CALIFORNIA

Basic Information on community association operations in this state

1. Is UCA the legal basis for community associations?	YES	**NO**
2. Do state laws/regulations (in general) apply to Condominium Associations and Homeowner Associations, and Coop Associations equally**?** • **The Common Interest Development Act (aka Davis-Stirling Act)** governs all. Common interest communities are typically referred to as HOAs. Civil Code 4000-6150. • **Certified Common Interest Development Manager. Business and Professions Code 10000-11506.** • **SB 745 housing omnibus bill** annually updates non-controversial provisions or mistakes in Davis-Stirling Act	**YES**	NO

3. What state agency regulates community associations or management?

DEPARTMENT OF CONSUMER AFFAIRS, REAL ESTATE DIVISION

4. Are community associations, HOAs registered as business entities or nonprofit corporations?

NONPROFIT, MUTUAL BENEFIT CORPORATIONS
Unincorporated associations are treated the same as mutual benefit corporations under CA law.

- **Nonprofit Corporation Law** is addressed in sections 5000 through10841 of the Corporations Code.

5. How many community associations in this state? *(Source: CAI Fact Book 2016 Statistics)*	**45,400 est'd**
6. Does this state have laws that regulate use of technology?	**YES** NO
If Yes, do these laws impact: • Information privacy; • Data access; • Identity Theft; • Data breaches?	 YES YES YES YES

Key Statutes - Association/CID specific Cyber Security, Data Access and Privacy

- **Civil Code §4045** specifies that the notice must be printed and placed in a "prominent location." The use of websites by associations to post notices does NOT meet these requirements. However, use of websites does comply with the "**ease of access**" requirement.
- **Civil Code §4055 –** defines the requirements of delivery via electronic means: requirement is satisfied if the information is provided in an electronic record *capable of retention* by the recipient. An electronic record is not capable of retention if the sender or its information processing system inhibits the *ability of the recipient to print or store the electronic record*.

Relevant Legislative Trends

Statutes that took effect in 2016 expanded security provisions and remedies for breach.

- **AB 1710 (Dickinson and Wieckowski) Data Breach, Information Security, SSN Confidentiality** ... requires sources of a breach to offer identity theft prevention and mitigation services to affected individuals at no cost, for no less than 12 months. The bill expands the information security law to require businesses that maintain, as well as those that own or license, the personal information of California residents to use reasonable and appropriate security measures to protect the information. Civil Code §§ 1798.81.5, 1798.82, 1798.85
- **SB 570 (Jackson) Breach Notice Format** requires data breach notices to be titled "Notice of Data Breach" and to follow a standard format. It also provides a model breach notice form. It requires that organizations who notify victims using the "substitute notice" method to post a website link to the notice conspicuously, as defined, and maintain the notice on the website for at least 30 days. In addition it defines the content requirements including the font size of notices. *Civil Code §§ 1798.29 and 1798.82*
    - Several amendments to security breach notification law S.B. 570 amend the required content of security breach notices, requiring that notices clearly and conspicuously display certain prescribed headings. A.B. 964 now defines the term "encrypted" for purposes of California's breach notification law as "rendered unusable, unreadable, or indecipherable to an unauthorised person through a security technology or methodology generally accepted in the field of information security." Both amendments went into effect on 1 January 2016.
- **AB 2828 (Chau) Data breach: encryption key**
  This law amends the data breach notification law to require notification of a breach of encrypted personal information, but only when the encryption key or security credential that could render the personal information readable or useable was, or is reasonably believed to have been, acquired by an unauthorized person. *Civil Code §§ 1798.29 and 1798.82 (amended)*
- **SB 1137** Status: Signed by Governor. Chap. 725
  Provides that ransomware is a computer contaminant that restricts access to the infected computer and demands that the user pay a ransom to remove the restriction. Makes it a crime for a person to knowingly introduce ransomware into any computer, computer system, or computer network.

- **AB 1412** Status: Signed by Governor.

Sacramento - Governor Brown signed Assembly Bill 1412, which corrects a problem created by one of last year's bills. When an absentee owner fails to annually update their contact information, AB 1412 allows associations to use the last address provided by the owner. The bill also extends limitations on personal liability to volunteer officers and directors of mixed-use developments. For more information, see AB 1412.

https://www.oag.ca.gov/privacy/privacy-legislation/leg2015

Statutes related to Data Security/retention/protection/disposal and penalties

Focus of statutes is on electronic data forms.

- **Cal. Civ. Code §§ 1798.81, 1798.81.5, 1798.82 and 1798.84** require that businesses **protect information** with reasonable and appropriate security, define personal information, and also **apply to data disposal within the private sector**. The law requires any person or business that conducts business in California and that owns or licenses computerized data that includes personal information to **disclose any breach** of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorized person..
- **Calif. Govt. Code § 8592.30-8592.45** defines **data breach notifications** and requires a consistent format, provides a template, and describes acceptable alternate notifications.

California defines private information more broadly than other states,

- It does not require a risk of harm analysis to require notification
- It does require notice to the Attorney general, within a specified time frame.
- It does permit private cause of action

As of January 1, 2017, California law will no longer include an encryption safe harbor.

- **A.B. 1541**, which amends the definition of "personal information" in the state's data privacy statute to include:
  - a username or e-mail address combined with a password or security question and answer for access to an online account; and
  - health insurance information.

Another California statute,

Identity theft statutes and penalties

California privacy law is enacted within the Business & Professions Codes, Civil codes, and Penal codes, and Health and Safety codes.

- **ID theft statute California Penal Code §368** – addressies crimes against vulnerable parties (elders, dependent adults, and persons with disabilities) with a focus on theft, embezzlement, forgery or fraud or violation of **§530.5** proscribing identity theft

- **AB 1541 (Assembly Privacy and Consumer Protection Committee) Information Security –** mentioned previously, adds (1) a username of email address in

combination with password or security question and answer; and (2) health insurance information to the definition of personally identifiable information.

- **Cal. Penal Code §530.5 to 530.8** Personal Information Trafficking and Mail Theft Prevention Act
- **California's unauthorized computer access law, Penal Code 502(c)** PC, is an important California internet fraud law. Also known as the "Comprehensive Computer Data Access and Fraud Act," this law makes it a serious crime to access a computer, computer data, or a computer network without permission (and usually with an unlawful purpose). Unlike with many other forms of California fraud, you can be guilty of unauthorized access to a computer even if you don't actually defraud anyone out of money or property
    - 1. Unauthorized Computer Access: Legal Definition and Penalties
    - 1.1. Unauthorized access; assisting with unauthorized access
    - 1.2. Altering, deleting or taking data
    - 1.3. Disrupting or denying computer services
    - 1.4. Using computer services without permission
    - 1.5. Introducing computer contaminants
    - 1.6. Using someone else's domain name or profile
    - 1.7. Unauthorized access to government or public safety computer systems
    - 1.8. Additional penalties

Related General Business/Organization Statutes (non-specific to Associations)

Most statutes related to data protection, breaches, and communication are in civil code. (Cal. Civ. Code §§ 1280.15, 1798.29, 1798.80, 1798.82 (as amended, 2016), 1798.84)

http://www.dwt.com/california/ however also references health and safety code 1280.15 and relates it to electronic media....Personally identifying information is defined as the person's surname in combination with any of a list of other identifying data including passwords.

Note - Association board members may be protected by the language that items collected "in good faith by employees or agents" are excluded.

https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf
https://www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart2017.pdf#page=12
describes that "notices" if delivered electronically must comply with Section 7001 of Title 15 of the United States Code governing electronic signatures/records