RISK INSIGHTS Property Management

Crendon Insurance Brokers

Protect Tenant Information from Identity Theft

As a property manager or landlord, 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. Collecting sensitive personal information is essential for thorough tenant referencing. However, because of this abundance of personal information, 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 under the Data Protection Act 1998. Unfortunately, when property managers or landlords are targeted, identity thieves usually take more than just one individual's information, which can result in costly fines. 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

People are becoming increasingly 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. Talking with prospective tenants about the safeguards you have in place can help them feel more comfortable releasing their personal information.

Safeguards

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

Because of the large volumes of person information they keep on hand, more and more property managers and landlords are becoming targets of identity theft.

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 organisations specifically authorised by the individual. Never release personal information over the phone, through the post or electronically unless the receiver's identity has been confirmed as legitimate.

Proper Disposal: Rubbish is a common target of identity thieves. To stop information from being picked out of the rubbish, use a shredder when discarding any paperwork that contains personal information.

Tenant Communications: When communicating with tenants by post 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 post directly into secure collection boxes, and only use electronic forms of communication if there are security measures in place to prevent public access.

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 instead, 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 organisation 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. Because post can often be a target for identity thieves, consider individual post boxes that require a key to access. To cure the common concern over information being obtained by rummaged-through rubbish, consider keeping rubbish bins 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.