NEW COLORADO LAW CREATES STRICT LIABILITY FOR SECURITY BREACHES OF TENANT PERSONAL INFORMATION

All Landlords Need Appropriate Written Policy To Be In Compliance

Overview

Colorado has a new statute that creates clearer liability for losing a customer's personal information, mandates the development of a written policy covering the destruction of the information, and establishes detailed procedures of how to notify customers in the event of a security breach. In order to comply with the statute, all clients will need to develop the required written destruction policy and should analyze how they store and destroy this information. To the extent this information is transferred to third party vendors (like screening companies and document preparation vendors), it would be prudent to modify the contracts with those vendors to get their warranty of compliance with this statute and an indemnification for their violation of the statue.

The new statute (found at CRS 6-1-713 - effective September 1, 2018), applies to all persons or entities (including landlords) that collect certain personal information. There is no exception for small businesses or landlords. Any person that collects this information is subject to the statue.

What's Covered

In order to assess a company's potential risk and what a proper destruction policy might be, one has to look first at the information covered by the statute. The list is as follows:

- social security number;
- a personal identification number;
- password;
- passcode;
- an official state or government-issued driver's license or identification card number;
- a government passport number;
- biometric data (generally fingerprints, DNA profiles, retina scans, and similar biological information);
- an employer, student, or military identification number;
- or a financial transaction device (credit card or similar electronic fund transfer card).

For most landlords, social security numbers and copies of government issued driver's license or identification cards and/or numbers would be the primary data on this list to be concerned about. However, if the landlord has a web-based payment system or third-party wire transfer system like the Walk in Payment Program (with account numbers, passwords, etc.) there may be other covered information to consider. Student housing providers and those receiving military orders to verify military based lease terminations might end up with still more of this information in their systems.

Project-based subsidized housing providers, who collect and maintain a host of information on sources of income, employer verifications, immigration status for the purpose of certifying the tenant's eligibility for and compliance with the subsidy program will have even more of this information to manage.

Destruction Policy

The first step for compliance with the statute is the development of a written destruction policy. The statute only specifies two considerations that have to be included in that policy, the timing of the destruction and the method.

As to timing, the statute specifies the destruction needs to occur when the information is "no longer needed". That element is certainly greatly open for interpretation, but a case could be made that this information remains "needed" at all times through and including the final settlement of the tenant's move out account (as the landlord might want to have this information available for the collection company).

A reasonable argument can also be made that this information (like all other information and documentation) is needed for the length of the various statutes of limitation for potential legal causes of action held by its customers. While most of the statutes of limitation that apply to landlord/tenant situations are three years or less, there are several that are six years. An industry standard has developed of keeping documentation for at least 7 years so that anything relevant to any claim brought might be available. Based on this standard, reasonable arguments can be made that destruction timing of 7 years after the last business dealings with the tenant is doing no more than keeping the documentation until it is "no longer needed."

Regardless of the outside time limitation on keeping the information, a prudent landlord might reasonably choose to destroy this information more quickly in order to eliminate the potential liability of losing the information.

As to the method of destruction, the statute specifies "shredding, erasing or otherwise modifying the information to make it unreadable or indecipherable." Shredding would seem to be the obvious choice for written documents. Clients will have to get competent IT advice on proper techniques for erasing or modifying electronic data. While not specifically required to be in the Destruction Policy, this statute requires the implementation and maintenance of reasonable security procedures (discussed below) to protect it from unauthorized access, use, modification, disclosure, or destruction. The Destruction Policy would be a convenient and prudent place to recite what those reasonable security procedures might be.

Notification of Security Breaches

The statute also mandates a procedure of notification in the event of a security breach. A security breach is defined as the disclosure of the above personal information in combination with the disclosure of the tenant's name. There is no requirement that procedures for dealing with a security breach be in writing or even be established in advance, only that notification (if and when it should ever have to be given) complies with the statute. Immediate first class mailing of the notice seems the most cost-effective and defensible system of notification.

The notice must include:

- The date, estimated date, or estimated date range of the security breach;
- A description of the personal information that was acquired or reasonably believed to have been acquired;
- Information that the resident can use to contact
- The toll-free numbers, addresses, and websites for consumer reporting agencies;
- The toll-free number, address, and website for the federal trade commission; and
- A statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

Security Measures

The statute requires anyone possessing this information to "implement and maintain reasonable security procedures and the practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations." Beyond this, it gives no guidance as to what a prudent security measure might be. However, it offers a couple of hints.

By defining a security breach as the loss of not only the personal identifying information but also the name of the party to go with it, one can eliminate the possibility of a security breach by making sure the tenant's name does not appear in the same database or document as the various identification numbers. One can envision a document or database that list information like social security numbers, passwords, driver's license numbers, etc. by a random customer number. One would have to reference to a different database or different document to see who the personal information applies to. Additionally, the statute defines a security breach as the "unauthorized" release of information. Therefore, a landlord can improve their position for the release of any information by getting the tenant's advance authorization for that release.

While security measures are beyond the scope of what lawyers have any particular expertise in, it occurs to us that having this information kept on a computer with the internet connectivity creates a risk. Keeping this information in the normal tenant file that is routinely accessed in non-secure environments also creates a risk.

Liability

Arguably causes of action based on negligence theories, breach of contract and breach of implied or express warranties already exist for the loss of this type of confidential information. At first read, one might not think liability had changed much and the only new issues are the required Destruction Policy and notification procedures.

However, the statute provides that the person that loses the information is liable for all damages without a finding of any specific wrongdoing. Therefore, the statute creates strict liability for a landlord for a security breach and will, therefore, make pursuing a cause of action following a security breach much easier. The good news is that the statute does not include a mandatory or minimum penalty. These types of penalties create financial obligations to people even when they have not suffered any specific loss. Consequently, these types of penalties are key ingredients to putting together a successful class-action lawsuit. Without a prescribed minimum penalty, one can anticipate significantly less litigation over the statutory requirements.

Vendor Contracts

The statute creates an obligation to make sure that, if any of this information is voluntarily transferred to a third party, the recipient of the information complies with statutory requirements. This personal information might routinely be transferred to outside screening companies, various vendors who provide services like lease preparation and even to a new management company in the event of an ownership or management changes. These contracts should prudently include a clause whereby the transferee guarantees that they will comply with the requirements of the statute and will indemnify and hold the landlord harmless for any failure to comply with the statute or any security breach as defined by the act. Example language is:

> ***Vendor represents and warrants that it will fully comply with the requirements of C.R.S. 6-1-713 (regarding information destruction and security breaches) and hereby indemnifies and shall hold customer harmless from any and all liability as sociated a violation of the statute and any security breach thereunder.***