



Identity Theft and Information Safeguarding

Industry Awareness and Prevention

By Julia Langston

As a consumer, it is extremely easy to empathize and relate to someone who has been victimized by an identity thief. We've all seen the credit card commercial that shows a victimized middle aged man, defeated in his olive green vinyl recliner, wearing a white tank top t-shirt, speaking in a high pitched woman's voice about a cute lacey designer camisole he just had to buy, with his credit card, for a mere \$1,200.

Yes, some of these commercials are hilarious; others are down right frightening. Yet, all are meant to be eye openers to the growing epidemic of identity theft. Unfortunately, this epidemic mutates and reinvents itself at an alarming rate and it seems identity thieves are always 10 steps ahead of the game.

Identity theft is often thought of in the context of the consumer; an unsuspecting individual has been victimized by disreputable schemers. However, identity theft is not merely a nuisance plaguing consumers, but a problem that is growing exponentially, targeting much larger hosts (businesses) that yield much larger returns. In fact, identity theft and fraud have become a national problem. The Federal Trade Commission's (FTC) identity theft estimate is close to \$50 billion in damages annually.

Multifamily Fights Back

Increased media attention to the issue of identity theft reveals that businesses are attacked on a daily basis, either knowingly or unknowingly. Theft of business information is on the rise and has become a part of our everyday news. Stories about Bank of America, LexisNexis, DSW, and ChoicePoint are glaring examples of the risks businesses face today.

As this problem continues to grow, it's important that property management companies become more aware of their own risks and vulnerabilities, and that the industry as a whole strives to understand the risks associated with identity theft. In turn, it needs to establish prudent

business practices to protect and prevent breaches that can harm the businesses within the industry over time.

Consider the following definition of identity theft and the impact this crime has on the multifamily housing industry: "The compromising of an individual's, an entity's, or an organization's personal or operational information, with the intention of using that information or data to commit fraud, theft, or gain access to additional information, such as, but not limited to, an entity's or organization's resources or their operational activities that can be used to further the scope and breadth of the identity theft-related crime." So how do you protect your business from identity theft? An excellent starting place for any business in the multifamily housing industry is to establish its own unique information safeguarding and security policy.

What Is at Risk?

Recently, the FTC released an information safeguarding rule that outlines obligations businesses have in securing consumer information. However, consumer information is not the only information at risk. Your organization's policies and procedures also are at risk of being used against you in a manner that can breach your security.

With that in mind, it is clear that there are many considerations when establishing an information safeguarding and security policy for a property management business. Especially today, when identity thieves are difficult to detect and not easily identified either before or after an incident has taken place. Identity thieves often adopt various means and methods tailored to the vulnerabilities of a particular organization. This means it's important to use preemptive measures that objectively identify potential risks.

To establish a policy that is preemptive and preventative, your organization must take time to review its own practices, and consider how its business might be



impacted should business-related information, or identifying information of a consumer maintained by your office, be compromised. The genesis of an effective policy begins with being an objective observer and honestly questioning where the vulnerabilities in your operations exist.

Don't hesitate to acknowledge a potential risk or vulnerability and don't just scratch the surface, look deeper into your organization and consider all potential risks. You can sort the critical from the not so critical later. No matter how improbable a breach of your system or operations may seem, have a plan in place and document how you would handle a security breach in the future.

As you begin, you should also understand the potential repercussions associated with not having an effective policy in place: civil lawsuits; federal and state agency complaints; agency actions or fines; media attention; criminal liability; and a loss of revenue or corporate depreciation.

Areas of Vulnerability

As you identify where your property's vulnerabilities lie, be sure to look closely at both internal and external risk. Here is a brief list of vulnerabilities you may want to consider:

Virtual Security

■ Have you reviewed your password and security processes lately? (Business agreements typically require certain assurances about passwords and security of systems used to obtain data.)

■ Does your organization change passwords frequently and use non-obvious passwords (no less than 8 characters, upper and lower case letters, use of numbers and symbols in place of letters)?

■ Does your organization update your virus protection software regularly?

■ Does your system administrator look for security repairs and patches you can download from your operating system's Web site regularly?

■ Have you established an internal policy that prevents users from downloading files or using hyperlinks from unknown sources?

■ Does your organization use a firewall (especially if you have a high-speed or "always on" connection to the Internet)?

■ Does your organization use a secure browser (software that encrypts or scrambles information you send over the Internet) to guard the safety of your online transactions?

■ Have you established limited password access for information stored on your systems?

■ Have you established a zero tolerance rule for password sharing?

■ How do you dispose of computer equipment? Do you break old motherboards and destroy hard drives?

Physical Security

The FTC's Information Safeguarding Rule requires "reasonable" measures to secure and dispose of reports; this includes taking the time to audit and identify physical security risks, such as access to records or information by unauthorized individuals. Sensitive consumer information should be locked up and only viewable by authorized personnel.

What is your organization's document retention policy? Where are they stored and who has access? Your organization needs established access safeguards (lock and key or passcard access). Documents containing sensitive information must be locked up in a secured area when unattended. Common mistakes many companies make is leaving vulnera-

ble information viewable by unauthorized persons in and around the office, such as documents left on desks, computer screens, trash with identifying information disposed of and unshredded, open conversations discussing social security numbers, and other bits of personal consumer information.

Does your organization destroy consumer or company information in a manner that renders the information unreadable? (For instance, disks, documents with company or consumer information, discarded photo copies, etc.) It's not enough to throw out documents or deleted disks, these items need to be destroyed. You should establish a disposal of records protocol so information doesn't accidentally land in the wrong hands.

5 Steps to Create a Policy

The first step in protecting your property management company is done by ensuring that the business owners and managers understand what identity theft is and how it can inevitably impact your business. This includes knowledge and understanding of the duties and obligations your business has in safeguarding information and preventing identity theft.

An effective means toward achieving step two of this goal is to appoint either an individual with in-depth knowledge of property management processes, or alternatively a committee of managers and peers. Either should be tasked with identifying and documenting potential identity theft exposure and security breach risks. Keep in mind the document being created will be static and the process ongoing due to the evolutionary nature of the problem.

The third step takes place only after potential risks have been identified. This step is the policy-making step of the process, in which the committee establishes prudent practices for the organization. It's important to create policies and procedures that are effective yet easily implemented. In other words, as the policy is being written, consider the reasonableness of the policy and the ability for employees to comply with such a policy. Ask: Does the policy solve the problem? Does the policy stifle productivity more than it protects the organization? Is the policy reasonable to everyone? Is there a better way to achieve this goal? Is there a way to ensure compliance with this policy?

The fourth step is to ensure implementation and compliance. To achieve the first part of this goal, it's important that employees are thoroughly trained on the information safeguarding policy created and that they are updated periodically of any changes or additions to that policy. The second part can be achieved through ongoing compliance auditing to ensure the policy is being followed by all employees.

The fifth and final step of the process is to continuously reassess the efficacy of the safeguards that have been put into place. This is a critical final step in the process that will secure company information, and that will ultimately protect the business and sensitive consumer information.

Recognizing an Identity Thief

As you work to close the cracks and crevices that identity thieves are constantly working to infiltrate, it's important to keep in mind that identity thieves aren't always easy to detect, recognize, or identify until after the fact. So, keep your staff on guard and aware.

When dealing with potential residents, your team should be aware of refusal to provide information or gaps or inconsistencies in information. They need to be aware of plots, ploys, and dupes used by identity thieves in an effort to distract you from wanted records or documents containing consumer information.

You should never be overly confident that your policies and practices are impenetrable and you always need to be on guard. Remember, most identity thieves are not working alone; 60 percent or more are believed to belong to an identity theft ring. Approximately 15 percent of identity thefts are related to violent crimes, drugs, and terrorism.

As your organization works to establish an information safeguarding and security policy, consider the strategies, resources, and products available to, and currently being used by the multifamily housing industry to combat and prevent identity theft. Understand the establishment of an information safeguarding and security policy is never final. It is a dynamic process that should never end so long as identity theft impacts our industry. **pro**

Julia Langston is director of legal and regulatory affairs at FirstAdvantage Safe-Rent. She may be reached at jlangston@fadvsafere.com