## TACKLING IDENTITY FRAUD AND ITS EFFECTS IN THE MULTIFAMILY RENTAL INDUSTRY

One of the most challenging situations in today's multifamily rental industry is the statistical fact that 75% of management companies with less than 30,000 units and an incredible 100% of management companies with more than that number of units are victims of fraud. We have reviewed material from recent articles and comprehensive statistics that have been published dealing with Synthetic Identity Fraud in the multifamily housing industry and we have condensed/merged some of the most recent information available on this topic from several primary resources that include the NAA, Experian, Idanalytics, Corelogic, CheckpointID, TransUnion and Forbes Magazine. ***As the NAA has pointed out, there is no question that apartment operators and managers, unfortunately, are very familiar with the detrimental effects that identity fraud can have on their business and know that no property is safe from the four basics types of identity fraud:***

1. **First-Person Fraud:** The applicant is acting for another person when renting an apartment. The applicant uses his or her real identity information on the application but isn't the person who'll be residing in the apartment

2. **Third-Party Fraud:** The applicant assumes a stolen identity and uses the victim's personally identifiable information (PII), including name, Social Security number (SSN), and date of birth (DOB).

3. **Identity-Manipulation Fraud:** The applicant alters some of his or her own identifying information in a way that looks as if it could be a typo or spelling error. Common examples include an SSN that's off by one number or includes transposed numbers, a slightly different name, or an altered birthdate.

4. **Synthetic Fraud:** The applicant creates a fake identity by fabricating all identifying information (SSN, name, date of birth), cob- bling together an identity from multiple stolen sources, or doing a mix of both. Real SSNs, typically from children, the elderly or deceased people, are often used in combination with made-up names and birth dates, but even the SSN can be fabricated.

Of the four types of identity fraud that commonly occur in the multifamily industry, the fastest-growing and the largest percentage of identity fraud that occurs in the apartment rental industry is synthetic fraud. Industry experts estimate that synthetic fraud accounts for 85% of all identity fraud in the country. Despite the revenue losses and the increased liability for resident safety that this situation creates for apartment communities, synthetic fraud is difficult to identify during the leasing process.

The most common format for synthetic fraud entails using a real SSN, typically stolen from a child, an elderly person or a deceased person, in combination with a fake name and

birthdate. It is not uncommon for a SSN to be fabricated altogether. Such fabricated SS numbers can easily be purchased from online disreputable sources that sell the false SSN as a credit profile number, or CPN, for use on financial applications such as leases.

One of the reasons synthetic fraud works so well in multifamily housing is that every inquiry sent to a credit bureau results in the creation of a credit file. Thus, if a SSN is being used for the first time, the process creates a new credit file with no negative records. That means that an inquiry using a fake SSN, a child's SSN, or the SSN of someone who has died and has been removed from the credit bureau records counts as a new file. The first time the inquiry is made, the response will show that no credit file exists for that identity. In addition to adopting a false SSN, synthetic-fraud perpetrators will use fake paycheck stubs to make it look as though they earn enough money to qualify and because of the nature of how the identity is created a synthetic-identity is often difficult to spot because no "victim" exists who reports the activity right away.

With fake identities so easy to produce, it is challenging for multifamily operators and managers to protect their properties? Using Resident-screening software technology can alert management when an applicant might be using a fake SSN, based on a discrepancy between the date the SSN was issued and the date of birth or age the applicant provided. Similarly, an alert might indicate an address discrepancy between previous addresses listed on the rental application and those listed on the credit report.

Costs to your bottom line caused by applicants who become residents through synthetic fraud include lost rent, attorney fees, court costs, law-enforcement service fees, locksmith and cleaning fees, property repair and replacement costs, storage fees, remarketing expenses, and labor and operational costs. Added to the preceding tangible costs are the intangible costs of reputational damage. But, the expense of synthetic fraud goes beyond monetary value. Fraudulent applicants who are concealing criminal histories, such as being registered as a sex offender, might commit new crimes that could endanger your current residents and employees. Accepting applicants into your community who are committing synthetic fraud increases your potential liability and jeopardizes the safety of all who live and work there.

Steps you can take to help prevent synthetic fraud at your property are:

1. **Use Additional Verification Methods** Use multiple layers of authentication to validate the identity of a prospective resident. Additional documents may include state- or government-issued photo identification, Social Security cards, Green Cards (also known as Permanent Resident Cards), passports, W-2 forms, a copy of the applicant's most recent utility bill, a paycheck stub and so on.

2. **Keep Your Resident Application Criteria Updated** Review and analyze your resident-screening criteria for operational processes and procedures. These criteria should be clearly stated on your company's application for residency in accordance with company policy and state and federal laws.

3. **Go Beyond SSN's** In a world where consumers are doing business predominately online, don't rely solely on Social Security numbers to authenticate a prospect's identity. You can avoid confrontations with prospects and stay within FHA guidelines and reduce your company's liability by using multiple layers of authentication to validate the identity of a prospective resident. Additional documents may include state- or government-issued photo identification, Green Cards (also known as Permanent Resident Cards), passports, W-2 forms, a copy of the applicant's most recent utility bill, a paycheck stub and so on.

4. **Educate Your Team** A key to preventing fraud is awareness. Educating your teams about the potential warning signs during the application process can help diagnose fraudulent activity. It's also important for employees to understand the best way to respond to an applicant whom they suspect has committed fraud.

5. **Use Technology to Reduce Your Risk and Ensure Compliance and Security** Today's resident-screening software technology not only takes the bias and guesswork out of deciding which applicants should become residents but reduces company liability, as well. Resident-screening technology can use Machine Learning models to catch synthetic fraud or provide alerts when there is a potential fraud. A third-party screening company can give you best practices for handling synthetic-ID fraud and suggest potential changes to your screening criteria that would provide additional fraud alerts.

It is important for our clients, to recognize and understand the growing trend of synthetic fraud, especially in the multifamily industry; specifically, this type of falsification as well as how to identify it, respond to it and prevent it. Updating relevant policies within your company will help arm your properties with the proper protection. If you have any concerns or questions regarding how you are prepared to identify and deal with identity fraud at your property, THS attorneys would be happy to discuss this with you.