



The Comprehensive Guide to

Spotting Fake Documents

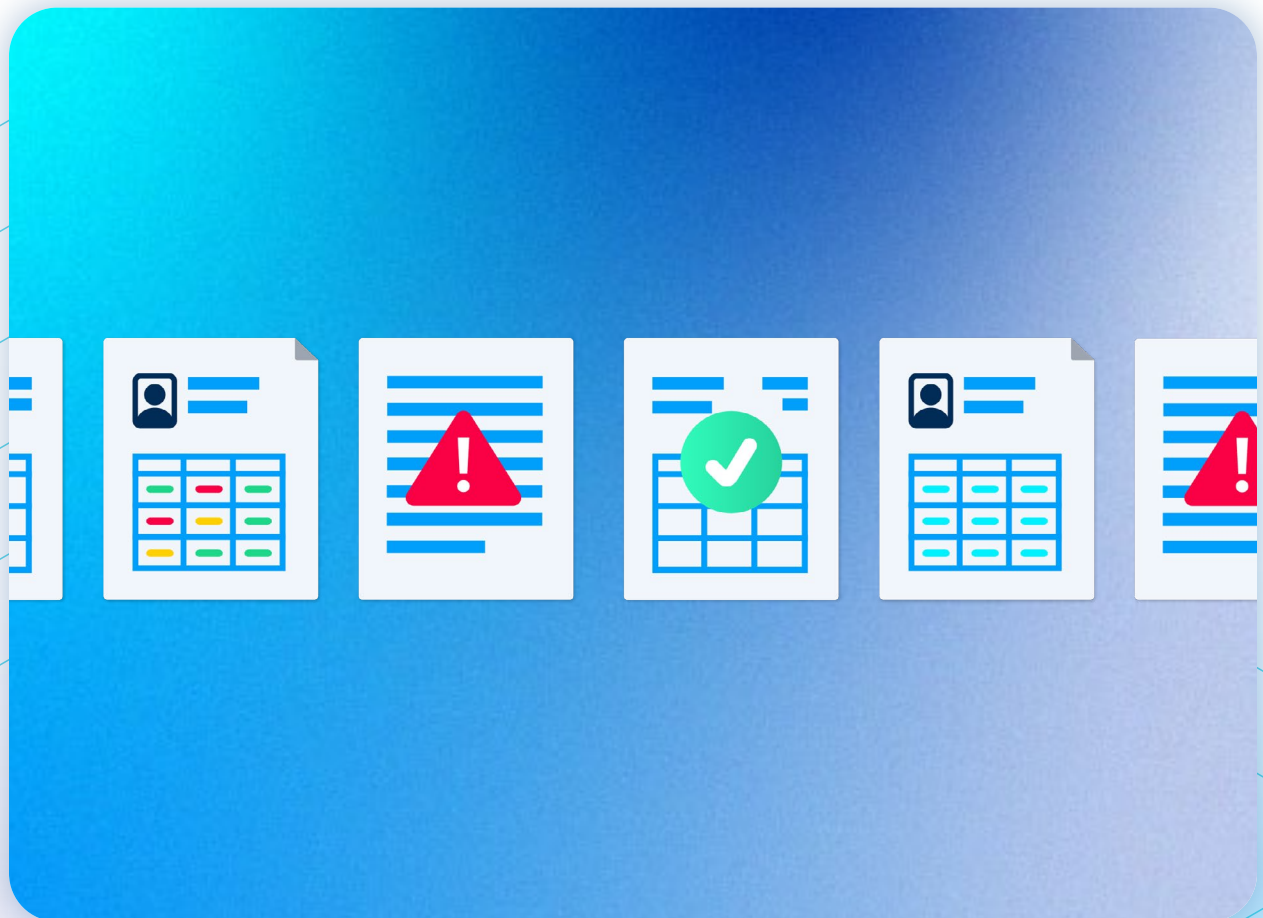


Table of Contents

3	Introduction
4	Fraud by the Numbers
5	How to Spot a Fake US Passport
7	How to Spot a Fake Social Security Number
9	How to Spot Fake Proof of Address Documents
10	How to Spot a Fake ID
12	How to Spot a Fake W-2
13	How to Spot a Fake Utility Bill
14	Digital Document Alteration: 101
15	How to Spot a Fake Bank Statement
17	How to Spot a Fake Pay Stub
18	Conclusion

Fake Documents, Real Consequences

Whether it's an application for a bank account, a loan, or an apartment lease, each requires all sorts of documents. So, if you're the one reviewing applications, expect to review at least 4-5 documents — ranging from passports and driver's licenses to pay stubs, bank statements, and utility bills.

And guess what? Each one could be a fake.

Document fraud is a rapidly evolving and growing problem — no one's immune. It spans industries, from banks and insurance companies to phone providers and property management firms. Everyone is susceptible to the increasing threat of document fraud.

What's worse, creating fake documents is easier than ever thanks to AI, the internet, and bad actors. Would-be fraudsters can simply Google “utility bill generator” or “pay stub template” to create fake documents in seconds.

Thanks to AI, scammers can forge more realistic documents faster and with less effort, [churning out passable fakes in minutes](#). But it's not just one-off fraudsters.

Fraud is a booming industry, complete with how-to tutorials and [fraud-as-a-service \(FaaS\) marketplaces](#). These services also come with 24/7 customer support and detailed instructions.

Central to these schemes is [synthetic identity fraud](#)—a technique scammers use that combines real and fake information. Data breaches leak personal data like names, addresses, and Social Security numbers, which fraudsters then take to piece together fake identities.

Consulting firm KPMG calls synthetic identity fraud “the fastest-growing financial crime in the United States,” and the Federal Reserve Bank of Boston estimated that [costs from synthetic identity fraud topped over \\$35 billion in 2023 alone](#).

Between AI, professional fraud schemes, and a tight housing market, fraudsters can quickly create forgeries convincing enough to slip past manual checks. In 2024, TransUnion reported that [38% of property managers didn't catch the fraud until after the tenant moved in](#).

And [the costs of missing fraud add up fast](#). You might take on bad debt when tenants who faked their income can't pay rent, potentially ending in an expensive eviction. Or you have to go to court to recoup costs from property damage. And last but not least, you might lose your reputation and the community's trust.

With such extreme consequences, you need to know how to combat document fraud before it creeps into your community. We're diving into eight commonly faked documents, including why these are top targets for fraud and how you can spot fakes before they hurt your business.

If a typical 350-unit property management portfolio experiences a low 2.5% fraud rate, [that portfolio would face an annual financial risk greater than \\$50,000](#).

Rental Application Fraud by the Numbers

70%

of properties reported the use of someone else's personal information or fraudulent ID documents¹.

70 weeks

The average minimum length of time it takes to evict a tenant².

\$4.2M

Victims of fraud had to write off an average \$4.2 million in bad debt¹.

50%

of property managers reported damage as a result of rental fraud³.

Sources:

¹ National Multifamily Housing Council's NMHC Pulse Survey: Analyzing the Operational Impact of Rental Application Fraud and Bad Debt

² Snappt's How Long Does it Take to Evict Someone?

³ RealPage Newsroom's RealPage Details Complexity of Fighting Fake Identities & Documents in Multifamily's Largest National Fraud Survey to Date

Also, look out for font variations, misspellings, or grammar mistakes that are clear signs of forgery. Lastly, pay attention to the layout. Passports follow strict rules, so if you see any mismatched alignment or unusual spacing, mark it as suspicious.

Next? Security features. Perhaps one of the most important elements of a passport, these features are a surefire way to tell whether a passport is authentic or a fake:

- **Machine-readable zone (MRZ).** The [MRZ](#) is a section of alphanumeric text at the bottom of the data page with the holder's photo and personal details. A machine scans this text to display information about the document and its holder. If it can't process the MRZ, the passport might be fake.
- **UV images.** Under UV light, passports will reveal illustrations that often represent a country's history or geography. Blurry, incorrect, or nonexistent UV images are signs of forgery.
- **Holograms.** Embossed holograms should change color as you move the document back and forth under a light. Fake embossing looks blurry and doesn't change color.
- **Watermarks.** Watermarks are superimposed text or images. They shouldn't change color under UV light or be placed in areas not commonly seen on real passports.

Last but not least, compare the personal details and signatures against other documents. Cross-referencing the passport holder's name and date of birth against other documents highlights inconsistencies that could suggest fraud. See mismatches? Examine the documents with more scrutiny.



Pro tip

Memorizing the security features of a US passport is hard enough, but this can feel impossible with hundreds of international documents. Use a reference, like PRADO's document library, or look for a document fraud detection tool that can automatically verify documents from hundreds of countries in seconds.

How to Spot a Fake Social Security Number

For decades, many organizations have considered Social Security numbers (SSNs) an individual's unique identifier. They're a crucial piece of data businesses rely on to run credit or [background checks](#), but SSNs are also necessary for:

- Filing taxes
- Signing up for health insurance
- Receiving government benefits
- And more

We often use them for high-risk activities, like opening bank accounts or collecting benefits. And that's why they're prime targets for fraudsters looking to use SSNs for identity theft or to create synthetic identities.

What is Synthetic Identity Fraud?

Synthetic identity fraud involves a mix of real and fake identity information. Cybercriminals mine personal information exposed in data breaches

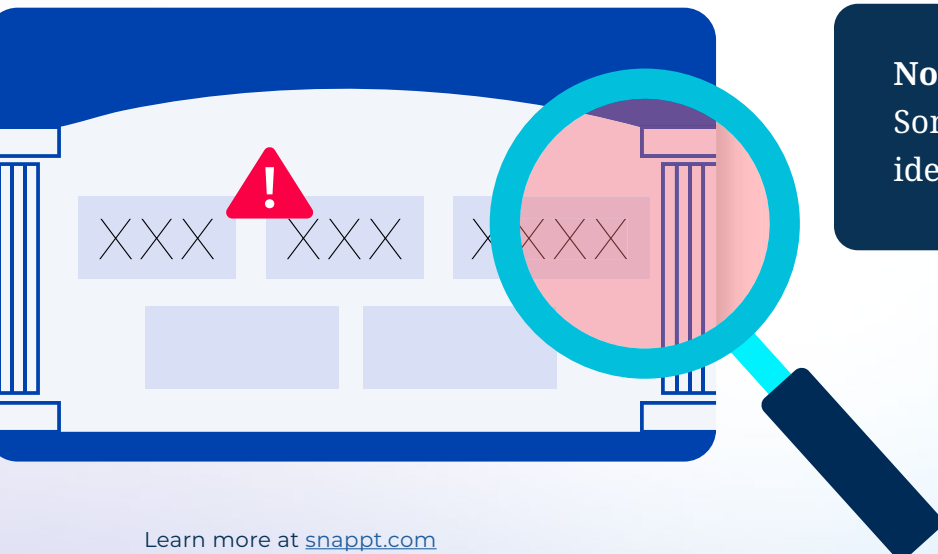
to fabricate an entirely new identity. This identity uses one person's SSN, another's email address, and yet another's date of birth.

And many Americans are at risk: [1,857 new data breaches in 2024 included Social Security numbers](#), each one an opportunity to create hundreds of new synthetic identities.

The American Bankers Association reported that [synthetic identities in account openings rose 18% in 2024](#), and synthetic fraud is making up a growing share of fraudulent activity. The Global Compliance Institute found that [over 80% of new account fraud is related to synthetic identity creation](#). In the US, each loss to synthetic fraud is around \$15,000.

Unfortunately, SSNs are easy to fake. They're always in the same format—000-00-0000. A quick glance at a Social Security card, which doesn't have special formatting or security features, won't tell you that the number is fake.

Note: Not everyone has an SSN. Some people may have a taxpayer identification number (TIN) instead.



Signs of a Fake Social Security Number and How to Spot Them

Catching a fake Social Security number is more about cross-referencing than document inspection. When you compare a Social Security card or SSN to other data, does it match up?

SSNs don't have the same built-in security features that passports or driver's licenses do, but there are a few things you can check for:

- **Impossible or non-permitted numbers.** SSNs never start with 000, 666, or 900–999. If an applicant presents one that does, it's a fake.
- **Mismatching digits to location.** Pre-2007, the Social Security Administration (SSA) assigned the first three digits of the SSN based on someone's location. For those born in the US, it was often their state of birth. If a US-born citizen received their SSN before 2007, the first three digits should align with their place of birth.
- **Issuance date.** After 2007, the SSA began listing an issuance date on Social Security cards. If the cardholder was born in the US after 2007, their card's issuance date should be no more than a couple of months after their date of birth.
- **Signature mismatch.** All SSN holders should have signed their card when they turned 18. Although people's signatures can change over time, the signature on the card should be similar to the signature on other documents.
- **Suspiciously short or non-existent credit history.** A major problem with fake identities is that the identity hasn't been around for very long. If you run an SSN through a [credit check](#), chances are the credit history will be short. Don't forget—recent immigrants or younger adults will have short credit histories.

Review the credit report for any previous addresses and see if they match utility bills or bank statements. For lease applicants, compare their rental history against the addresses in their credit report.

A more foolproof method involves using the SSA's Consent-Based Social Security Number Verification Service (CBSV). You can find it on the administration's [Business Services Online \(BSO\) portal](#). The CBSV allows private companies to check that the SSN, name, and date of birth match SSA records.

Keep in mind that people who received an SSN later in life, like immigrants, will have a much later issuance date compared to their date of birth. Any card issued before 2007 will not have an issuance date.

How to Spot Fake Proof of Address Documents

Fraudsters might want to establish false residency in a specific location to apply for benefits, open a bank account, and more. They can do so by providing proof of address through many document types, including:

- Utility bills
- Certified mail
- Bank statements
- Lease agreements
- Tax forms
- Driver's licenses
- Voter registration cards
- Vehicle registration

The problem? Many of these documents are easy to fake. Online templates for utility bills and bank statements are everywhere. And with a wide array of legitimate formats across banks and utility providers, it's hard to catch inconsistencies.

Signs of Fake Proof of Address Documents and How to Spot Them

With wide variation between document formats, verifying proof of address can feel impossible. But catching a fake proof of address is all about the details.

First, check that the address is real and belongs to a residential address. For example, if you type the address into a tool like Google Maps and the street image is for an office building or a Starbucks,

chances are that's not the person's real residence.

Also, check the elements in the address, such as a missing unit number or an incorrect ZIP code. Then, look at the document itself. A quick skim can help spot serious issues:

- **Outdated documents.** Utility bills and bank statements should be no more than three months old. IDs should not be expired, and [lease agreement](#) dates should be current.
- **Screenshots.** All documents should be originals—never accept screenshots.
- **Formatting problems.** Pixelation, blurry text, misaligned columns, inconsistent fonts, or outdated logos can all point to alterations or forgeries.
- **Contact details.** Proof of address documents should include contact details from the issuing party, like a utility company or property management firm.

Once you've confirmed the address is legitimate, compare it against other documents the applicant shared. The address should match across all current documents, including lease agreements and bank statements.

How to Spot a Fake ID

Driver's licenses are commonly used to verify address and date of birth, opening the door to age-restricted activities and purchases. These high-demand documents are widely available online for cheap. And thanks to GenAI, fraudsters can create a convincing driver's license for \$15 in under two minutes.

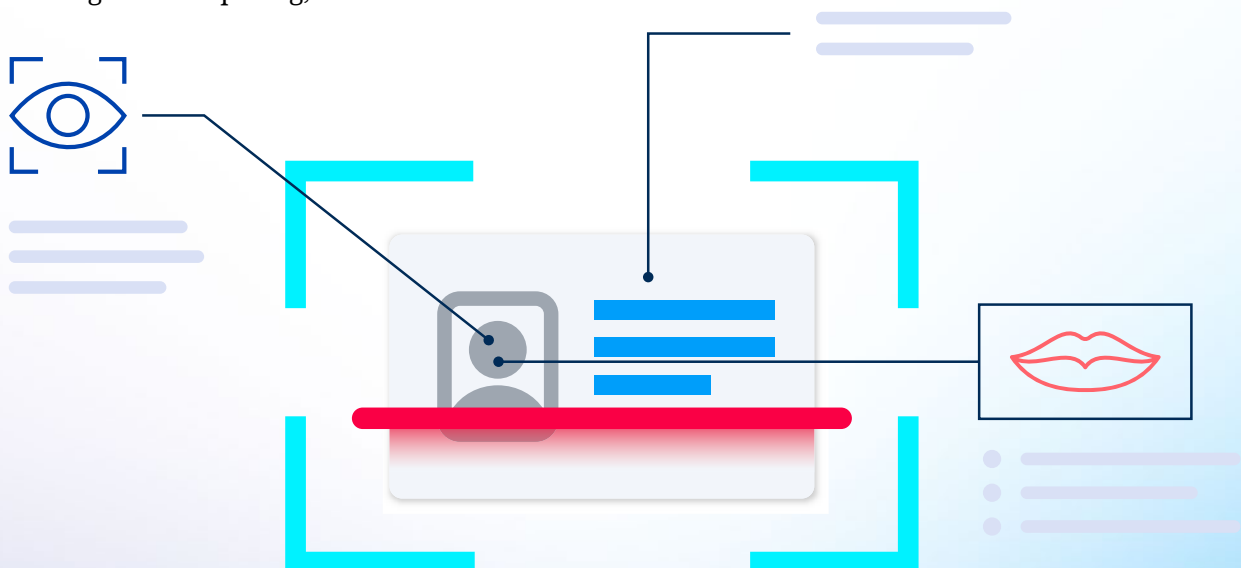
In addition to being easy to create, each state has its own formatting and design standards, so authentic IDs may be hard to validate with over 50 legitimate designs. In high-traffic areas like restaurants and grocery stores, driver's licenses often only get a quick skim. Fraudsters rely on this surface-level review to perpetrate their scams.

Signs of a Fake ID and How to Spot Them

Take your time to carefully review every detail of the ID to ensure you don't miss the red flags that point to a fake. First, look at the ID itself for physical signs of tampering, like:

- **Size.** Driver's licenses are a standard size—the same as a credit card—so hold the license up to a real credit card to see if the edges line up.
- **Lamination.** States use a high-quality laminate that isn't widely available. Look for bubbling, lifting, and ragged edges.
- **Printing quality.** An authentic ID shouldn't have blurry text or mismatched fonts. Formatting and spacing should be consistent.
- **Photo.** Photos should be clear and without pixelation. A raised or taped photo is a clear sign of synthetic ID fraud.
- **Many IDs include a smaller, secondary photo on the front and/or back of the ID.** Make sure the primary and secondary photos match. Depending on the issuer, the secondary photo may be a mirror image of the primary photo.

Like passports, driver's licenses have security features to make counterfeits easier to detect. Many states publish these standards online and share notices of design updates, so you can easily spot a fake.



Look closely for correct watermarks, holograms, UV images, and laser perforation—an image made up of very small holes that’s hard to see unless under direct light. You’ll also want to compare the data on the ID with public datasets:

- **Barcode.** Most IDs include a barcode that, when scanned, returns basic data about the license holder, including name, age, and address. These scanners are available through apps that use your phone or tablet’s camera.
- **Voter registration.** Voter registrations are public. They include a voter’s name, birth year, and address. You can use sites like [Vote411](#) to find a state’s voter registration.
- **American Association of Motor Vehicles Administrators (AAMVA).** For some (but not all) states, the AAMVA verifies a driver’s license holder’s name, birthdate, expiration date, and barcode.

Last but not least, compare the information on the ID to the holder and other documents.

Cross-reference personal data like name, date of birth, and address to other documents, including passports, tax forms, bank statements, and pay stubs.

Ask yourself if the ID holder’s physical appearance matches the physical appearance information on the ID. Compare the signature on the driver’s license to the one on the applicant’s passport, lease agreement, or Social Security card. And if the applicant is under 21, check that the orientation aligns—many states use vertical orientation for drivers under 21.

Pro tip: Professional organizations like [the National Notary Association](#) offer guides for checking both international and domestic IDs, but manual review is time-consuming. [Automated ID verification](#) is quick and accurate, combining [AI-enabled document inspection](#) and biometric checks like facial recognition.

Bonus points—if you’re completing remote ID verification, many [selfie ID verification tools](#) include liveness checks that confirm the person is a real person and not just a photograph.

Passport and ID Security Features

Passports and driver’s licenses share many security features. When reviewing an identity document, look for the placement, accuracy, and print quality of these features.

Hologram

These images appear when you move the ID back and forth under a light. Authentic holograms change color and aren’t blurry.

Watermark

This text or image is often superimposed on another element of the ID, like a secondary photograph. Watermarks shouldn’t change color when you move them under a light.

Laser perforation or engraving

Passports feature laser-engraved text, like serial numbers or personal data, and driver’s licenses may have a laser-perforated image specific to that state.

UV images

As the name implies, UV images appear when you hold an ID up to a UV light source. These images often feature a country or state’s history or geography. They shouldn’t be blurry.

How to Spot a Fake W-2

W-2s are a common way to provide proof of income, but fraudsters often falsify them to inflate earnings when applying for loans, credit cards, and leases. Accepting a false W-2 might mean approving a tenant or credit card holder who can't make payments, creating the risk of bad debt.

Although W-2s are government forms, formatting inconsistencies across states and employers can make it difficult to spot forgeries. Plus, many employees opt to receive their W-2s online, making them a prime target for fraudulent templates and digital alteration.

Signs of a Fake W-2 and How to Spot Them

Catching a fake W-2 comes down to three steps:

1. Independently verifying employment
2. Checking the math on deductions and tax rates
3. Comparing the numbers against pay stubs and bank statements

First, review the employer information. If you're also verifying employment, now is a great time to independently confirm the employer's name, address, website, and phone number to ensure that the organization is legitimate.

Next, number crunching. Check that the math checks out:

- **Rounded numbers.** The IRS wants exact figures, so be wary of numbers that end in .00.
- **State and local tax rates.** Confirm that the amount withheld aligns with the correct tax rate. For example, if a state has a flat income tax rate of 4.5%, the amount withheld divided by state wages and tips should equal 0.045.
- **Federal tax withholdings.** Review the amounts withheld for federal income, Social Security, and Medicare taxes to ensure these amounts aren't suspiciously high or low.

Then, check for IRS formatting requirements:

- **Official text.** "Form W-2 Wage and Tax Statement" should appear at the bottom of the document.
- **Copy letter.** Employers must file multiple W-2 copies with federal and state agencies, each labeled "A," "B," or "C." Employees should only receive Copy B or C—not A.

And, of course, use supporting documents like bank statements and pay stubs to verify income and catch inconsistencies that could point to fraud.

How to Spot a Fake Utility Bill

With so many providers across utility types (electrical, gas, internet, and so on), it's nearly impossible to verify a utility bill on formatting alone. But there are a few things you can check to suss out the fakes.

Review the basic information and look for inconsistencies or missing data:

- **Name and service address.** Check that the account holder and service address match other documents, like a driver's license. Confirm that the service address is for a residence, not a business.
- **Account number.** Missing account numbers or those that contain multiple sequential digits are suspicious.
- **Billing period and date issued.** Ask for the most recent utility bill and determine when the billing period ended. If the bill was issued a month or more after the billing period ended, keep looking.
- **Issuing company.** Independently verify the utility provider's address, website, and contact information. Compare the bill's font, colors, and logo with the provider's website.
- **Payment instructions.** Payment options should be by check, phone, or online portal. Legitimate utility providers don't accept payments by Venmo or Zelle.
- **Units of measure.** Confirm that the itemized charges use standard units of measure. For example, confirm that an electricity bill charges by kilowatts (kW) rather than watts.
- **Rates and rate schedule.** Ask for the provider's rate schedule and cross-reference this against the bill's itemized usage and charges.
- **Payment instructions.** Ask the provider if they can share their payment instructions, including the billing portal website address, phone number, or where to mail checks.
- **Account information.** Some utility providers will allow you to share an account number, and they can confirm the account details. Note that because of data privacy laws, not all utility providers will share this information.

You can also contact the utility company to verify essential pieces of data, like:

Still unsure? Ask for multiple months of bills. Look for unexplained, large swings in usage from month to month. Also, check that the remaining balance on one bill aligns with the starting balance on the next.

You'll also want to look for other tell-tale signs of document fudging, like inconsistent fonts, misaligned columns, document elements, numbers, misspellings, typos, or grammatical errors.

Digital Document Alteration: 101

With GenAI, online templates, and readily available photo editing software, digital documents are easy to alter or fabricate from scratch. Whenever you're looking at a digital document—whether it's a utility bill, W-2, or bank statement—look for these signs of forgery:



Branding

Fonts and brand colors should be consistent across the document. Look for out-of-place bold or italic font, changes in font size, or different font families. Company logos should match what's on the company website.



Formatting

Columns and document elements should all be aligned. Examine number and decimal alignment, especially. Accounting software will ensure all digits and decimals are lined up precisely.



Metadata

Legitimate originals aren't likely to be image files, like .jpg or .png. Check the date created against the billing month. For example, if the file's creation date is in March for a bill issued in January, the document may be fake.



Blurring or Pixelation

Text, logos, and images should all be crisp. Any pixels or fuzziness is unusual and warrants a closer look.



Grammar, Misspellings, and Typos

Official documents from the bank, government, or a utility company will not have grammatical errors or misspelled words.



Organization Information

Independently research the utility provider, employer, or bank and compare the website, phone number, and other contact details on the document to what you find online.

How to Spot a Fake Bank Statement

Healthy bank account balances can make [prospective lessees look attractive to lenders](#). Property managers and financial institutions consider bank statements part of applicants' overall financial health and stability. Because of this, bank statements are frequently doctored to make accounts look more flush than they really are.

Each financial institution has its own statement formatting, so variations across banks can make alterations harder to spot. Plus, banks sometimes change their statement formatting, adding another challenge to verifying the authenticity of a statement.

Missed bank statement fraud can lead to the acceptance of unqualified applicants who are in worse financial shape than they first appear. These applicants might then miss rent or loan payments, and the approving institutions may [take on bad debt](#) as a result.

Signs of a Fake Bank Statement and How to Spot Them

Most scammers only need patience and access to a tool like Photoshop to doctor a bank statement. But would-be fraudsters may slip up when it comes to the precise amounts, formatting, or math.

Account Statement
Business Checking Account

Statement Period:
Account Number:

Account Summary

Checks Paid

Look closely at the document's appearance, including the values on each line, text, and layout:

- **Decimals.** Real bank statements use exact amounts, so many transactions with round numbers (ending in .00) should be a red flag.
- **Spacing.** Accounting software maintains even, precise alignment for numbers and decimals across columns and rows. Even with editing tools, changing the numbers on a bank statement can throw off the alignment because different numerals may have different widths.

For example, changing a narrow numeral like “1” to a wider “5” might shift all the characters around it.

- **Brand logo and colors.** Check the bank's website to confirm that the logo, font, and colors on the statement match.
- **Font.** Many companies, including banks, use custom fonts you can't find in Photoshop, Word, or Google Docs. Mismatching fonts, like mixing a serif and a sans serif, can be a sign of an altered document.
- **Typos.** Bank statement templates receive multiple rounds of editing before publication, so read the text carefully to spot misspellings, typos, or grammatical mistakes.

Next, crunch the numbers. Forgers might be able to edit the numbers on a bank statement, but even with AI, they may not do the math correctly. Run through the deposits and withdrawals to see if the transaction amounts and resulting account balances are correct.

Ask for multiple months of statements and look for inconsistencies. Ask yourself:

- Does the ending balance on one bank statement match the starting balance of the next one?
- Does the account have excessive funds, but also many overdraft fees?
- Do any withdrawals look suspicious? These might include multiple automatic withdrawals of high amounts, off-cycle paycheck deposits (not on the first, 15th, or last of the month), or unusually large cash deposits.

Lastly, use the other documents available to you to cross-reference. For example, you might compare pay stub payments to deposits or get an employment verification letter and review the stated salary against deposits. Or compare the rent in a lease agreement to monthly payments and review transfers between the applicant's other checking and savings accounts.



Pro tip

Bank statement fraud can be subtle, but inconsistencies rarely hide for long when you cross-check documents. Always verify deposits against pay stubs or income verification and confirm that ending balances align month to month. If something doesn't add up, trust the math—it's often your first clue to fraud.

How to Spot a Fake Pay Stub

Pay stubs are one of the most popular ways to [establish proof of income](#)—and one of the [most commonly forged documents](#). Online generators and templates make forgeries insanely easy. And pay stubs don't have standard formatting or security features, so they're difficult to authenticate.

Signs of a Fake Pay Stub and How to Spot Them

Checking a pay stub for fraud is all about verifying employer and salary data and cross-referencing it with other documents. Use the information on the pay stub itself to get started:

- **Research the employer.** Look into the organization on the pay stub. Is it a legitimate entity? Does its address and other contact information match what's available online?
- **Verify employment.** Go one step further through employment verification. Follow all applicable laws to receive permission from your applicant to contact their employer, and then request that the employer provide the applicant's name, title, income, and dates of employment.
- **Run the math.** Pay stubs should list tax withholding and pre-tax deductions, like health insurance premiums. Check that the amount withheld from the paycheck roughly aligns with federal, state, and local tax rates. Be wary of suspiciously high or low withholdings and deductions.



Pro tip

[Manual income verification](#) can be time-consuming, and even with careful, methodical review, you still might not catch fraudulent documents. [Connected payroll software](#) can [integrate directly](#) with payroll systems to verify employment and income more quickly and accurately.

And don't forget to review the document itself. Even with photo editing tools and AI, fraudsters may miss minor formatting details, including inconsistent font, grammatical errors, misspellings, and alignment issues.

Accounting software lines up all digits and decimals precisely, so if the columns and spacing seem off, take a closer look.

Last but not least, compare the data between documents:

- **Bank statements.** Does the take-home pay on the pay stub correspond with deposits on bank statements?
- **Tax forms.** Do the wages on the pay stub align with the earnings reported on a W-2 or [tax returns, like a Form 1040](#)?
- **ID.** Does the name and address of the pay stub recipient match their driver's license?

Stay Ahead of Fraudsters with Fraud Detection Technology

Every document poses unique risks, and each one only tells part of an applicant's story. Only by inspecting each document and cross-referencing them can you get a full picture and more confidence in its authenticity.

Scammers take advantage of inconsistent formatting across banks, utility providers, and governments. And they're betting that reviewers won't look too closely—or that you're [multitasking and tired](#). Unless you apply the same checks to every document every single time, forgeries will slip through the cracks.

Missing the fakes can have major consequences. Protect yourself by boosting your manual review with advanced fraud detection technology. By combining a human-in-the-loop approach with fraud detection tools, you can catch fraud the first time.

Because no matter how aware you are of the fraud markers, it's nearly impossible to spot them all without robust tech to help. These tools can automatically review documents and return an analysis [in under 10 minutes](#), making your work faster, easier, and more accurate.

You want a tool that can do it all—verify income, confirm identity, and detect fraud—to protect your business and your applicants. Trust is a two-way street. You want to trust the applicants' data and identity, and the applicant wants to trust that your process is fair, transparent, and secure.

Fraud prevention and AI-powered analysis from Snappt can grow that trust to enhance your [multi-layer fraud detection strategy](#). Snappt's [Applicant Trust Platform](#) provides a secure, transparent, and accurate way for property managers and tenants to navigate the leasing process.

Turn Risk Into Reliability

See how the Applicant Trust Platform™ keeps your communities safe and secure.

[Learn more →](#)



S N A P P T

snappt.com

