entrata®

Preventing Fraud in Multifamily

How to reduce the risk of fraudulent applications and payments

Introduction

Having the ability to process rent payments and applications online is a blessing and a curse for many multifamily businesses. On the one hand, it speeds up the process of getting funds from residents into your accounts. On the other hand, it opens the door for applicants to commit fraud by shielding their true identity or obfuscating their financial position to get approved.

Despite everyone's best efforts, fraud is still rampant across the industry. Research from NMHC has found that 93.3% of properties have experienced fraud in the last twelve months.[1] Fraudulent applications have a significant impact on a property's bottom line, and result in delinquent rent payments and unfortunately evictions. It also results in frustration for your site team and residents around units involved in the eviction process—all of which are costly for your properties.

It is estimated that evictions that come as a result of late payments cost the property $7,500 on average for each eviction. When you take into account that there are more than four million evictions every year in the US alone, those costs really add up.[2]

1. NMHC Pulse Survey: Analyzing the Operational Impact of Rental Application Fraud and Bad Debt
2. Application Fraud Is on the Rise for Multifamily Properties

In addition to the actual monetary costs associated with each eviction, there is the potential loss of future revenue if resident frustration leads them to leave negative reviews of the property. Your online reputation has a significant impact on whether or not potential residents submit applications, and a bad reputation will definitely steer applicants to another property.

One of the root causes of delinquent payments, and, as a result, evictions, is application fraud. This is why it's important to have guardrails in place to nip that fraud in the bud from the very beginning. In this ebook we'll talk about the types of fraud that are on the rise, how you can recognize them, and steps you can take to limit the number of fraudulent applications and payments you receive.

Types of application fraud to look for

First Party Fraud. In this scenario, the applicant has someone they know that can pass the credit checks and income verification on their behalf, but the original applicant has no intention of ever living in the unit. While this type of fraud does happen, it's less frequent than the other types of fraud we'll describe because the original applicant is putting their credit on the line.

However, it's one of the hardest to stop and detect because it involves a real person going through the application process. And once the actual resident is moved in, the process of removing them for application fraud can be not only costly, but also time consuming.

Third Party Fraud/Identity Theft. Next, is actually stealing someone's identity. Identity theft has been on the rise in recent years. The FTC reports that losses associated with fraud topped $10 Billion last year, which is a 14% increase from the previous year.[3] One third of all Americans have been the victim of identity theft at some point in their lifetime. It's so common that someone is the victim of identity theft every four seconds.[4] Consumers lost $650, on average, for each incident of identity theft.[5]

Identity manipulation. Sometimes applicants will slightly alter their identity to conceal who they are. Things like changing their date of birth or transposing numbers in their social security number.

3. As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public
4. Identity Theft Crime and Punishment: 2023 ID Theft Crime Statistics and Sentencing
5. Consumer Sentinel Network | Data Book 2022

Synthetic Fraud. In this scenario, the applicant creates a new person out of whole cloth, purchasing the new identity on the dark web, including a name, date of birth, and social security number. These could either be completely fabricated, or be the name, DOB, and SSN of a child or deceased person. These can be difficult to catch at first, especially if you're only using credit reporting because when a new SSN is submitted to the credit bureau, it isn't flagged, it just creates a new report that doesn't have any credit associated with it.[6]

There are significant costs associated with synthetic fraud, including, 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.[7] However, the bigger threat can come to your residents. If you let residents into your community who have committed violent crimes, you put other residents at risk if they were to commit new crimes in the future.

Protecting your multifamily business from fraud

With how rampant fraud is in the multifamily industry, it's not a matter of *if* you'll experience it, but *when*. If you aren't taking the necessary measures to prevent fraud from happening, and mitigating the risk of potential fraud, you're opening a pandora's box that could lead to lost revenue that you may never recover.

While technology introduces the potential for more fraud to occur in the multifamily industry, there are strategies and tools that, when implemented, can significantly reduce the risk of potential fraud at your properties. Throughout the rest of this ebook, we will outline best practices for mitigating the risk of potential fraud from applicants.

6. Tackling Identity Fraud and Its Effects In the Multifamily Rental Industry
7. Tackling Identity Fraud and Its Effects In the Multifamily Rental Industry

Thorough initial screening needed

While running a credit check is a no-brainer, that is just one piece of the puzzle. If you can't tell from what you've read so far, there are a number of ways to trick or evade the credit reporting process for identity thieves.

Part of a thorough background check involves not just financial solvency and credit worthiness, if you want to check their online presence. To paraphrase an old idiom, if you find anything about it on the internet, did it even happen? You might be wondering how this relates, but if the applicant doesn't leave a trail at all on the internet, that should raise some suspicion.

Now, not everyone is going to leave a big footprint on the internet. This shouldn't be a reason to preclude applicants from renting from you, but it should trigger another set of protocols that vet them further.

Another concern that is becoming increasingly more prevalent is the rise of synthetic identity, which is where a fraudster creates a new identity by combining both real and fake data, like using one person's social security number and date of birth, while fabricating an address. Synthetic identities also occur through manipulation of documents, like changing the name on a pay stub, adding a different name, or changing the birth date on a driver's license.[8]

If you still have concerns about the applicant, a manual screening might be warranted. It's helpful if you have technology in place to automate much of this work. Once an application is submitted, the wheels start turning on the back end, and almost immediately you should be able to approve or deny an initial application. If any additional verification is needed, a one-time code being sent to the phone number or email address submitted, for example, can also be triggered automatically, depending on the workflows you have set up for approval.

Have income verification workflows in place

Once the initial screening has been completed and passed, the next step in fraud prevention is to first ensure that the banking information provided is correct, and second, that there are funds available to process the payment.

8. Synthetic identity fraud: How to detect and prevent it

The first payment you'll likely receive from the resident is likely a deposit, either to hold the unit, or a security deposit of some type. With larger payments like these, it might make sense to use certified funds, either through a money order or MoneyGram. Some property management solutions even have tools in place to collect certified funds. This would provide the least amount of friction to the applicant because they could create the certified funds request directly from the application portal and send it directly to you.

For regular monthly payments, you'll also want to have guardrails in place to protect not only you, but your residents as well. Since 2021, NACHA, the governing body of the ACH network, has required that everyone accepting online payments have a "commercially reasonable fraudulent detection system" in place.

The best solutions can not only detect if the account is real (account number, username, and password exist), but also if there are enough funds available to cover the payment. You might be wondering why it should matter to you. Shouldn't the onus be on the resident to provide proper information? And for the most part that is true, but just think of all the time and effort spent chasing down payments after the fact. It's better to know beforehand and have a plan in place to get another payment method lined up or create a payment plan to help the resident get caught up.

The money and time can really add up. Before Entrata built Account Verification to help its customers solve this problem, its customers saw $238M in preventable ACH returns, with more than 280,000 returns in the twelve months prior. Those returns cost 970 workdays, and the average conversation with residents to recoup payment is five minutes, but many are much longer than that. That's time lost by on-site staff that could be used to conduct tours or help existing residents have a better overall experience at your property.

$238M
Preventable ACH returns

280,000
Returns in the twelve months prior

970
Workdays

How Entrata can help

Entrata has a wide range of tools to help your business mitigate risk and avoid fraud, both in the application and payment processes. Operators need this type of multilayer security approach to prevent fraudsters from getting into their communities. Entrata's solutions deliver multilayer security that ensures the right people get approved during the application process. They include:

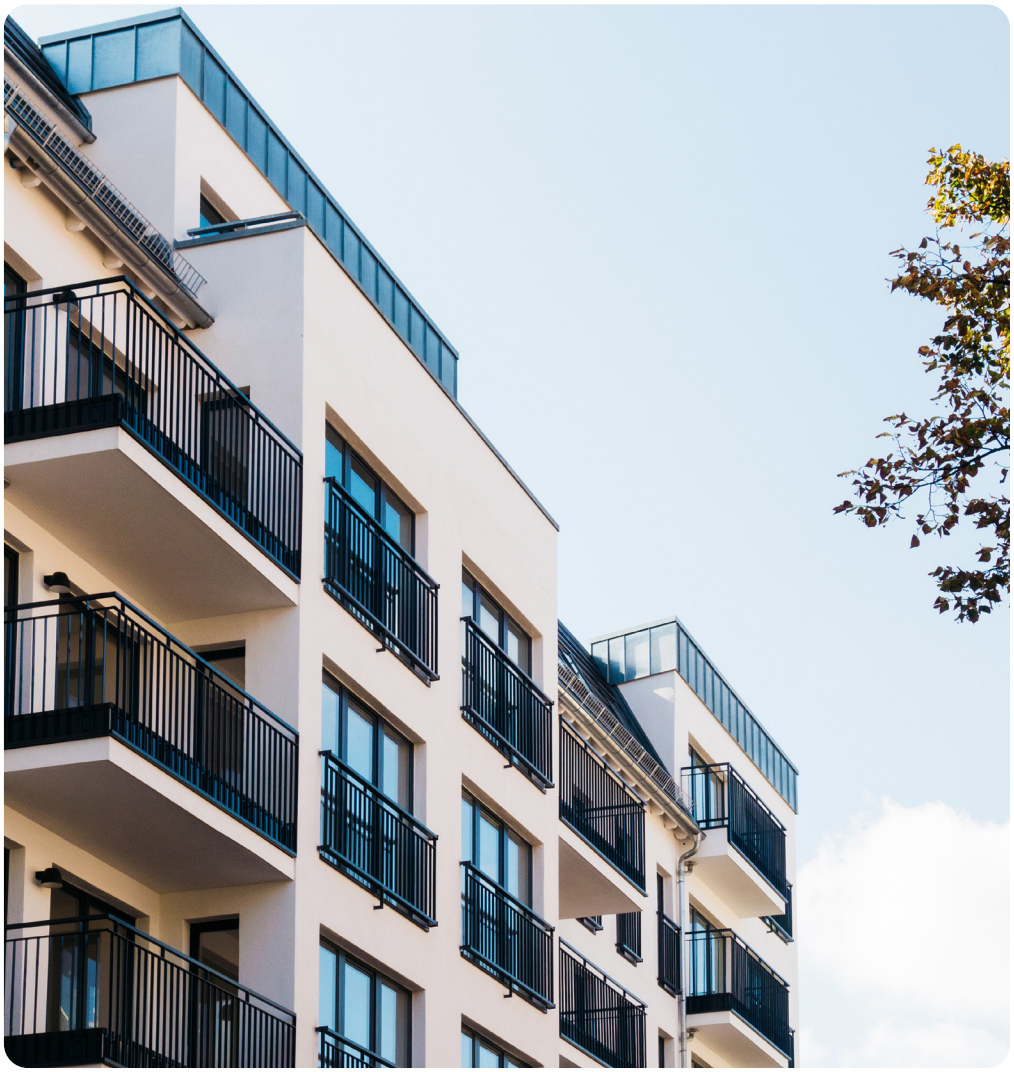
ResidentVerify

With ResidentVerify, you no longer have to outsource your applicant verification process. You'll be able to choose the vetting criteria that best fits your properties, and once you set them in motion, everything happens automatically. By having your screening within your application process, you can then offer or require residents to sign up for certain programs based off of their screening results easily, within the application workflow. For example, you could offer deposit alternatives or other insurance products.

Stop worrying about compliance violations that used to be a part of the screening process. ResidentVerify follows your criteria strictly, while removing the time-consuming manual verification process. And because ResidentVerify takes advantage of thousands of data points, you can have the peace of mind that comes from knowing you're reducing risk, while saving your team loads of time and money.

Properties using Income Verification are able to seamlessly track an applicant's ability to pay from right within the actual application. The end result is a faster application process for you and the applicant, helping them move to the next step of the process, or move on to another property if they can't meet your requirements.

An added benefit to the ResidentVerify screening process is it allows you to collect application and other fees up front, right from the ProspectPortal, so you won't have to chase them down later.



ResidentPay

There are two main features of ResidentPay, Account Verification, and Funds Verification that work hand in hand to ensure that payment information residents provide is accurate/exists, and that there are funds available, so the payment isn't returned. With ResidentPay Account Verification, you get real-time account verification, which will help reduce the number of fraudulent payments and other returns. Account Verification also helps meet the NACHA requirement described previously.

With Funds Verification, an automatic balance check will be performed on the applicant's or resident's bank account at the time of payment. If insufficient funds are detected, the payment will not process, drastically reducing the rate of payment returns due to insufficient funds. Having this done automatically will eliminate the need for your staff to track down returned payments. They can start working with the resident immediately to get an alternative payment method in place to help them avoid any late fees they may incur.

Snappt partnership

Entrata recently partnered with Snappt, enabling owners and operators to run income documentation directly in Entrata. This is an excellent option for applicants that don't want to provide their banking information, while still giving you the ability to automatically verify income.

Learn more

To learn more about how Entrata can help reduce fraud at your properties as part of both the application and payment process, request a demo today.

entrata®

Entrata powers over 20,000 communities worldwide helping clients achieve and exceed their goals.