Kimball, Tirey & St. John LLP

Business Record Retention

Jamie Sternberg, Esq. and D. Patrick O'Laughlin, Esq.

Updated July, 2018

Q: How long should a property owner keep business records?

A: The time period to keep records depends on why they are being maintained. Generally records should be retained as long as possible, but at least four years.

There is no single, simple rule establishing the minimum time to retain records. Record retention periods must be determined on a case by case basis, after completing a cost/benefit analysis. The cost to retain the records must be weighed against the likelihood that they will be needed. Think about why the records are being kept. Are you legally required to keep them? Do you have a business need for them? Focusing on the issues you are most concerned about is an important part of the cost/benefit analysis.

One factor to consider is the applicable time limitations that may apply to claims relating to the records. There are many different time periods that could apply. The "statutes of limitations" that are most likely to apply are as follows:

- Two years for a verbal contract, for an alleged breach of a real estate agent's duty to inspect and disclose, or for personal injury
- Three years for certain real estate broker/agent transaction and trust records and for alleged fraud claims
- Four years for a written contract and for an alleged breach of fiduciary duty
- Up to seven years for some IRS purposes (although some have no limitations)
- Ten years for latent (not immediately noticeable) construction defects

Extensions of these time limitations can exist in different situations. Some of these extensions can be based upon:

- Delays in discovery of injury
- Personal injury claims to people younger than 18 years old
- Cross-complaints and indemnity claims

If the records are needed for tax reasons (to establish basis in property or otherwise), you should keep the documents for at least as long as you own the property, plus an additional amount of time, preferably six years or more. While generally the IRS must initiate action to collect taxes within three years from the date the tax return is filed, or two years from the date tax is paid, both the IRS and FTB have six years to start legal action if the taxpayer's income is understated by more than 25%. There is no statute of limitations if a taxpayer files a false or fraudulent return or never files a return at all.

The two most common documents stored by property managers and landlords are leases and tenants' rental applications. Since almost all rental agreements or leases are reduced to writing, landlord should keep leases (or documentary evidence of the terms of the agreement) for at least four years after the tenant vacates.

The information contained in a tenant's rental application can be at issue for claims concerning fair housing among other things. Since fair housing issues can be quite broad and amorphous, there are various statutes of limitations that may be applicable.

While a tenant or former tenant has only a year to file a complaint with HUD of DFEH, there is a two-year statute of limitations on filing a lawsuit based upon discrimination in state or federal court. That statute is tolled if the person first files an administrative complaint with HUD or DFEH (which is extremely common). The time that the case is with the agency does not count against the statute. So, under some circumstances, the statute can be extended to three or more years.

Pursuant to Business & Professions Code §10148, a real estate broker must retain for three (3) years copies of:

- all listings
- deposit receipts
- cancelled checks
- trust records and
- other documents in connection with transactions for which a real estate license is required

The time period begins to run from the date of closing, or if the transaction is not consummated, from the date of listing.

AB 2136, effective January 1, 2015, provides that real estate brokers are not required to maintain electronic messages "of an ephemeral nature" that are not designed to be retained or to create a permanent record, such as text messages and instant messages.

Additionally, a real estate broker must maintain records for four years of funds solicited or accepted for a purchase or loan transaction where the broker (directly or indirectly) obtains use or benefit of funds other than for commissions, fees and costs and expenses.

Generally, retain records for at least four years and if the cost to store the records isn't excessive, consider retaining them for a longer period.

Title 10, Chapter 6, Reg. 2729 specifically authorizes a broker to use electronic image storage media to retain and store copies of required documents provided that:

- The electronic image storage is not erasable and does not allow changes.
- The stored documents are made or preserved in the regular course of business;
- The original record from which the stored document was copied was made or prepared by the broker or broker's employees at or near the time of the act, condition or event reflected in the record;
- The custodian of the record is able to identify the stored document or record, the mode of its preparation, and the mode of storing it on the electronic image storage;
- The electronic image storage media contains a reliable indexing system that provides ready access to a desired document, appropriate quality control of the storage process to ensure a good quality image, and date ordered arrangement of stored documents or records to ensure a consistent and logical flow of paperwork to preclude unnecessary search time.
- The broker maintains at his/her office a means of viewing the electronically stored documents.

If requested by the DRE, the broker is required to provide a paper copy of any document(s) at the broker's expense.

Deciding how long to retain business records is a business decision that should be made after considering the applicable laws, the cost of record retention and the likelihood that the record will be needed.

Safeguarding Sensitive Information

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to have measures in place to maintain the confidentiality and security of sensitive customer information, such as personal credit information. Financial institutions may be defined as businesses, regardless of size, that are significantly engaged in providing financial products or services. The Safeguards Rule requires companies to develop a written information security program that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information at issues. As part of its plan, each company must:

- Designate one or more employees to coordinate its information security program;
- Identify and assess reasonable foreseeable risks to the security, confidentiality and integrity of customer information in each relevant area of the company's operation;
- Design and implement a safeguards program, and regularly monitor and test it;
- Select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

Violating the Safeguards Rule could lead to an administrative enforcement action initiated by the Federal Trade Commission (FTC). The GLBA does not provide consumers with a private right of action. However, because a violation of the GLBA may give rise to a claim under a state's unfair business practices law, consumers may be able to enforce the GLBA utilizing this mechanism.

California specifically requires a business that owns or licenses personal information about a California resident to 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. Generally, client records containing personal information must be destroyed either by shredding, erasing or otherwise modifying the personal information in the records to make it unreadable or undecipherable. "Personal information" is any information that identifies, relates to, describes, or is capable of being associated with a particular individual, including (but not limited to) 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 card number, debit card number, or any other financial information. A violation of the California specific provision may lead to civil liability for damages and/or civil penalties.

Document Destruction

In 2003, the Fair Credit Reporting Act was amended with the creation of the Fair and Accurate Credit Transactions Act (FACTA). Under the umbrella of the FACTA, the Disposal Rule was implemented and became effective June 1, 2005.

Any business, large or small, that uses consumer reports for a business purpose must properly dispose of sensitive information in order to prevent "unauthorized access to or use of the information." Disposal includes shredding, burning, destroying, and/or pulverizing. Sensitive information is defined as data that is identifiable to an individual person and has the potential to be used, such as social security numbers, driver license numbers, credit card numbers, account numbers, passwords, judgments in civil cases, medical information and financial data such as credit ratings.

The Disposal Rule applies to information in paper, computer, or any other format. It requires reasonable disposal measures to protect against unauthorized access to or use of the information, so that the personal information cannot be read or is incapable of being reconstructed. Discarding consumer reports in a trash can is not just an irresponsible business practice, it is also illegal.

Although the Disposal Rule applies to consumer reports and the information derived from consumer reports, the FTC encourages those who dispose of any records containing a consumer's personal or financial information to take similar protective measures. Businesses should also conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Due diligence could include: 1) reviewing an independent audit of a disposal company's operations and/or its compliance with this rule; 2) obtaining information about the disposal company from several references; 3) requiring that the disposal company be certified by a recognized trade association; or 4) reviewing and evaluating the disposal company's information security polices or procedures. The statute indicates these suggestions are examples and are not exclusive or exhaustive methods for compliance.

It is prudent to immediately cease destruction of all potentially relevant or discoverable documents when a lawsuit or government investigation is pending or even threatened. The two-year statute of limitations period dates from the consumer's discovery of the violation, not the date of the violation itself. However, the consumer must bring the action within five years of the date of the violation, regardless of the discovery date. Non-compliance with the Disposal Rule may result in action initiated by the FTC or a private cause of action, where damages may include, but are not limited to, actual damages, punitive damages, statutory damages up to $1,000.00 per violation, civil penalties, costs and attorney's fees.

If you have any questions regarding the contents of this article, please call (800) 574-5587.

Kimball, Tirey & St. John LLP is a full service real estate law firm representing residential and commercial property owners and managers. This article is for general information purposes only. While KTS provides clients with information on legislative changes, our courtesy notifications are not meant to be exhaustive and do not take the place of legislative services or membership in trade associations. Our legal alerts are provided on selected topics and should not be relied upon as a complete report of all new changes of local, state, and federal laws affecting property owners and managers. Laws may have changed since this article was published. Before acting, be sure to receive legal advice from our office. For contact information, please visit our website: www.kts-law.com. For past Legal Alerts, Questions & Answers and Legal Articles, please consult the resource section of our website.

© 2019 Kimball, Tirey and St. John LLP