Navigating the Risks: Privacy and Data Security Considerations in Residential Rental Transactions

Dana B. Rosenfeld

October 21, 2010

Apartment rentals by residential landlords (and their management companies) frequently involve the transfer and processing of personally identifiable information ("PII") from tenants, including bank and credit card information, social security numbers and dates of birth (among other items). Property management companies, apartment building owners, real estate agents and other related businesses may handle a few or many pieces of PII in the course of a single rental transaction. Additionally, these companies may require credit reports, background checks, or criminal records on potential tenants. The collection and use of PII and credit information can create significant risks for businesses if this information is inadvertently disclosed or vulnerable to misuse by hackers or rogue employees.

Businesses that handle PII face a number of legal obligations, and the consequences of not taking privacy and data security obligations seriously can be severe. Companies are confronted with a variety of rigorous laws and regulations, including a wave of state laws that have mandated specific types of data safeguards. From an enforcement perspective, Congress is considering adding civil penalties for data security violations under pending legislation and the Federal Trade Commission has announced several recent settlements with companies that allegedly failed to sufficiently protect personal data under their control.

With the amount of risk associated with managing PII and the consequences for legal violations, how can a residential real estate owner or management company minimize these risks and help ensure compliance with the various federal and state laws governing privacy and data security? This article outlines the privacy and information security considerations that residential real estate owners and management companies should take into consideration when collecting information about tenants.[1]

Privacy Policies

A patchwork of state and federal laws set requirements for providing notice to customers about how an entity collects, uses and protects information. Companies that collect information online should post privacy policies to provide notice to consumers. Companies that do not collect information online but collect PII by other means also should develop privacy policies, including notice to consumers at the time of collection or use of personal information, and data handling and use procedures for their employees to follow. In general, privacy policies should disclose what personal information is collected from tenants, how the personal information is used, what measures are in place to protect the confidentiality of the data, and any parties with whom the tenant's information is

shared.

FCRA

The federal Fair Credit Reporting Act ("FCRA") regulates the activities of consumer reporting agencies ("CRAs"), which is defined as a business that assembles reports containing a consumer's or employee's credit payment records, driving records, criminal history, or other similar information for use by other businesses ("consumer reports"). An investigative consumer report, a separate type of report also regulated under the FCRA, includes interviews with a consumer's or employee's friends, neighbors and associates. A majority of states also have enacted their own versions of the FCRA which may provide for additional consumer protections.

Companies involved in renting residential real estate may use consumer reports or investigative consumer reports for a variety of reasons, including, most commonly, tenant screening. A business seeking to obtain a consumer report for an applicant seeking credit must provide notice to the tenant, obtain consent, and notify the tenant in the event that an adverse decision is reached.[2] Businesses utilizing consumer reports must also have policies and procedures in place to ensure compliance with the federal and, where applicable, state FCRA requirements.

Collection of Information

Information collected should be the minimum necessary for a business purpose; the more data a company holds, the higher the risk of potential liability and damages in the event of a data breach. Thus, companies should review the information commonly collected from prospective or current tenants or other parties, assess the necessity of the information, develop intake and application forms, and train personnel to collect only information needed to facilitate a tenant's prospective rental.

The purpose of collecting information should be clearly stated and the use of the information limited to the stated purpose. For instance, if collected information will be used following a transaction to market services or for advertising purposes, such as joint marketing initiatives with business partners, that use should be clearly disclosed to the tenant at the time the information is collected.

Data Security

Securing data that has been collected is a first and necessary step to developing a comprehensive data security plan. In order to properly secure data, companies usually must engage first in an evaluation of the collection, use and storage of PII. Sensitive PII warranting enhanced security protections includes forms containing social security numbers (SSN), such as credit reports, taxpayer ID numbers, financial information including bank account and credit card information, and criminal history. Among other things, companies should ask where PII is stored and whether it is held in paper form or electronically; what security measures are in place to protect PII from improper distribution; and what training has been provided to employees relating to their access to and use of PII?

Access to PII should be restricted to those employees who have an identifiable business need for the information. PII should be secured and kept confidential by the company's employees and the company's "standard of care" for PII should be included in employee training, policies and procedures. Password protection and/or encryption of data are other important safeguards, and technological issues should be taken into consideration, such as protection of computer systems from hackers or viruses that could expose data. Any transfer of data should only be made with verification of the other party's identity and in compliance with a privacy policy.

Evaluating current data-handling practices provides another opportunity to review how much personal data your business collects and whether the information should continue to be collected. Historically, businesses have collected and stored large volumes of customer and employee data without regard to the usefulness of such data. Nonetheless, limiting data collection and improving security practices can reduce your data security risk profile, in addition to limiting potential data storage costs.

If your business accepts debit or credit cards, such transactions should be conducted in accordance with the Payment Card Industry Data Security Standard ("PCI DSS"). The PCI DSS sets forth standards for processing payments to limit credit card fraud and applies to companies that hold, process or exchange cardholder information from cards issued by the major card brands.

Document Disposal

If some collected PII is no longer essential to your business, such records should be disposed of in a responsible way and in compliance with applicable state or federal laws. For instance, the FCRA requires that consumer reports and information obtained from a CRA that is used or expected to be used for employment purposes be disposed of using practices that are designed to prevent the unauthorized access to - or use of - information in a consumer report.

Reasonable disposal measures could include establishing and complying with policies to:

- burn, pulverize or shred papers so that the information cannot be read or reconstructed;
- destroy or erase electronic files or media so that the information cannot be read or reconstructed; or
- conduct due diligence and hire a document destruction contractor to dispose of material.

Similar methods may be used for proper destruction and disposal of any PII data, regardless of whether it is subject to the FCRA requirements.

Conclusion

In today's environment, with high profile data breaches, the increasing cost and burden of data breach notices, greater consumer awareness of privacy issues, and increasing regulatory activity, reviewing your company's privacy and data security policies in advance of a problem can be a cost-saving step. Forms, training and procedures tailored to your specific business and deliberate data collection and storage policies provide both a defense against privacy or data security breaches and prepare a company to react promptly and properly if a breach does occur. While this article has provided an overview of relevant laws, determining the specific laws and regulations that apply to your residential real estate business activities will give direction and focus to setting appropriate privacy and data security policies.

Kelley Drye & Warren LLP

Kelley Drye & Warren's Privacy and Information Security practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients,

performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

Dana B. Rosenfeld
(202) 342-8588
drosenfeld@kelleydrye.com

---

[1] Note that information collected on employees as part of pre-employment or pre-promotion background checks is also subject to privacy and data security laws and regulations.

[2] Use of consumer reports for employment purposes, whether the initial employment decision or for promotion, reassignment, and retention, have additional requirements, including a pre-adverse action and post-adverse action notice.