REALPAGE FRAUD SURVEY:

Uncovering the Impact of Rental Application Fraud in Multifamily

REALPAGE®

Contents

Click an entry below to jump to that section.

Introduction

Welcome to the 2024 National Multifamily Fraud Research Study. The insights and research team at RealPage® is pleased to provide you with this study and all its discoveries. Our mission in conducting this rental fraud study, the largest of its kind in the multifamily real estate industry, was to add data-driven clarity to the leasing fraud conversation by shedding light on the causes of leasing fraud in multifamily communities nationwide, identifying advanced technologies and methodologies being used by savvy fraudsters, and offering strategies for mitigating risk.

Leasing fraud hits multifamily property owners hard.

Multifamily leasing fraud has risen by

more than

40%

since 2023

and has cost property owners an average of

$4.2 million

Source: Globe Street. January 29, 2024

With those staggering numbers in mind, we set out to determine ***why*** leasing fraud has risen sharply and offer early detection solutions so property owners and investors can mitigate risk.

METHODOLOGY

A total of

402 qualified participants

completed the survey conducted online **Jan. 2 - 9, 2024.**

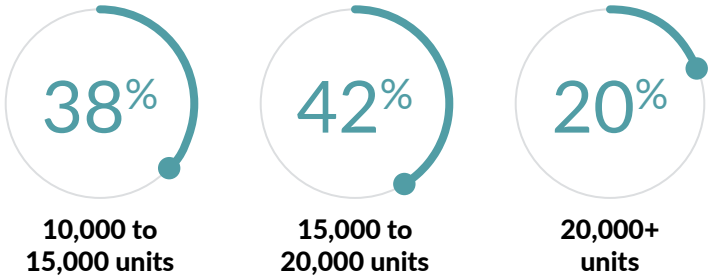
Participants comprised property managers in centralized and property-centric or regional roles, responsible for evaluating and/or approving rental applications at multifamily companies with at least 10,000 units.

PARTICIPANT ROLES

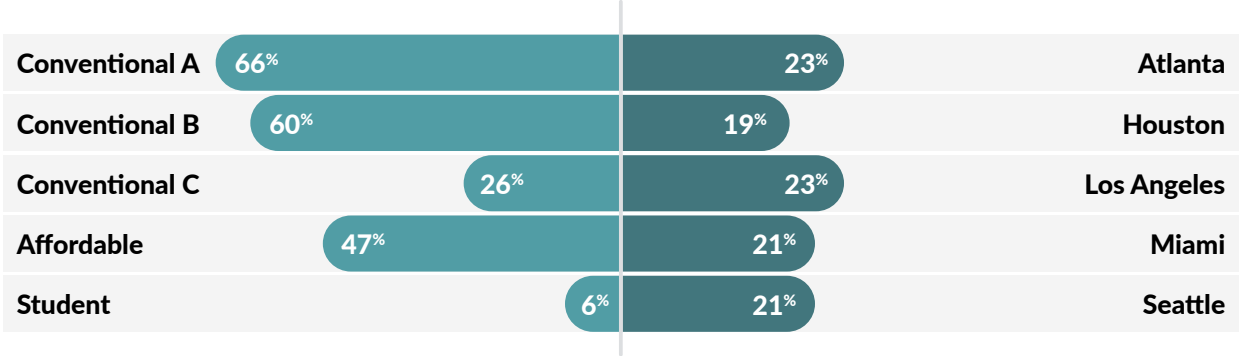
49%
Property managers with **centralized roles**

50%
Property managers with **property-centric or regional roles**

PORTFOLIO SIZE



ASSET CLASSIFICATIONS



GEOGRAPHIC LOCATIONS

Against the backdrop of alarming prevalence, sophistication and growth of fraudulent rental application activity, this study participant group confirmed our long-held belief about the cause of rising leasing fraud and that it occurs in just about every multifamily community.

This white paper reveals insightful discoveries about:

Leasing fraud

Gaps in preventative measures

Length of time it takes property managers to uncover it and begin eviction proceedings

These are the exact insights that property managers, asset owners and trend watchers need to know but can't find anywhere else.

Many of the findings detailed in this report may seem to echo what you've long believed or witnessed but never had data to support. Other findings may just change the way you think about applicant screening.

Sincerely,
RealPage

Section 1: Statistics on Rising Fraudulent Rental Activities

Throughout the U.S., incidences of rental application, financial and identity fraud are on the rise, fueled by readily accessible technologies and internet platforms. Rental fraud risk spans all parts of the rental lifecycle: pre-move-in remarketing scams; check, debit card, credit card and ACH fraud; and unqualified approvals based on stolen or synthetic identity, fake renter history, fabricated employment documentation and falsified income "verification."

Once renters move in, the risk to property owners and their legitimate residents goes up significantly via lost revenue, eviction fees, reputational harm, increased resident churn, and even the threat of the rental unit being used as a haven for illegal activities like drug and sex trafficking. Eviction comes with costs as well as property theft and damage. All this sets in motion a ripple effect of reputational harm and brand damage to the multifamily community and its owners, investors, property managers — and even residents.

But fraud's risks aren't always tangible. There are also intangible risks that are insidious and far more dangerous to multifamily operators and their residents.

Our findings uncover the impact of fraud on multifamily communities, with five major discoveries revealed via our fraud research study:

Discovery 1:

75% **of multifamily property management decision makers report increased fraudulent renter behavior.**

Discovery 2:

93% **of multifamily companies have observed that rental fraud is becoming more organized and sophisticated.**

Discovery 3:

97% **of multifamily companies agree that reducing fraud is their top priority.**

Discovery 4:

80% **of multifamily decision makers in centralized roles are more likely to report increased fraud frequency.**

Discovery 5:

99.5% **of multifamily properties have experienced six fraud impacts:**

- Property damage (55%)
- Reputational harm (51%)
- Criminal activity in units (49%)
- Eviction/early lease termination cost (47%)
- Loss of good residents (42%)
- Nonpayment of rent (15%)

Section 2: Understanding the Multifaceted Causes of Rental Fraud

75% of property managers who participated in our fraud study reported an increase in fraud in their multifamily communities, citing causes that include the ease of obtaining fake or stolen documents, the normalization of dishonesty that makes fraud culturally acceptable and the lack of consequences for supplying false information on rental applications.

In other words, the cause of rental fraud is now a multifaceted problem that goes unpunished. And that makes it highly attractive to would-be fraudsters and organized crime rings.

The 8 most prevalent causes of rental fraud

1. Organized rings of rental fraudsters that exploit social media and other communications channels

31% of study participants say organized fraud rings are the biggest driver of rental fraud, and 63% believe that organized rings of fraudulent actors are actively targeting multifamily properties. The problem, then, is not attributable to lone-wolf bad actors and isolated incidents of dishonesty.

Facilitated by social media and other online communications channels, today's rental fraud is often carried out via preplanned, coordinated efforts by organized groups of fraudsters who specifically aim to exploit vulnerabilities in rental application processes. Their efforts have resulted in not just fraud against multifamily owners but also the formation of new black markets.

2. Ease of obtaining fake documents

41% of the property management decision-makers who participated in this study say fraudsters are enabled by the ease of obtaining fake documents (digital and physical). Thanks to high-speed internet, fraudsters can now search the internet with lightning-fast speed to find realistic-looking fake documents that don't immediately sound an alarm bell in leasing agents' minds.

This heightened accessibility also enables fraudsters to submit fake documentation without the delay that existed before the advent of search engines and high-speed internet connectivity. What used to take days or weeks to obtain can now be in a fraudster's hands in mere seconds. Moreover, sophisticated software and artificial intelligence (AI) enable fraudsters to present realistic-looking fake documents that don't immediately raise a red flag. And that greatly complicates the applicant screening process.

3. Accessibility of information on creating fake information and documentation

23% of study participants blame social media for the rise in rental fraud. Social media and search engines comprise the world's largest library of information on everything, including how to create realistic fake information and documentation for rental applications and steal existing information. And when AI tools, which didn't become accessible to the masses until November 2022, are used to carry out the instructions obtained through social media, savvy fraudsters can — in just ***mere seconds*** — create a portfolio of fraudulent digital and physical documentation for rental applications.

4. Lack of consequences

41% of study participants say the lack of legal consequences for applicants caught falsifying rental application information fuels the rise in fraud incidents.

5. Lack of formal metrics for tracking rental fraud

Less than one in four study participants (22%) say their multifamily properties have formal metrics for tracking rental fraud and its impact on their business. A startling 56% say renter fraud in their apartment communities is "informally tracked" via spreadsheets, 19% say they don't specifically track renter fraud but do track other financial metrics such as rent nonpayment, and 3% say they don't do any kind of fraud tracking, relying instead on anecdotes and personal experiences.

6. Inconsistent use of validation approaches across rental portfolios

When asked about validation methods used and the frequency of their use, property managers revealed that they use:

Basic background screening services (i.e., criminal background check, credit score)

- 32% portfolio-wide
- 40% at high-risk properties only (where there is high fraud and high bad debt)
- 19% in high-risk regions only
- 8% only when mandated by the property owner

Rental history screening services (evictions, skips)

- 29% portfolio-wide
- 30% at high-risk properties only (where there is high fraud and high bad debt)
- 27% in high-risk regions only
- 15% only when mandated by the owner

Financial document verification services (pay stub, W2, bank statement, etc.)

- 30% portfolio-wide
- 27% at high-risk properties only (where there is high fraud and high bad debt)
- 26% in high-risk regions only
- 16% only as mandated by the owner

Identity document verification services (passport, driver's license, etc.)

- 21% portfolio-wide
- 33% at high-risk properties only, where there is high fraud and high bad debt
- 22% in high-risk regions only
- 24% only when mandated by the property owner

Advanced identity verification (device assessment, facial recognition, etc.)

- 17% portfolio-wide
- 31% at high-risk properties only (where there is high fraud and high bad debt).
- 26% in high-risk regions only
- 27% only when mandated by the property owner

Rental applicants (87%) and application reviewers (86%) both find fraud reduction processes to be "tedious and frustrating." Centralized decision-makers are more likely to experience applicant complaints about frustrating screening processes, with 34% of study participants reporting that prospective residents are frustrated with their multifamily communities' fraud reduction processes versus 16% of decision-makers in property-centric or regional roles.

Further, 27% of prospective residents frequently complain about communities' fraud reduction processes and another 60% occasionally complain. Only 13% never complain.

And applicants and property managers aren't the only complainants. Our study revealed that leasing agents and other employees also find their communities' existing rental fraud reduction processes to be tedious and frustrating:

- 48% frequently complain
- 38% occasionally complain
- 14% never complain

7. Manual methods used to aggregate data from different solutions

Almost two-thirds (65%) of our study participants say their communities use manual methods to aggregate data from different solutions. Further, when asked how their company puts together and analyzes the information gathered from these different solutions to screen and validate rental applications, their answers were startling:

- Only 35% use a tool that automatically pulls data from all collected information into a single view
- 29% manually input data into a spreadsheet or other software
- 36% manually evaluate information derived from each separate service/solution

In other words, 65% don't see the full applicant picture in one comprehensive snapshot view. Yet, 88% of property management professionals characterize their rental fraud solutions as "good" or "excellent."

8. Need for improved training efforts

Most study participants said their companies train employees to identify rental fraud. But their training methods differ:

- 39% say their companies have required fraud training
- 58% say their companies provide fraud training materials to employees for self-guided learning, but expert-led training is not required
- 3% say there is no fraud training in their multifamily communities

Section 3: Examination of Fraud Occurrences

Almost three-quarters (73%) of study participants revealed that an average of 59% of renter fraud is detected after move-in, not before, with Atlanta at 60%, Houston at 59%, Los Angeles at 60%, Miami at 55% and Seattle at 62%.

That's unsurprising, considering that income verification is one of the top application screening components, and it is, according to 45% of study participants, the most challenging fraud type to detect.

The most difficult-to-detect fraud types

The five most difficult-to-detect fraud types are income misrepresentation, fake or manipulated renter identities, identity theft, staff pushing through unqualified candidates, and fraudulent co-signers or guarantors:

1. 45% income misrepresentation (i.e., fake pay stubs)
2. 40% fake or manipulated identities (i.e., Credit Privacy Numbers (CPNs) and synthetic or counterfeit identification)
3. 39% identity theft (i.e., stolen identification and mail)
4. 36% site staff pushing through unqualified candidates
5. 34% fraudulent cosigners or guarantors

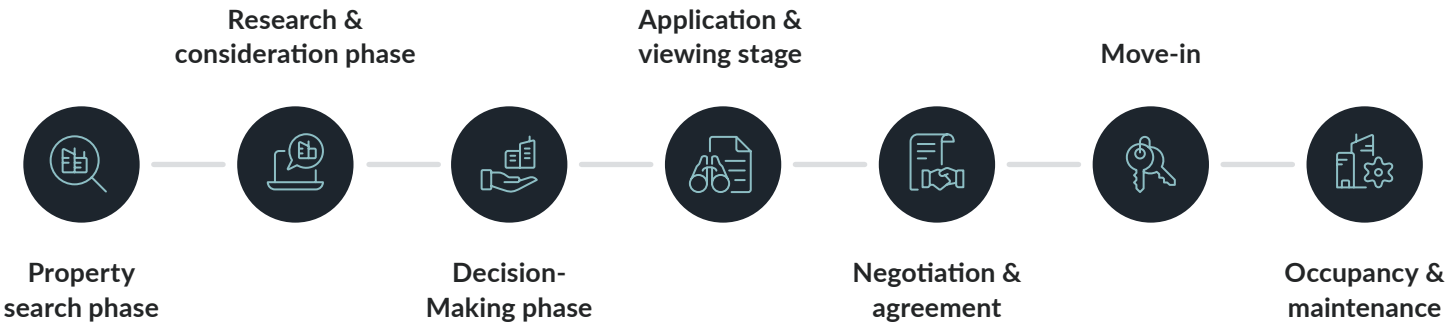
These revelations align with technological advancements available online to all who seek to use them for fraud. These tools enable fraudsters to produce highly realistic-looking fake information — everything from photos, personally identifying information (i.e., driver's license and other state-issued IDs), bank statements, employment records, W2s and pay stubs.

Our findings also reveal that property managers in centralized roles are more likely to identify difficulties with site staff pushing unqualified rental candidates, and an equal percentage (45%) of centralized and property-centric property managers consider income misrepresentation to be the most difficult form of renter fraud to identify during the screening process.

Identifying fake or manipulated identities (i.e., CPNs, synthetic or counterfeit IDs) is more difficult for property managers in property-centric or regional roles (44%) than it is for property managers in centralized roles (37%). Yet, identifying instances of identity theft (i.e., stolen IDs, stolen mail) is harder for centralized property managers (40%) than it is for those in property-centric/regional roles (37%).

Site staff pushing through unqualified candidates is a challenge faced almost equally by property managers in both types of roles — 37% centralized PMs and 33% property-centric/regional PMs. This may be due to their perception of applicant screening processes as "tedious and frustrating."

Overview of fraud throughout renter journey



Property search phase

Not all that long ago, when prospective residents were too busy to tour a property or lived out of town, they would mail a disposable camera to a multifamily property's leasing office, ask the agents to take photos of the unit and the community and then mail the camera back to them for processing. But technology has changed that, enabling video tours, virtual tours, online applications and leasing.

While these capabilities streamline the touring, application and leasing processes for legitimate, qualified renters, they also make it easy for fraudsters to find the perfect target for their rental fraud schemes because they provide all the information the fraudster needs to create their fake rental listing.

Research & consideration phase: Phishing and fake rental listings

Social media phishing scams involve cybercriminals posing as legitimate entities to deceive users into revealing sensitive information. These scams often target multifamily property management companies, real estate professionals, and potential renters. Some phishing scams involve financial transactions or requests for sensitive financial information. That information is passed on to rental leasing agents and property managers during the application screening process.

Fraudsters also use fake online rental listings for apartments that either don't exist or for which they aren't the leasing agent, using attractive photos, video tours and descriptions to lure potential tenants who then unwittingly apply and qualifying information (i.e., employment status and name of employer, pay stubs or W2s, etc.). The fraudster then uses that scam-begotten information when applying to lease an apartment in a multifamily community.

In another version of the fake rental listing scam, the fraudster advertises an apartment that actually exists, but the fraudster is not the leasing agent. Using stolen photos and descriptions from legitimate apartment listings, the fraudster places an "apartment for rent" ad. When an unsuspecting renter responds to the ad, the fraudster claims that they cannot show the unit without upfront payment from the prospective renter. If the unwitting victim is interested in renting the apartment, they're instructed to send a deposit to the fraudster. Shortly thereafter, the property is no longer available.

In the meantime, the unsuspecting renter shows up at the actual leasing office to get the keys to the apartment they believe they have rented only to find out that they have been scammed. While this doesn't cause financial harm to the actual property owner, over time, it does cause reputational harm.

Decision-making phase: Payment fraud

Regardless of your rent collection method, each one has its associated risks. Payment submitted by an applicant doesn't equal the funds received. Property managers and leasing agents should treat those early renter and applicant payments as questionable until the funds have cleared the bank after the applicant or renter initiates the transaction.

1. Money orders.
There are countless scenarios in which money orders are being used for fraud. In many cases, a legitimate money order is purchased for a small amount but then altered to show a different amount.*

Source: United Credit Union

2. Checks.
The overpayment scam is one way fraudsters use checks to pay rent and the security deposit at the time of lease signing. New applicants and newly moved-in residents will pay exactly the amount owed, then "change their mind" and request a refund a day or two later. When the property manager issues a refund to applicants and new renters in that short time period, they set themselves up to be victims of fraud.

3. P2P payments.
Also known as peer-to-peer (P2P) payments, P2P payments are transactions that take place on digital wallets such as Venmo and PayPal. The main concern with P2P payments in terms of fraud is the property manager's inability to refuse payments when this method is used. This is particularly concerning for residents making partial payments to complicate the eviction process.

4. Debit and credit cards.
Fraudsters are skilled in using stolen credit and debit cards (and associated bank account information tied to debit cards). With these payment methods in hand, they make a rent payment today and then request a refund tomorrow. At some point, the person to whom the debit or credit card belongs will report to the financial institution the unauthorized charge or debit that shows up on their monthly statement. The financial institution will investigate and discover that the community is not the fraudster. But they will still reverse the charge (referred to as a chargeback) — a financial loss for the property owner.

Application & viewing stage: Application fraud, unqualified approvals

Study participants identified five types of application fraud that were experienced in their multifamily communities in the 12 months prior to the study:

1. Fake or manipulated identities (58%)
2. Misrepresented income (57%)
3. Identity theft (53%)
4. Site staff pushing through unqualified candidate approvals (51%)
5. Fraudulent cosigners or guarantors (31%)

As presented earlier in this report, fraudsters have sophisticated technologies and methods that make it easy to commit application fraud. They often operate as part of organized fraud rings that know how to perpetrate fraud without their fraud being detected early in the application and approval process. They know how daunting and expensive the eviction process is, so after they perpetrate application and leasing fraud, they move on to what is commonly known as "squatting" (nonpayment of rent).

Negotiation & agreement: Lease fraud, cosigner fraud

The fraudster's goal is to sign a lease and obtain the keys to the apartment. To make that happen, they use all fraud-committing measures, including misrepresenting income and introducing fraudulent cosigners or guarantors into the leasing process. They sign the lease and move in with no intention of paying rent. Their goal is to occupy the apartment rent free for as long as possible. They know that even after the property manager uncovers their fraud and pursues legal action, it will take considerable time before a court of law will order their eviction.

Fraudsters also sign leases for the purpose of illegally subletting apartments to third parties. The fraudster signs the lease without intending to live in the apartment or pay rent. Instead, they use online listing sites to advertise and sublet the apartment. Fraudsters find it easy to sublet their apartment, require six months' rent upfront from the new, unauthorized tenant, and then take off. When the property manager stops receiving rent payments, that's when they discover that someone other than the original tenant is now living in the apartment. At that point, the property owner and the person who sublet the apartment are out of substantial amounts of money.

Move-in: Key fraud, fraudulent deposits

A normal part of apartment leasing is the security deposit, with many property owners and managers requiring the first and last month's rent in addition to a month's rent as a security deposit. Fraudsters have an arsenal of payment scam methods at their disposal, and those methods work well when leasing an apartment in a community that accepts cash, checks, credit cards and payment processors like Venmo and PayPal.

What makes deposit payment fraud noteworthy isn't just that you are being scammed — it's that it happens when you don't necessarily think it is. In other words, you think that you are being paid, but you are not.

1. ACH scams.

Generally, ACH payments are secure and present management companies with the convenience of receiving online payments from their residents without the hassle of processing cash or checks. Nevertheless, it's important to be aware of how ACH payments can be problematic and expose you to scams from a malicious third party (i.e., a fraudster) or your tenants.

Some property owners access the ACH Network directly through their bank. The low cost per transaction, control over the process and prior relationship with a banker may all contribute to the decision to go this route. However, the ACH Network can be a dangerously powerful tool. Once permitted to access it, all you need are an account and routing to forcibly take funds out of an account and send them to yours. In the hands of legitimate property owners and managers, this is a perfectly safe method. However, when you rent to a scammer, this method of receiving security deposits and rent becomes dangerous.

Delinquent tenants have no shortage of excuses. Likewise, if there's a way to dodge a rent payment, they'll find it. With ACH, there are a couple of different schemes they use:

- **Debit chargebacks**
  It is always possible to dispute an ACH charge, and, as long as the funds are still in the receiving account and the dispute is ruled in their favor, those funds will be returned. Suppose a fraudulent resident submits an online payment using a debit card but doesn't have a history of paying via that method. In that case, they may be able to successfully dispute the charge and pull the money back out of your account. They know they won't be able to do it continuously but can do it right before an eviction proceeding, go into court and show a judge that they've paid the rent. If the rent has been paid, an eviction will not be ordered.

  The result of this scheme is a one-two punch. After initiating the chargeback, the fraudster succeeds in not paying the rent ***and*** resetting the eviction process, which causes the property owner to incur more financial loss.

- **Deposit schemes**
  While it is common practice for business owners to give their account and routing numbers to businesses, like the vendors from whom they buy parts and supplies, the practice does not play out well with renters. Coupled with a few other key pieces of information, account and routing numbers can be used by fraudsters to gain access to a multifamily property's online banking account (and, as noted above, if the account is ACH Network enabled, that can be quite dangerous).

  Moreover, when property owners arrange to have residents pay rent by depositing the money into the property's account each month, the property owner or manager loses control over payment rejection. This might sound trivial, but it must be noted that if a residentdeposits as little as $1 into the property's bank account, it might compromise the owner's ability to evict them.

  In situations where you use ACH to take funds out of the renter's account for rent payment, fraudsters have other nonpayment strategies related to ACH:

  - **ACH Return Code R03: No account or not able to locate an account**
    In this case, the account numbers provided by the fraudster to the property manager or leasing agent are the proper number of digits. Still, the name on the account either doesn't match that of the fraudster or the account number is linked to a closed account. In the meantime, the lease is signed, and the keys are in the fraudster's hands.

- **ACH Return Code R07: Authorization is revoked by the receiver**
  In this case, the resident revokes previously approved debits from his or her account. Fraudsters know that they have 60 days from the date of the payment to claim that it is an unauthorized transaction. So, they sign the lease and agree to pay the security deposit and rent via ACH that you initiate.

  Once the lease is signed and they live in the apartment for 30 days, they are considered to have established the apartment as their permanent residence (which later complicates attempts to evict them). Then, they revoke the payment.

- **ACH Return Code R08: Stop payment**
  This is exactly what it sounds like. The fraudster places a "stop payment" on his/her/their account to stop payments from their account to the property's account.

2. Credit card chargebacks.
Credit card transactions are incredibly convenient and are often in high demand from renters. Legitimate renters are not the problem. However, fraudsters know how to circumvent paying the credit card bill after charging the rent to their card. That circumvention tool is appropriately called a "chargeback," the process of returning funds to the buyer — in this case, the fraudster.

A credit card chargeback happens when an individual calls the credit card issuer to dispute a charge that has been made using their credit card. This option allows credit cardholders to dispute payment for something that someone else purchased using their card without their knowledge or consent.

Rental fraudsters take advantage of this process by disputing charges for rent payment. All the fraudster needs to do is call the credit card issuer to dispute the charge. If the bank goes ahead with the chargeback, the card issuer withdraws the rent money from the property's bank account.

Occupancy & maintenance: Squatting, trafficking

Fraudsters often rent apartments to use as a home base for illegal activities, such as drug or sex trafficking. They sign a lease with no intention of ever paying rent. Today's rental fraudsters know not only how to commit leasing fraud but also how to "play the system" when eviction proceedings commence. They're skilled in methods of delaying convictions and will do so as long as they need the apartment to carry out their illegal "business" activities.

Another tactic, squatting, is as old as the ages. It's easier to carry out in its present form than most property managers would think. It's called the prospect's unexplained urgency to rent. The fraudster's initial contact with the property manager or leasing agent is fraught with urgency, often expressed as despair over their need to quickly find a suitable place to live. This leads the leasing staff to either not use all screening methods or to push the application through to quick approval. Once the fraudster signs the lease and moves in, the rent goes unpaid and other trouble ensues. Evicting the fraudster will prove daunting, and even when those efforts are successful, the fraudster almost always leaves behind a trail of destruction.

Section 4: Challenges and Impacts

Operational challenges caused by rental fraud

The majority of fraud is detected after move-in, not during the application process because 40% of centralized property managers and 42% of property-centric and regional managers find it difficult to manage inconsistent processes and standards for each property. They say it's their most significant challenge.

Participants also cited eight additional fraud reduction challenges:

1. Too many people with the ability to override application rejection decisions (39%)
2. Lack of financial motivation among onsite staff to prevent rental fraud (39%)
3. Pressure to maintain occupancy (38%)
4. Fraud prevention services increase operational costs (36%)
5. Employees don't understand the signs of rental fraud (35%)
6. Inadequate staffing to conduct effective screening (30%)
7. Fear of losing good tenants due to complicated application processes (30%)
8. Potential to be perceived as discriminatory (17%)

Applicant screening methods

According to study participants, the applicant screening methods most often used by property managers to detect renter fraud are financial documents (70%) and basic background screening (69%). However, credit scores and criminal background checks are ineffective when a fraudster uses a stolen identity. The same holds true for pay stubs, W2s, bank statements and other financial information when stolen documents are submitted with a rental application.

Rental history screening services (i.e., evictions, skips) are used by 57% of study participants, with ID document verification services (i.e., passport, driver's license, etc.) following closely behind at 52% usage.

Advanced identity verification (device assessment, facial recognition) is used to a greater degree among property managers in centralized roles (41%). The percentage drops significantly among regional managers (29%) and property and site-level managers (25%).

The low incidence of such advanced verification is a vulnerability that fuels rental fraud. Forged identity documentation is easy to obtain or create using sophisticated tools readily available online. Moreover, approaches for validating information are used inconsistently across rental portfolios.

Metrics used to track rental fraud

When asked about the metrics used to track rental fraud, 77% of study participants said application rejections are their primary method of tracking fraud, with skips and evictions second at 64%. The move-out reason is used by 60% of study participants to track fraud. Bad debt is used by only 29% of study participants.

And therein lies the problem. In other words, the systems and standards used by study participants are largely inconsistent and, therefore, incapable of providing the full gamut of information needed to detect fraud before move in.

Even more startling is the revelation that 65% of study participants use manual verification methods, which are prone to error and don't provide the full picture of fraud after aggregating data from different solutions. And 88% view those rental fraud solutions as "good" or "excellent." Yet, 73% say they saw increased fraud in their multifamily communities in 2023. These opposing revelations point to inadequate fraud detection processes as a major reason fraud is rising.

Financial and reputational impacts

All 402 study participants say using only basic fraud validation solutions impacts overall financial results.

Screening only: 48% with screening only say fraud impacts >15% of their financial results

- 10% say screening only has a >20% impact
- 38% say screening only has a 15% - 20% impact

As other forms of verification are added to the fraud validation process, the impact begins to change:

Financial/ID verification: 26% of those with financial / ID verification say fraud impacts >15% of their financial results

- 4% say financial/ID verification has a >20% impact
- 22% say financial/ID verification has a 15% - 20% impact

Advanced verification: 28% of those with advanced verification say fraud has >15% impact on their financial results

- 3% say advanced verification has a >20% impact
- 25% say advanced verification has a 15% - 20% impact

When asked to imagine a scenario where rental fraud prevention technology advances to the point where fraud could be eliminated, all 402 study participants agreed that their portfolio's overall financial results would improve, with the majority saying finances would improve by 10% - 15%.

- 43% would see 10% - 15% improvement
- 30% would see 15% - 20% improvement
- 13% would see >20% improvement
- 13% would see 5% - 10% improvement
- 1% would see only 1% - 5% improvement

Impact of centralization on fraud prevention

Rental application approvals are trending towards centralized decision making, as 59% of study participants agree that decisions at their multifamily companies are becoming more centralized. 40% say decisions are still being made locally and only 1% say there has been no change.

	Property managers in centralized roles	Property managers in property centric/ regional roles
Managing inconsistent processes and standards for each property	40%	42%
Too many individuals overriding application rejections	41%	35%
Onsite staff are not financially motivated to prevent rental fraud	43%	31%
Pressure to maintain occupancy	38%	38%
Increased cost of implementing fraud prevention services	33%	33%
Employees don't understand the signs of rental fraud	35%	36%
Inadequate staffing to conduct effective screening	28%	35%
Fear of losing good tenants due to complicated application processes	26%	35%
Potential to be perceived as discriminatory	22%	10%

Likelihood of reporting fraud prevention challenges

Centralized decision makers are also more likely to report challenges, specifically difficulties with site staff pushing unqualified candidates through the approval process. This is mainly attributable to the level of difficulty experienced by staff when attempting to identify fraud during the screening process, with 37% saying the push represents their greatest challenge.

Unsurprisingly, 47% of centralized decision makers cite detecting income representation as their greatest challenge, followed by counterfeit or manipulated identities at 37%, identity theft at 40% and fraudulent cosigners and guarantors at 35%.

Those in property-centric roles report similar challenges: income representation (45%), counterfeit or manipulated identities (44%), identity theft (37%), and fraudulent cosigners and guarantors (32%).

Section 5:
Best Practices and Recommendations

88% of property management professionals characterize their rental fraud solutions as “good” or “excellent,” yet those using manual validation or spreadsheets find an average of 62% of fraud ***after*** the resident has moved in (61% manual methods, 63% spreadsheets). As underscored earlier in this report, finding fraud after move-in leads to financial losses resulting from unpaid rent, the cost of eviction proceedings, and theft/property damage.

Property management companies with mature applicant screening tools have better fraud prevention outcomes and are less likely to report increased fraud activity in their communities. Detecting fraud before a resident moves in is the key to better outcomes and lower incidents of fraud. Study participants validated that assertion, with 55% saying advanced verification enables them to detect fraud before the resident has moved in.

While 68% of study participants viewed basic screening only as an “excellent” method of verifying identity and financial documentation, that response is sharply contrasted with participants’ response to the question of rising fraud in their communities: 73% reported an increase in fraud in their communities, and 73% also report that 59% of fraud is detected only ***after*** residents move in, not before. If basic screening were enough, a greater percentage of fraud would be detected ***before*** move-in, not after.

Preventing fraud before it can cause financial, property and reputation damage is essential for mitigating risk and curbing the rise of fraud nationwide. We recommend the use of advanced verification and tools that provide single-view analysis.

Are prospective renters who they say they are?

First, you’ll need a sophisticated identity verification process that should be introduced to prospective renters as early as possible in the application process or even before a tour. This is akin to having a security sign on one’s front lawn. Sometimes, simply having such a sign deters fraudsters and causes them to move on to a softer target. But, as we’ve seen the fraud landscape shift and fraudsters become more emboldened over the past few years, property managers still need an extremely high-functioning identity verification solution. We recommend a solution that enables a five-phase process.

Sophisticated identity verification solution: A five-phase process

1. Data verification

Collect core personally identifiable information, such as first/last name, DOB, SSN, address, email/phone and multiple authenticated data sources to verify that the information provided is real and not stolen or related to malicious/fraudulent activities.

2. Device & network verification

Validate the prospect's device, phone number, IP address, and its historical associations & reputation. Verify that they can access it through a one-time passcode.

3. Identity document verification

Verify that a physical photo ID is not fraudulent and the Personal Identifiable Information (PII) on the ID matches the data from the first process. Ensure you can verify a wide range of ID types including non-U.S. IDs.

4. Biometric verification

Verify that the applicant is a real person by using a live "selfie" that is compared to and matches the selfie face-to-face on the document.

5. Contextual analysis

This last step should be implemented consistently throughout the process, as it is one of the most important functions. All data collected and verified should be cross-referenced wherever possible to ensure that each step builds on the results of the former step.

This solution has many variants, with different levels of involvement from the leasing staff and the prospective renter. The tool you implement should be robust yet easy for all parties to understand.

A good solution should also save some manual steps by storing verified documents and results in the PMS. For the best consumer experience, this should be performed during the application or touring process when information is collected from prospects rather than waiting and reengaging them after completing the application.

Income verification: Can the prospective renter afford the unit selected?

A technical income verification process should be in place to validate prospects' ability to make timely rent payments. There are three methods of verifying income:

1. Bank verification

Leverage modern financial APIs (Application Programming Interfaces) to allow prospects to connect their deposit data directly so you receive an instantly verified understanding of an applicant's income.

2. Payroll providers

Connect directly to a prospect's payroll company to instantly retrieve verified paystubs.

3. Document verification

Allow prospects to provide income documentation that can be scanned and analyzed for fraud using highly curated AI & machine learning models. It can then be run through an optical character recognition program that extracts and parses the income data into your PMS.

Prospective renters need to verify income in only one of these three ways. However, because not all prospective renters are the same, offering a wide variety of methods is important. Document verification is by far the riskiest method and should be relied on as a failsafe alternative to your leasing staff making their own un-supported decision.

When evaluating an income verification software solution, remember that any data not directly provided by prospects or altered consumer-provided data will likely be subject to FCRA compliance. As with identity verification, any income verification documents or results should be easily understood and stored in the PMS to reduce the leasing team's effort.

Using verified PII increases accuracy in applicant screening

Once the applicant's PII and financial data are confirmed, both can be utilized, partially or entirely, by an applicant screening solution to determine if the applicant aligns with the property's requirements. It's imperative for the initial step in applicant screening to validate that the submitted PII is accurate and belongs to the applicant. This will ensure precise results in applicant screening searches. The risk of using unvalidated data can be detrimental to a property, resulting in missed landlord-tenant records, criminal histories and inaccuracies in credit reports.

Moreover, ensuring the overall safety of the property, residents and staff is paramount. Validating that applicants are who they claim to be and that their data is accurate instills confidence that any criminal records used in housing decisions align with the property's acceptance criteria. Errors in name spellings and birthdates can impair criminal searches, prohibiting using social security numbers and other unique identifiers to access records.

Scoring methods available in today's applicant screening landscape

Many screening providers employ statistical or AI models, integrating diverse inputs like credit tradeline data, credit score, rent-to-income ratio and debt-to-income ratio to assess the overall risk the applicant poses. Conversely, some screening providers offer only rules-based screening options or a combination of rules-based scoring with statistical methods.

Using credit tradelines alongside rent-to-income calculations gives property managers insight into an applicant's overall financial health, capacity and willingness to fulfill rental obligations and other financial commitments throughout their lease term. Numerous screening providers automatically disqualify applicants with specific collections indicating outstanding balances with rental communities or utility companies.

Utility collections are another challenge that potentially obstructs applicants from securing utilities in their name upon moving into the apartment. Applicants with rental and utility collections are considered high-risk due to the strong predictive correlation between past behaviors and future actions. This may lead to properties incurring significant bad debt if the applicant prematurely terminates their lease.

Screening companies can further assess the risk of an applicant not completing their lease term by examining landlord-tenant data and previous rental history. Like rental collections, any negative data linked with a previous rental suggests an increased likelihood that the applicant will leave the property with outstanding balances.

Conclusion

As savvy fraudsters continue to acquire more and more sophisticated methods of perpetrating rental fraud and as multifamily is increasingly caught in the crosshairs of organized fraud rings, it's astonishing that 68% of property managers say basic screening only is an "excellent" method of verifying applicant information. That's sharply contrasted with the 75% who say fraud has risen in their multifamily communities since 2023 and that more than half of fraud (59%) is detected only ***after*** residents have moved in.

The sad fact is that if basic screening were sufficient for fraud detection and prevention, a greater percentage of fraud would be detected ***before*** move-in, not after. This underscores the need for advanced verification methods and tools that facilitate single-view analysis portfolio-wide so fraud can be detected early in the application process.

Unfortunately, spreadsheets weren't designed for fraud detection, prevention or tracking. They simply lack the analytical tools necessary for those tasks. An eyeball examination of identity and financial documents is also insufficient for detecting fraud, given the sophisticated methods fraudsters use to acquire or create fake documentation. The risk is incredibly high across a portfolio of properties where fraud detection is a per-property operation.

Suppose you want to move the needle on fraud detection in your multifamily communities and increase the likelihood of detecting it before the lease is signed. In that case, you need to consider adopting a robust solution with advanced capabilities, single-view analysis and document storage. RealPage Screening solutions provide the tools, knowledge, and insights to lease confidently while limiting risk.

We use the industry's largest rental payment history database, in-depth criminal background information and extensive credit checks — including credit reporting from Equifax and Transunion — to help ensure the security of your property and residents.

RealPage Artificial Intelligence (AI) Screening is more than just a credit score on the ability to pay — it's about the applicant's willingness to pay. This innovative solution leverages the power of AI and machine learning to precisely analyze your applicant pool, which delivers a stronger predictor of future performance and renter behaviors. It's proven to reduce bad debt and financial loss by an average estimated savings of $39 per unit per year.

Our screening solution, built to meet the needs of the multifamily industry, is the first — and only — AI-enabled scoring model that offers:

- Revolutionary, AI-based predictive scoring model
- Seamless integration with your rental application and leasing process, no matter what property management system you use

RealPage Identity Verification uses comprehensive and dynamically updated identity intelligence and pattern recognition to detect fraudulent applications. An integrated and seamless three-step approach verifies an applicant's identity within seconds and provides a contactless ID validation process. Properties can confidently prove applicants are who they claim to be before they move forward in the application process, reducing future eviction risk and expense.

Plus, RealPage is a fully integrated solution for applicants and property staff. It enhances the user experience and cuts down on manual processes and time wasted throughout the leasing journey. And it's the only enterprise identity platform that guards against identity fraud at the points of tour, application and payment. Screening a prospect before a "self-tour" safeguards the property and reduces friction during the application process by re-using the verification from the tour. All interactions occur via the prospect's mobile phone, and validation results are available ***in just seconds*** (pass or fail) in a contactless experience.

Contact RealPage today to learn more about how our AI Screening solution can help you stem the rising tide of fraud in your multifamily communities.

realpage.com | 1-87-REALPAGE

REALPAGE®