NEW LEGAL REQUIREMENTS FOR NY REAL ESTATE COMPANY DATA SECURITY AND PRIVACY

By Kenneth K. Fisher
kfisher@cozen.com

Originally published by the Brooklyn Barrister, Fall 2021

Landlords are used to thinking of themselves as housing people and businesses, but the law looks at them as housing data as well. Just as they are expected to keep their premises safe and secure, they have legal obligations to keep information they collect secure as well, and limitations on how it can be used. With the advent of new requirements, counsel for owners, managers, and service providers should encourage their clients to update their practices and procedures.

It is no surprise that real estate companies are subject to attempts to steal their data, experienced by upwards of 30% of companies according to a 2018 KPMG study. The industry collects sensitive personal and financial data on tenants, as well as its own employee financial, and other private data, but until recently, without the scrutiny imposed on financial services. And, of course, real estate professionals are just as susceptible to brute force phishing attacks indiscriminately targeting email, phones, websites and social media, as anyone else.

Major companies as well as small organizations have been victims of data breaches, including Douglas Elliman Property Management in April of 2021, Long & Foster in 2020 and First American Financial Corp in 2019. These data breaches, which involved millions of sensitive records, are publicly known because of disclosure requirements imposed by statute. Companies in these circumstances are vulnerable to actions by regulators, lawsuits by those whose information was compromised, and ransomware demands by hackers. They also run the risk of damage to their brand and credibility, not to mention disclaimed data breach insurance coverage or future higher premiums.

In addition to data security and privacy obligations, owners and managers have restrictions on the kind of information they can collect about residential tenants from building security systems, and utility systems where provided, and what they can do with that information.

The principal statute, applicable to any business or organization which collects private information, including information landlords routinely collect such as account numbers, credit card numbers and email addresses, is the *NY Stop Hacks and Improve Electronic Data Security Act*, known as the NY SHEILD Law, NY Gen Bus. Law § 899-bb. Adopted by the state legislature in 2019 and supplementing federal laws on credit information collection and privacy [see 16 CFR Part 314, the *Fair Credit Reporting Act* (15 US Code §1681), and the *Gramm-Leach-Bliley Act* (15 USC §6801], the NY SHIELD Law is best known for requiring companies to disclose to parties whose data has been unlawfully exposed, either inadvertently or as a result of criminal activity, that the exposure has occurred.

The law goes beyond this. It imposes an affirmative obligation on organizations which obtain such data to take reasonable steps to safeguard the information. This includes designating who is responsible for the implementation of a data security program, identifying risks and developing procedures to address them, and ensuring that appropriate training is conducted. A threat assessment involves more than company technology. Information stored on premises needs to be physically secure. Third party vendors need to be vetted for their own security precautions. Period updates and improvements, such as two factor authentication requiring a code separate from passwords, are necessary to meet constantly evolving threats.

Another area where both technology and regulation are changing involves the information collected on residential tenants by and for building security systems. Access to the recordings should be password protected, and if possible, on a system that creates a log of who accesses them. Periodic training should remind employees with access to video recordings that they cannot be used for purposes unrelated to work. Owners and managers should also remind their employees that they may violate federal, state or city fair housing laws if tenants are targeted for surveillance based on some discriminatory criteria, such as race, religion or national origin.

Similarly, companies who have or are considering transitioning to “smart access” electronic key fobs and similar systems, instead of physical keys, should be aware that the information collected is regulated, as is the use to which it may be put.

Landlords and their agents cannot discriminate in requiring identifying information or limiting the number of fobs because of any status protected by the fair housing laws.

Owners and managers may require “adequate proof of identity” before issuing a key fob, but not solely a NYS driver’s license, and may not keep a record of a license or passport number, where it was issued or listed address, even if different from the address of the building. Tenant photos may be obtained, but cannot be displayed on the fob itself. The fob system can keep a record of each time it is used to open the front or other door, but may not be used to record when a tenant leaves the building (DHCR Docket No. XK110024OD, 2010)

The City of New York has recently gone a step further with the adoption by the City Council of the Tenant Data Privacy Act on May 28, 2021, Local Law 63 of 2021. Landlords are prohibited from using the data to harass tenants and must remove, anonymize or destroy the information within 90 days and within 90 days after a tenant moves out, unless the information is needed for stopping illegal activity.

The law requires owners to provide tenants with a “plain language” privacy policy. Security safeguards are required. Sale of the collected data is prohibited and tenants have a private right of action for a violation.

The fobs cannot be used to track tenant whereabouts. Moreover, the act goes beyond building access system information. Unless otherwise required by law, a landlord may not collect any information about a tenant’s use of gas, electricity or other utility except total monthly usage. If the landlord is the building internet provider, only aggregated information or information needed for billing purposes can be collected. Commercial use of individual usage information is prohibited.

While the law is currently in effect, however, owners of smart access buildings are not liable for a violation until January 1, 2023, in order to allow owners to replace or upgrade their systems. Landlords who have not established-and maintained-a data security program on the premise that it can’t happen to them, are at risk and should be advised to get into compliance, train their staffs and stay current in this rapidly changing technological environment.