.<sup>16</sup> If an agency or business has its own notification procedures as part of an information security policy that is consistent with the timing requirement in the law, then notice under that policy will satisfy the notification requirement.<sup>17</sup>

### **What Triggers the Notification Requirement?**

The requirement of notifying California residents arises when the business or agency experiences a “breach of the security of the system” where residents’ “unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”<sup>18</sup> A “breach of the security of the system” occurs when there has been an “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information.”<sup>19</sup>

The legislature attempted to exclude any accidental unauthorized access from the notification requirement. For instance, if an employee of a covered agency or business is doing work for the employer and obtains unauthorized access as part of doing his or her job in “good faith,” then the disclosure is not a breach as long as no further unauthorized disclosure takes place.<sup>20</sup>

### **Remedies**

A “customer” injured by a covered business’s violation of SB 1386 can sue the business to recover damages.<sup>21</sup> A court can also issue an injunction to stop the business from violating SB 1386.<sup>22</sup> A business cannot avoid liability by having the injured person sign a waiver of rights under SB 1386, and any such waiver is void.<sup>23</sup>

A violation of SB 1386 would involve a business’s failure to notify an affected California resident following a security breach. Alternatively, the resident could sue the business if the business unreasonably delayed in notifying the resident. The violation of SB 1386, however, would not arise from the breach itself, but rather only the failure or delay in notification.

### **Direct and Indirect Compliance**

SB 1386 does not require covered businesses or agencies to take any precautions to prevent security breaches. Rather, SB 1386 is directed to notification following a breach. Thus, direct compliance with SB 1386 focuses on following the incident response requirements of notification to affected California residents.

Another, more indirect, route to compliance is possible, though. If a covered business or agency can avoid breaches from occurring in the first place, it will not trigger a notification requirement or face the risk of violating SB 1386’s requirements. The best way for a business or agency to avoid the expense, loss of reputation and liability following notices to customers of a security breach is to take steps to prevent breaches from occurring at all.

### **AB 1950: Protection of Personal Information**

AB 1950 takes the logical next step following breach notification and requires actual security controls to protect certain “personal information” as defined in its section of the California Civil Code.<sup>24</sup> A copy of that section appears in the Appendix. By enacting AB 1950, the Legislature intended to protect the personal information about California residents by encouraging business to adopt reasonable security practices.<sup>25</sup>



### **Who Is Covered?**

AB 1950 covers any business that owns or licenses “personal information” about a California resident. The law specifically covers businesses that own or license “personal information” that is part of the business’s internal customer account records or held in order to transact business with the resident.<sup>26</sup>

Note that AB 1950 does not cover state agencies. On the other hand, AB 1950 may extend further than SB 1386 in that its scope is not limited to businesses that “conducts business” in California. In addition, AB 1950 is not limited to businesses holding “computerized data.” Thus, it apparently covers businesses holding records that are exclusively in paper form.

AB 1950, however, contains a series of exclusions. It does not apply to health care providers, plans, or contractors covered by state privacy laws or health care entities covered by the federal Health Insurance Portability and Accountability Act.<sup>27</sup> AB 1950 also excludes financial institutions<sup>28</sup> and entities receiving driver’s license information under contracts under the California Vehicle Code and its confidentiality provisions.<sup>29</sup> Finally, AB 1950 contains a catch-all exclusion for businesses falling within more stringent state or federal laws.<sup>30</sup>

### **What Information Is Covered?**

AB 1950 contains its own definition of “personal information.” The law begins by defining “personal information” the same as SB 1386: first name or initial and last name in combination with a Social Security number, driver’s license or identification card, or account number in combination with an access code.<sup>31</sup> AB 1950, however, also sweeps in “medical information” within the definition of “personal information.”<sup>32</sup>

Significantly, AB 1950 does not limit itself to unencrypted “personal information.” Thus, the security requirements of AB 1950 apply whether or not the personal information is encrypted. Nonetheless, like SB 1386, “personal information” does not include publicly available federal, state, or local government records.<sup>33</sup>

### **What Is Required?**

AB 1950 requires covered businesses to “implement and maintain reasonable security procedures and practices.” The procedures and practices must “protect the personal information” against the listed threats: “unauthorized access, destruction, use, modification, or disclosure.” AB 1950 does not require a “one size fits all” approach. Rather, the covered business need only implement those procedures and practices that are “appropriate to the nature of the information.”<sup>34</sup>

For businesses sharing personal information about California residents with nonaffiliated third parties, an additional security control applies. In specific, the covered business sharing the information must require the third party, by contract, to implement and maintain the same kind of reasonable security procedures and practices the covered business must implement. That is, the contract with the third party must require the third party to use reasonable procedures and practices “appropriate to the nature of the information” to protect personal information from “unauthorized access, destruction, use, modification, or disclosure.”<sup>35</sup>

### **Remedies**

AB 1950 appears in the same title of the Civil Code as SB 1386. The remedies of lawsuits for damages and a court injunction under Civil Code Section 1798.84 apply to violations of any section in the title, including the sections introduced by AB 1950 or SB 1386. Thus, the remedies listed above for SB 1386 apply to AB 1950 as well. Of note, however, is the fact that with the addition of AB 1950, an injured California resident can sue not just for the failure or delay in notifying the resident of the breach. Rather, AB 1950 now allows the resident to sue for damages caused by the breach itself.



## Identity Theft Laws beyond California

Although California has frequently led the states in legal innovation (for good or ill), and California is an important and large state, California is not the only state to weigh in on identity theft issues. Almost 20 states have adopted some form of security breach notification law, and legislation is pending at the federal level and in over 10 more states. Therefore, businesses outside of California will have to determine whether state or local laws impose breach notification requirements, even if they are not bound by California identity theft laws.

Clearly, though, the laws in states outside California have their inspiration in SB 1386. The laws in states such as Arkansas, Montana, North Dakota, and Washington closely resemble California's SB 1386. Each state's law, however, must be examined to determine differences with SB 1386.

For instance, one issue dealt with differently by the various states is what event triggers the notification requirement. Some states have raised the bar on the trigger for notification to avoid requiring notification when the breach is minor or unlikely to lead to harm.

In any case, these state laws deal with security breach notification. As with SB 1386, direct compliance focuses on incident response and proper notice to affected residents. Nonetheless, as with SB 1386, the least painful method of compliance is indirect compliance by way of security controls to prevent breaches from occurring, making breach notification unnecessary. Moreover, at least one state has adopted a law similar to AB 1950.<sup>36</sup>

## The Application Security Link in the Compliance Chain

Online merchants and other businesses with Cloud, Mobile or Web applications see the compelling business opportunity to reach new customers and increase their sales through the Internet. Nevertheless, they also want to avoid the fate of companies like DSW Shoe Warehouse. Accordingly, securing their applications has become a top priority.

Securing applications involves performing a risk assessment to identify the universe of possible security threats in a rapidly-changing environment. In particular, businesses will want to know whether their Cloud, Mobile and Web applications have vulnerabilities and what those vulnerabilities are. Whether businesses procure online applications or develop them in-house, they will likely be judged on the efforts they take to ensure that they have minimized security risks affecting their applications.

AB 1950 places a large premium on preventing unauthorized access to personal information. Nonetheless, application security controls cannot be a mere afterthought, added just before moving a code base to production systems. Rather, application security should be part of the design, and security should be checked during development by QA engineers or information security professionals. For instance, the application should not permit hackers using malicious code or injection techniques to utilize inputs to obtain unauthorized access to information or cause a buffer overflow enabling the hacker to gain control over a server hosting a Cloud, Mobile or Web application.

Following the implementation of a Cloud, Mobile or Web application on production systems, periodic retesting is important to ferret out vulnerabilities that can only be seen in the application's operating environment. Some vulnerabilities are apparent only when the application is in run time. For instance, session hijacking techniques pose a threat of unauthorized access to an application user's data and may permit a hacker to perform operations to misuse data as if the hacker were the user. Since AB 1950 requires businesses to prevent unauthorized access to or misuse of personal information, businesses hosting Cloud, Mobile or Web applications that make use of personal information must check for vulnerabilities to threats like session hijacking.

Although many of the security vulnerabilities involved with securing Cloud, Mobile or Web applications are well-known, businesses procuring these applications are not always assessing or managing the risks efficiently. Traditional risk management has involved highly manual assessment and testing techniques. For instance, a business could hire someone to perform



manual penetration testing of its applications, although with time pressures to roll out applications before competitors, the testing may not be as timely or thorough as a company may want. Also, time pressures turn security professionals into bottlenecks during development, while everyone waits for them to conduct the tests and document the results adequately for appropriate follow-up. Moreover, in the absence of internal resources, businesses find it necessary to hire outside consultants and system integrators to perform the tests at an extremely high cost, sometimes \$100,000 per assessment or more.

Some businesses implementing Cloud, Mobile or Web applications have used rudimentary tools for preliminary scanning, but these static scanning-based tools frequently prove to be inadequate. Their main failing is the large number of false positives and the limit in the range of vulnerabilities they can uncover. With these limits, these scanning tools add little value.

### **Cenzic's Application Security Solutions for Assisting in Identity Theft Law Compliance**

Cenzic's application security solutions provide a solution to businesses seeking to secure Cloud, Mobile or Web applications in an automated fashion with limited staff and time to perform testing. Cenzic's Hailstorm technology uses a Stateful Assessment™ approach. Businesses implementing Cloud, Mobile or Web applications can use Cenzic's solutions to perform automated security quality assurance checks on their applications. In addition, it can make use of user-defined tests for detection of vulnerabilities to attacks, such as phishing, circumvention of access controls, and code injection.

Cenzic's application security solutions help businesses with Cloud, Mobile or Web applications protect personal information. The automated checks it performs expose vulnerabilities and thus helps to prevent unauthorized access, destruction, use, modification, or disclosure as required by AB 1950. Cenzic's solutions play a crucial role for companies that need to protect Cloud, Mobile and Web applications. Further, companies successfully preventing security breaches through the rigorous testing made possible by Cenzic have no breaches to report to customers under laws like SB 1386. For more information showing how Cenzic's solutions facilitate AB 1950 and SB 1386 compliance, see the compliance chart at the end of this white paper.

Also, Cenzic has created a package of policies addressing SB 1386. It checks for vulnerabilities associated with unauthorized access or disclosure of sensitive data, such as personal information. For example, one policy checks whether forms are submitted to an application unencrypted, when the application should be using SSL.

In addition to facilitating compliance, Cenzic's application security solutions provide crucial benefits for businesses deploying Cloud, Mobile or Web applications. Most importantly, Cenzic allows businesses with these applications to obtain the results of manual penetration testing at a fraction of the cost.

Automated checking permits developers to test for vulnerabilities more frequently throughout the software development lifecycle in a more closely controlled manner. Not only can checking be done more frequently, but Cenzic makes it more practical to test earlier in the development lifecycle, saving development and testing costs.

Cenzic's application security solutions provide a single, consistent security control during the development process. Its ability to check and recheck for vulnerabilities facilitates change control. If the business procuring a Cloud, Mobile or Web application uses a third party to develop the code, Cenzic again assists in providing a disciplined control during the development. The business can use Cenzic as an assessment tool to ensure the developer is creating secure code.

Cenzic's application security solutions also saves time for otherwise busy security staff members and prevents them from becoming bottlenecks during development. Security professionals can use their knowledge to design tests, manage the review process, and review the tests results. They don't need to conduct and repeat manual tests themselves. QA engineers can use Cenzic to perform the tests in an automated fashion instead of taking up the time of security professionals.



Even after development or procurement, and a Cloud, Mobile or Web application goes live on production systems, the business can use Cenzic’s solutions for continued assessment to check for the application’s security in the production environment. Any new vulnerabilities that are uncovered can inform changes in security policies for appropriate responses, can motivate code changes, and can help in the design of new tests for additional future assessments. The Cenzic Intelligence Lab (CIA) continually develops new attack objects. Cenzic provides these objects to customers as updates on a regular basis. Because 400+ new application vulnerabilities appear every month, the updates from Cenzic’s CIA permit customers to stay ahead of new developments.

### About Cenzic

Cenzic provides an application security intelligence platform to continuously assess Cloud, Mobile and Web vulnerabilities. This helps brands of all sizes protect their reputation and manage security risk in the face of malicious attacks. Today, Cenzic secures more than half a million online applications and trillions of dollars of commerce for Fortune 1000 companies, all major security companies, government agencies, universities and SMBs.

### Cenzic Products

Cenzic Enterprise	Cenzic Enterprise is a software solution that assesses the security of Cloud and Web applications and supports security risk management throughout the software development lifecycle. Cenzic Enterprise provides a company-wide view of security vulnerabilities and status to executives as well as customized views for other users from a Web-based dashboard.
Cenzic Desktop	Cenzic Desktop is a single-user version of Cenzic Enterprise. It is designed for the power user that wants to run their security assessments on Cloud and Web applications from a single system.
Cenzic Managed Cloud	With Cenzic Managed Cloud, Cenzic’s security experts remotely perform full vulnerability testing on Cloud, Mobile and Web applications. From a Web-based dashboard, users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Cloud	Cenzic Cloud allows users to test their own Cloud and Web applications for basic attacks and receive actionable results all within their own Web portal – no security experts needed.
Cenzic Hybrid – Software + Cloud	Cenzic Hybrid provides access to both Cenzic Enterprise software and Cenzic Managed Cloud services. Vulnerability testing can be done either by using the software on premise or by leveraging Cenzic’s expert security services team.
Cenzic Mobile	Cenzic Mobile service is delivered as a managed service. Cenzic’s security experts remotely perform full vulnerability testing on mobile applications. All testing is managed from a Web-based dashboard where users can request assessments, view results, run reports, analyze trends and re-test applications to verify remediation efforts.
Cenzic Services	Cenzic services and training help those responsible for Cloud, Mobile and Web application security to implement best practices and procedures to protect data from hacker attacks.



### California Identity Theft Law Compliance Chart

This chart contains examples of the features and policies, in Cenzip solutions, that facilitate compliance with AB 1950’s requirements and avoiding breaches that would trigger the need for notification under SB 1386 and similar laws. These policies are from Cenzip’s policy packages for “best practices” and SB 1386 programs. In addition, Cenzip’s application security solutions allow users to write custom objects to address specific potential vulnerabilities for a given Cloud, Mobile or Web application.

#### Preventing Unauthorized Access

Requirement in California Civil Code	Manual Testing and Available Scanning Tools	Cenzip
A business owning or licensing personal information about a California resident shall implement and maintain reasonable security procedures and practices to protect against unauthorized access. <sup>37</sup>	<p>Some password security tools enable enforcement of password policies. Other enforcement entails manually checking to ensure that access control is enforced.</p> <p>Manual checking to determine if hackers can bypass authentication schemes without supplying authentication information.</p> <p>See below for additional unauthorized access capabilities. Unauthorized access occurs before data can be destroyed, used, modified, or disclosed without authorization.</p>	<p>Automated checks for consistent application of access control policies, such as requirements for strong passwords, enforcement at registration, and lock-out following login failure.</p> <p>Automated tests to flag Web applications permitting hackers to bypass authentication schemes, such as through session hijacking, manipulation of session credentials, and replay attacks.</p> <p>See below for additional unauthorized access capabilities. Unauthorized access occurs before data can be destroyed, used, modified, or disclosed without authorization.</p>

#### Preventing Unauthorized Data Destruction

Requirement in California Civil Code	Manual Testing and Available Scanning Tools	Cenzip
A business owning or licensing personal information about a California resident shall implement and maintain reasonable security procedures and practices to protect against unauthorized destruction. <sup>38</sup>	See “Preventing Unauthorized Access” and “Preventing Unauthorized Use.” Unauthorized access or use precedes unauthorized data destruction.	See “Preventing Unauthorized Access” and “Preventing Unauthorized Use.” Unauthorized access or use precedes unauthorized data destruction.



**Preventing Unauthorized Use**

Requirement in California Civil Code	Manual Testing and Available Scanning Tools	Cenzic
A business owning or licensing personal information about a California resident shall implement and maintain reasonable security procedures and practices to protect against unauthorized use. <sup>39</sup>	Some tools to check the vulnerability to injection attacks and buffer overflows, but otherwise manual testing is required.  See also "Preventing Unauthorized Access."	Automated checking of Web applications for vulnerabilities to known injection attacks and buffer overflows permitting attackers to take control of host computers.  See also "Preventing Unauthorized Access."

**Preventing Unauthorized Modification**

Requirement in California Civil Code	Manual Testing and Available Scanning Tools	Cenzic
A business owning or licensing personal information about a California resident shall implement and maintain reasonable security procedures and practices to protect against unauthorized modification. <sup>40</sup>	See "Preventing Unauthorized Access" and "Preventing Unauthorized Use." Unauthorized access or use is a prelude to unauthorized modification.	See "Preventing Unauthorized Access" and "Preventing Unauthorized Use." Unauthorized access or use is a prelude to unauthorized modification.

**Preventing Unauthorized Disclosure**

Requirement in California Civil Code	Manual Testing and Available Scanning Tools	Cenzic
A business owning or licensing personal information about a California resident shall implement and maintain reasonable security procedures and practices to protect against unauthorized disclosure. <sup>41</sup>	Manual penetration testing used to determine if files, directories, and directory listings are remotely accessible without authorized access.  Manual testing for cross-frame scripting and cross-site scripting vulnerabilities.  Manual checking for forms permitting content caching.	Automated checking for ability to obtain unauthorized access to remotely accessible files, directories, and directory listings. Files and directories may contain personal information.  Policies to permit automated checking for cross-frame scripting and cross-site scripting vulnerabilities that could expose personal information to unauthorized disclosure.  Policy for automated checking for forms which allow content caching of data such as personal information.



**Oversight of Nonaffiliated Third Parties**

Requirement in California Civil Code	Manual Testing and Available Scanning Tools	Cenzic
<p>A business that discloses personal information about a California resident to a nonaffiliated third party shall require, by contract, that the third party implement and maintain reasonable security procedures and practices.<sup>42</sup></p>	<p>Manual testing of nonaffiliated third parties receiving personal information, which tends to occur at random times. While not explicit in the statute, a contract requiring a third party to use security procedures and practices will be effective only if the business can assess the third party's performance of contractual security requirements.</p>	<p>Facilitates systematic checking of nonaffiliated third parties' protection of personal information from unauthorized access, destruction, use, modification, or disclosure, as described above.</p>

**Encryption of Personal Information**

Requirement in California Civil Code	Manual Testing and Available Scanning Tools	Cenzic
<p>Although SB 1386 does not require businesses or state agencies to encrypt computerized personal information about a California resident, a security breach triggers a notification requirement only if the personal information is unencrypted.<sup>43</sup></p>	<p>Manual, ad hoc testing to ensure that data are encrypted during Web application sessions. Thus, businesses and state agencies encrypting all personal information will fall outside the breach notification requirements of SB 1386.</p>	<p>Cenzic can run automated tests to determine if https pages can be accessed through http, fooling users into believing their sessions are encrypted, when they are not.</p> <p>Automated checking for forms that should be using SSL for submission but do not.</p>



## Appendix

SB 1386 and AB 1950: Selected Sections from the California Civil Code

### Section 1798.29.

Disclosure of breach of security by agency that owns or maintains computerized data [SB 1386].

- A. Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- B. Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- C. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
- D. For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
- E. For purposes of this section, “personal information” means 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:
  1. Social security number.
  2. Driver’s license number or California Identification Card number.
  3. Account number, 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.
- F. For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- G. For purposes of this section, “notice” may be provided by one of the following methods:
  1. Written notice.
  2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
  3. Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$ 250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:
    - a. E-mail notice when the agency has an e-mail address for the subject persons.
    - b. Conspicuous posting of the notice on the agency’s Web site page, if the agency maintains one.
    - c. Notification to major statewide media.



- H. Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

**Section 1798.81.5.**

Intent of legislature; Reasonable security procedures; Contract required for similar protection upon disclosure; Definitions; Exceptions to applicability [AB 1950]

- A. It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information. For the purpose of this section, the phrase “owns or licenses” is intended to include, but is not limited to, personal information that a business retains as part of the business’ internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.
- B. A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.
- C. A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.
- D. For purposes of this section:
1. “Personal information” means an individual’s first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the date elements are not encrypted or redacted:
    - a. Social security number.
    - b. Driver’s license number or California identification card number.
    - c. Account number, 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.
    - d. Medical information.
  2. “Medical information” means any individually identifiable information, in electronic or physical form, regarding the individual’s medical history or medical treatment or diagnosis by a health care professional.
  3. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- E. The provisions of this section do not apply to any of the following:
1. A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).
  2. A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code.
  3. A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).



4. An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.
5. A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

**Section 1798.82.**

Disclosure of breach insecurity by business maintaining computerized data that includes personal information [SB 1386]

- A. Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- B. Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
- C. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.
- D. For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
- E. For purposes of this section, “personal information” means 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:
  1. Social security number.
  2. Driver’s license number or California Identification Card number.
  3. Account number, 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.
- F. For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- G. For purposes of this section, “notice” may be provided by one of the following methods:
  1. Written notice.
  2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.



3. Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$ 250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
  - a. E-mail notice when the person or business has an e-mail address for the subject persons.
  - b. Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
  - c. Notification to major statewide media.
- H. Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

**Section 1798.84.**

Violations and remedies [applies to SB 1386 and AB 1950]

- A. Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
- B. Any customer injured by a violation of this title may institute a civil action to recover damages.
- C. In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars (\$ 3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars (\$ 500) per violation for a violation of Section 1798.83.
- D. Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.
- E. Any business that violates, proposes to violate, or has violated this title may be enjoined.
- F. A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.
- G. The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.



## Footnotes

- 1 Companies announcing the loss of backup tapes in 2005 include Bank of America, Ameritrade, and CitiFinancial.
- 2 Evan Schuman, Data-Theft Case Proves Need for New Disclosure Law, CIO Insight (Jul. 22, 2005) <<http://www.cioinsight.com/article2/0.1540.1840121.00.asp>>.
- 3 For instance, Arkansas has adopted a personal information protection law very similar to AB 1950. Ark. Code Section 4-110-104(b).
- 4 Cal. Civil Code Section 1798.29.
- 5 Section 1798.82.
- 6 Section 1798.84.
- 7 Section 1798.82(a).
- 8 Corporations Code Section 2105(a).
- 9 Section 191(a).
- 10 Civil Code Section 1798.29(a).
- 11 Sections 1798.29(e), 1798.82(e).
- 12 Sections 1798.29(f), 1798.82(f).
- 13 Sections 1798.29(a), 1798.82(a).
- 14 Sections 1798.29(c), 1798.82(c).
- 15 Sections 1798.29(a), 1798.82(a).
- 16 Sections 1798.29(g), 1798.82(g).
- 17 Sections 1798.29(h), 1798.82(h).
- 18 Sections 1798.29(a), 1798.82(a).
- 19 Sections 1798.29(d), 1798.82(d).
- 20 See Sections 1798.29(d), 1798.82(d).
- 21 Section 1798.84(b). Note that Section 1798.84 does not apply to state agencies.
- 22 Section 1798.84(e).
- 23 Section 1798.84(a).
- 24 Civil Code Section 1798.81.5.
- 25 See Section 1798.81.5(a).
- 26 Section 1798.81.5(a).
- 27 Section 1798.81.5(e)(1), (3).
- 28 Section 1798.81.5(e)(2). AB 1950 defines “financial institution” with reference to a section in the California Financial Code that refers to the same definition in 12 U.S.C. Section 1843(k) that the federal Gramm-Leach-Bliley Act (GLBA) uses. Effectively, if a financial institution is covered by GLBA, it is excluded from the scope of AB 1950.
- 29 Civil Code Section 1798.81.5(e)(4).
- 30 Section 1798.81.5(e)(5).



- 31 Section 1798.81.5(d)(1)(A)-(C).
- 32 Section 1798.81.5(d)(1)(D).
- 33 Section 1798.81.5(d)(3).
- 34 Section 1798.81.5(b).
- 35 Section 1798.81.5(c).
- 36 For instance, Arkansas has adopted a personal information protection law very similar to AB 1950. Ark. Code Section 4-110-104(b) and more may do so in the future. These laws will emphasize the need for effective security controls to prevent breaches.
- 37 Cal. Civil Code Section 1798.81.5(b).
- 38 Section 1798.81.5(b).
- 39 Section 1798.81.5(b).
- 40 Section 1798.81.5(b).
- 41 Section 1798.81.5(b).
- 42 Section 1798.81.5(c).
- 43 See Sections 1798.29(a), 1798.82(a).