LloydSadd INSURANCE BROKERS
NAVACORD®

Protect Tenant Information from Identity Theft

As a property manager, you handle a large volume of personal information. Not only do you have to keep existing tenants' information on hand, but you also have information collected from prospective tenants during the rental process.

Sensitive personal information, like social identification and driver's licence numbers, are essential for, among other things, a thorough background check on possible renters. However, because of the abundance of personal information they are responsible for, more and more property managers are becoming targets of identity theft. If personal information that you are responsible for is obtained and used, you could be liable for the damages. Unfortunately, when property managers are targeted, identity thieves usually take more than just one individual's information, resulting in costly litigation for multiple losses. To protect yourself, it is important to take the appropriate measures to safeguard any personal information given to you by prospective, current and past tenants.

Assuring Tenants

Individuals are becoming increasingly more concerned about how their personal information is handled. The information a potential tenant discloses to you during the leasing process is essentially everything a criminal would need to successfully steal his or her identity. For you, their personal information is necessary to ensure that you are getting a good tenant, but they may still have fears that you need to address. Talking with prospective tenants about the safeguards you have in place can help them feel more comfortable releasing their personal information during the leasing process.

Safeguards

Identity thieves use a number of approaches to obtain personal information. To prevent unauthorized access, you must institute safety measures that strictly manage how personal information is handled. Here are some considerations for securing tenant information:

Computer Protection – Keep electronic attackers from successfully accessing your network by password-protecting files and keeping your virus protection and firewall up to date. Also, avoid storing tenants' personal information on laptops that are frequently used outside the home or office and could be easily stolen. If you need to access this information on the go, consider remote network access that will allow you to get the information you need from a central secure location.

Releasing Information – Personal information should be released only to those persons or organizations specifically authorized by the individual. Never release personal information over the phone, through the mail or electronically unless the receiver's identity has been confirmed as legitimate.

Proper Disposal – Keep electronic attackers from successfully accessing your network by password-protecting files and keeping your virus protection and firewall up to date. Also, avoid storing tenants' personal information on laptops that are frequently used outside the home or office and could be easily stolen. If you need to access this information on the go, consider remote network access that will allow you to get the information you need from a central secure location. Trash is a common target of identity thieves. To stop information from being picked out of the garbage, use a shredder when discarding any paperwork that contains personal information.

Tenant Communications – When communicating with tenants by mail or electronically, always try to include as little sensitive information as possible. If it cannot be avoided, always do your best to ensure that it reaches the tenant in a secure fashion. Put outgoing mail directly into secure collection boxes, and only use electronic forms of communication if there are security measures in place to prevent public access.

Social Insurance Numbers – Keep the number of documents that include Social Insurance numbers to a minimum. Unless listing the number is absolutely essential, do not include it.

Employees – It is important to make wise hiring decisions to prevent employee theft or leaks. Only those employees who require it to carry out their daily duties should have access to tenants' personal information. Employees should not have access to all records, but only to those that apply to their work. If an employee is terminated for any reason, make sure that access to any tenant information is immediately restricted.

Instituting a plan that regulates how your organization deals with tenant information will help keep your tenants safe while protecting your company from liability.

Additional Protection

While your responsibility to the tenant does not include how they themselves protect their sensitive information, there are some things that can be done to make a location less ripe for identity thieves. As mail can often be a target of identity thieves, consider individual mailboxes that require a key to access. To cure the common concern over information being obtained by rummaged-through trash, consider keeping dumpsters in fenced or otherwise enclosed areas. Not only can this prevent opportunities for identity theft, but it can also prevent non-tenants from filling up your waste containers. Providing this additional protection to tenants can show your commitment to safeguarding their personal information.

If you have questions specific to your business, or would like additional information, please reach out to your local advisor.