2024 Document Fraud Report

inscribe

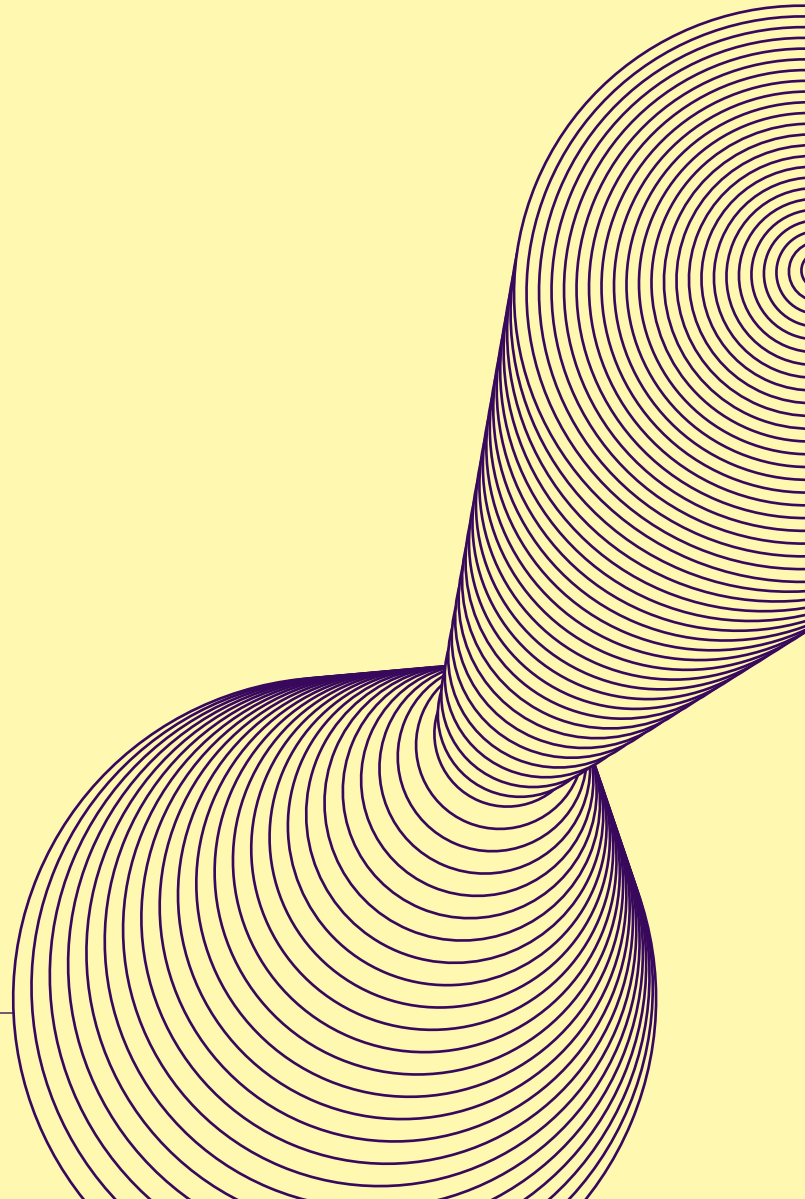
Contents

About this report

Our annual Document Fraud Report was built after an extensive review of the documents Inscribe analyzed throughout 2023, as well as data from a survey of risk and ops leaders taken at the end of the year.

Fraud and credit losses are still on the rise

How we build trust in financial services is changing. A highly digital world has enabled businesses to work with customers from all over the globe and at higher volumes, where decisions must be made in seconds (rather than days) to stay competitive – and many more data sources must be reviewed to establish trust.



Nearly 80% of risk leaders said they saw a YOY increase in fraud attempts during 2023.

At the same time, opportunistic fraudsters and organized criminals are adapting to new onboarding flows and, in some cases, launching coordinated attacks to take advantage of increased automation. This type of fraud can be make-or-break if not addressed.

Companies have traditionally had risk teams manually review customer data for underwriting or KYB/KYC requirements. Despite a digitally transforming world, many of them still do. These teams are expensive and struggle to scale while effectively protecting a business from evolving risks. And the end result is this: Risk teams are growing to untenable sizes, but fraud and credit losses are still on the rise.

In fact, we recently surveyed risk and ops leaders and nearly 80% said they saw a YOY increase in fraud attempts during 2023. Surprisingly, only 42% of these companies have a solution to help them detect fraud in the documents they rely on to make risk decisions. This is especially concerning given that financial services companies saw a 79% increase in document fraud in 2022, and document fraud doubled in 2023.

Why do fintechs and financial institutions still accept documents?

While the use of open banking data is becoming more common, many financial institutions and their consumers lack the technological capability to provide that data or simply don't feel comfortable with connecting bank accounts. Documentation, however, is an accessible and equitable way to build trust with customers. When a customer applies to open an account or take out a loan, financial institutions must conduct due diligence to assess that customer's eligibility. Eligibility is determined by three principles:

01

Validity

Can I do business with this customer?

02

Trustworthiness

Should I do business with this customer?

03

Creditworthiness

How much business should I do with this customer?

Even a risk team's most experienced investigators simply can't see what's been altered in fraudulent documents.

Documents enable you to make those determinations based on data, not conjecture. You can reliably verify an applicant's identity, address, borrowing power, and more by showing that the information has been confirmed by another reputable institution (a bank, utility provider, government, etc.). Documents create borrower transparency and, as a result, trust.

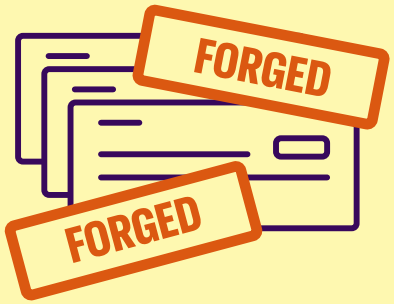
But fraudsters thrive on the anonymity and ease of a digital world; they forge documents with Photoshop, sell counterfeits online, and even teach others how to make fake documents in public social media forums.

And because 90% of document fraud signals are invisible to the human eye, even a risk team's most experienced investigators simply can't see what's been altered. Forcing manual review teams to find these unseeable alterations creates inaccuracies, inefficiencies, long customer wait times, and employee burnout.

What's more? Document fraud can take many forms and can be perpetrated for various reasons. Below are some of the most common types of document fraud.

Counterfeit documents

Counterfeit documents are documents that are created to look like genuine documents but are not authorized by the issuing authority. For example, counterfeit passports may look like genuine passports, but they may also have subtle differences in design or typography.



Forged documents

Forged documents are documents that have been altered or modified without the knowledge or consent of the original document owner or issuer. For example, a forged check may have the original signature of the account holder, but the payee and amount have been changed.

Fake documents

Fake documents are documents that are created to deceive or mislead someone. They may be entirely fabricated or contain some truthful information mixed with false information. For example, a fake W-2 may have a person's real name but a false address.

The key to unlocking document fraud detection

Fraud prevention is truly a cat-and-mouse game. Because fraudsters are always evolving their techniques, the solution needed to fight fraud is deeply technical, requires using the most innovative models, and necessitates ongoing improvements to remain effective instead of once-and-done. Risk teams need technologies that specialize in racing fraudsters to the next vector of fraud detection.

Companies that continue to build large risk teams will fail to scale effectively and, even worse, subject themselves to compounding fraud and credit losses. The old world of building large manual review teams is over. The new world, enabled by machine learning, will allow risk teams to spend their time on what they are best at. The winners will embrace AI to make fast, fair, data-driven approval decisions that will ultimately benefit their customers and their bottom line.

At Inscribe, AI allows us to uncover trends in how fraudsters evolve their document manipulation techniques, and we believe that knowledge is power. This report is meant to empower banks, lenders, fintechs, and enterprise companies with AI-powered Risk Intelligence. With our second annual Document Fraud Report, we're sharing the top fraud risks revealed by our data because when fraud-fighting communities come together, we can outsmart fraudsters.

From first-party fraud to fraudulent templates (and fraud advice) that are readily available online, we've packaged up the most critical risks we think teams who fight fraud should be aware of in 2024, as well as some best practices for detecting it.

SNAPSHOT

Key 2024 fraud risks

A company's risk team has always been its primary asset in fighting fraud. But frontline fraud fighters must be enabled to continually evolve their methods in order to keep up with fraudsters. Here's a quick snapshot of the must-know risks for teams who fight fraud:

RISK #1

During tough economic times, fraud attempts increase due to financial hardship

- → 80% of risk leaders said they saw a YOY increase in fraud attempts.
- → 15% saw an increase in first-party fraud, while 13% saw an increase in third-party fraud.
- → Only 42% have a solution to help them detect fraud in the documents they rely on.

RISK #2

First-party fraud, a hidden fraud loss for many, continues to threaten lenders

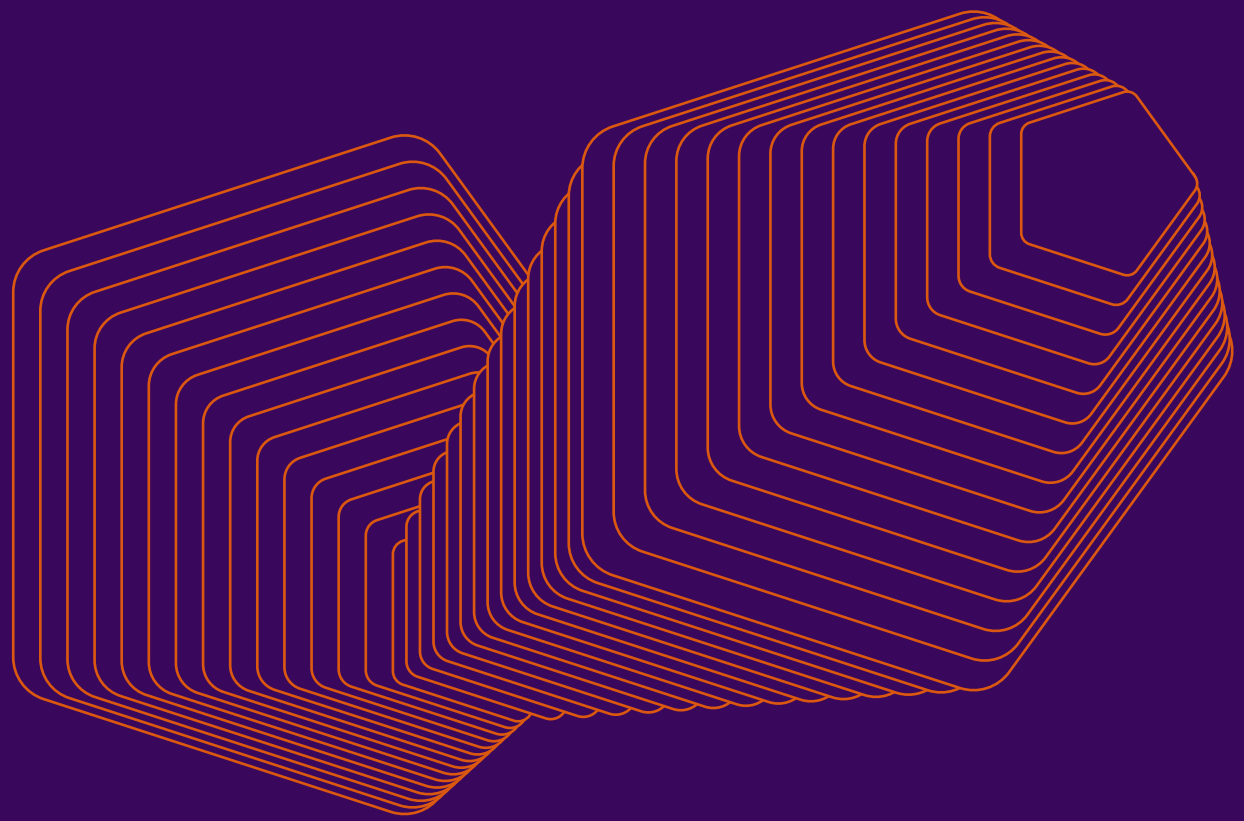
- → 94% of fraudulent application documents include alterations to financial details.
- → 60% of fraudulent personal loan applications include signs of first-party fraud – doubling YOY.
- → 46% of fraudulent SMB loan applications include signs of first-party fraud.

RISK #3

Fraudulent templates (and advice) are easier than ever to acquire through social media

- → The number of unique document templates detected has increased by nearly 20%.
- → What's more concerning are the types of templates detected: Fake bank statement templates detected increased by 69% and fake pay stub templates increased by a whopping 512%.

Risks you need to know in 2024



RISK #1

When the economy slows, fraud grows

Nearly 80% of risk leaders saw a YOY increase in fraud attempts.

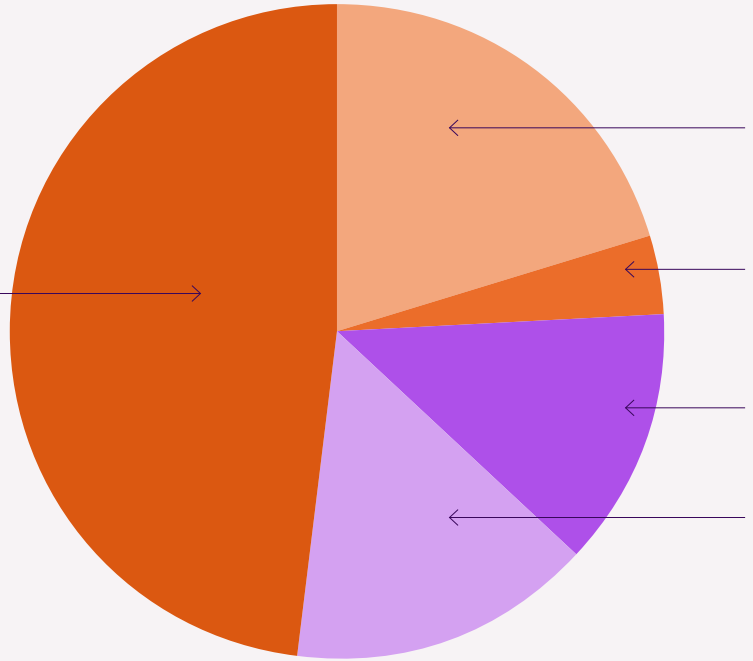
High interest rates, mounting credit card debt, and increasing loan delinquencies in the U.S. and worldwide clearly signal that many people are struggling to make ends meet. These trends matter because fraud thrives when economies suffer.

A study from the Association of Certified Fraud Examiners concluded that the 2008 economic crisis led to financial pressure, and subsequently, an increase in fraud. The same thing happened during COVID-19: Annual fraud complaints to the FBI increased 69% with total losses exceeding $4.2 billion. This trend is recurring.

01

In our recent state-of-the-industry survey, nearly 80% of risk and ops leaders said they saw a YOY increase in fraud attempts during 2023. More specifically, 15% saw an increase in first-party fraud, 13% in third-party fraud, and 48% in multiple fraud types.

Have you seen an increase in fraud attempts in 2023?



48%
Have seen an increase in multiple types of fraud

20%
Have not seen an increase in fraud attempts

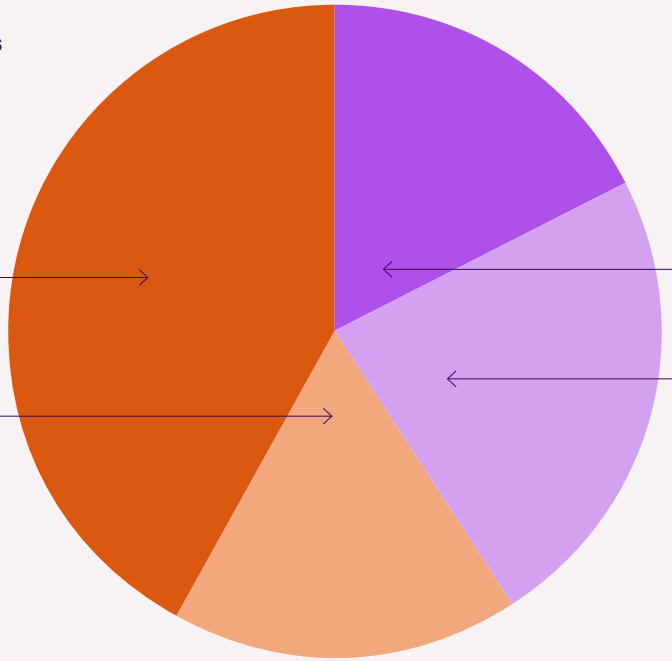
4%
Don't have a way to measure increases in fraud attempts

13%
Have seen an increase in third-party/ synthetic fraud

15%
Have seen an increase in first-party fraud

Surprisingly, only 42% of these companies have a solution to help them detect fraud in the documents they rely on to make decisions. 17% don't check documents for fraud at all, 24% review documents if something looks suspicious, and 17% review every document manually.

Do you check applicant documents (bank statements, pay stubs, tax forms, etc.) for signs of fraud or manipulation?



42%
Yes, with a document fraud detection solution

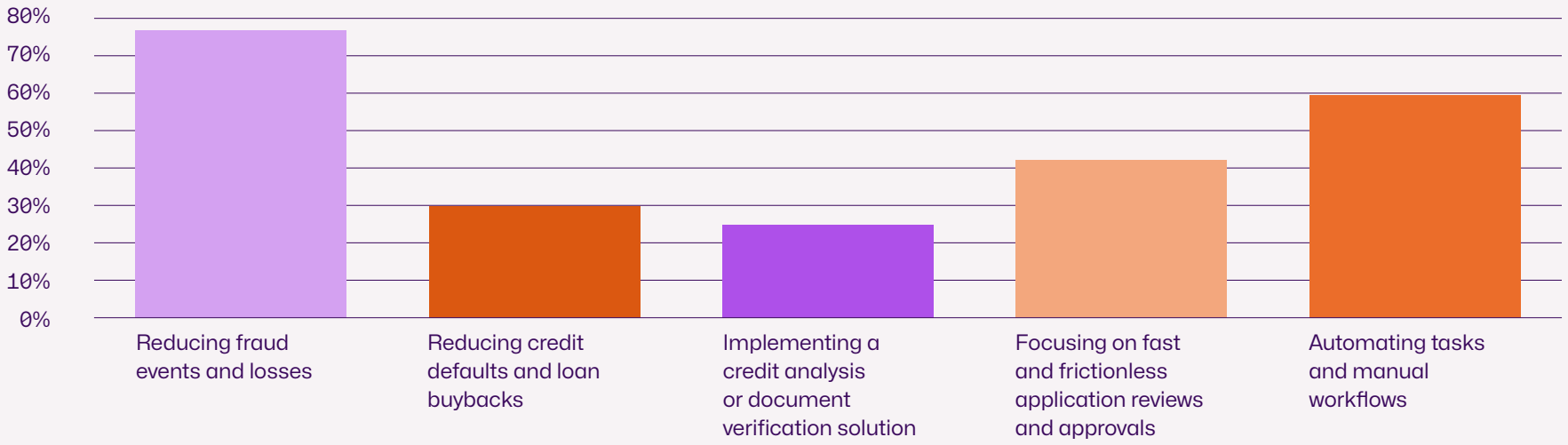
17%
Yes, we review every document manually

17%
No, we don't check documents for fraud

24%
We only review documents if something looks suspicious

So, how are risk leaders planning to address the problem of fraud? 77% said they plan to focus on reducing fraud events and losses this year, while 59% said they'll focus on automating tasks with manual workflows. These priorities were followed by focusing on fast and frictionless application reviews and approvals (42%), reducing credit defaults and loan buybacks (30%), and implementing a credit analysis or document verification solution (25%).

Which of the following initiatives are you planning to implement within the next 6–12 months?



Economic downturns can lead to significant shifts for businesses, such as changes in regulations, markets, or customer behavior. These changes can create new opportunities for fraudsters to exploit vulnerabilities in the system. In addition, companies tend to reduce their monitoring and supervision of potential fraud due to budget cuts or staff reductions. These lowered defenses provide an opportunity for bad actors to engage in fraudulent activities undetected.

Fraud detection is critical in any economic climate – but during times of economic uncertainty, it becomes table stakes for companies to remain vigilant and take proactive steps to protect themselves. The companies that do are not only able to protect their reputation and revenue, but they win the market by being an institution that customers trust.

How to fight document fraud

It's nearly impossible for a human reviewer to spot something that is one or two pixels off in any given document. But with Inscribe, risk teams know with certainty if a document is fraudulent and why, all within seconds. Inscribe provides a Fraud Rating for each customer, giving you an aggregated high- or low-risk score based on their application documents. Inscribe also highlights any fraud signals detected in the documents submitted so you can easily understand the severity of any alterations found. This helps you protect your organization from inflated loans or credit lines.

Some signals Inscribe uses to uncover document fraud

Suspicious software

Determines if Adobe Photoshop or other software was used.

Overlaid text

Indicates if text has been added over an image on a document.

Device fingerprinting

Surfaces repeat applications from the same source.

EXPERT SPOTLIGHT

Anurag Puranik

Head of Risk,
Coast

Adopt tricks and technology to spot fraud signals in seconds

Anurag Puranik, Head of Risk at Coast, points to some unconventional signals to detect fraud. In his experience, fraudsters generally don't use accounting software programs, such as QuickBooks, or leverage professional accounting services. They will simply set up different accounts and move money around to give the appearance of a real business. Even something as basic as having an accounting software transaction in a bank statement could be an important signal that a customer is legitimate and trustworthy. When used in context with

other review methods, this point can be used to help the company make a decision about the customer.

“You can’t identify signals manually because it would be too time-intensive,” he admitted. “But you can leverage vendor insights to manage these tasks and provide a quick view. For example, we use Inscribe for this, and it has been really valuable because it helps us reduce our review time to just one or two minutes per customer.”

Inscribe’s X-ray feature scans a document and identifies any areas where the file has been manipulated. It then enables a side-by-side comparison of the submitted version with the original so that teams can quickly assess where and how a file was changed.

“I love this X-ray feature,” Anurag said. “Before we used Inscribe, it would take our team half an hour to do a bank document review, but now it’s an extremely fast, automated process.”

See more tips from Anurag ↗

> **“You can’t identify fraud signals manually because it would be too time-intensive. But you can leverage vendor insights to manage these tasks and provide a quick view.”**
>
> Anurag Puranik

RISK #2

First-party fraud threatens lenders

60% of fraudulent personal loan applications include signs of first-party fraud — doubling YOY — while SMB holds firm at a concerning 46%.

In the financial services and lending industries, a fraudster's goal is to secure a loan for a big-ticket item, such as a car or mortgage. They will alter their documentation to inflate income, manipulate assets, or invent revenue streams in order to fraudulently qualify for a financial product.

02

That's why the signs of first-party fraud can usually be found in an applicant's documentation, such as pay stubs, bank statements, financial statements, or tax documents. Applicants knowingly alter their financial details, but not their identity, within these documents.

Types of fraud

First-party fraud
A fraudster uses their real identity, but falsifies financial details such as salary, bank account balance, or transaction categories.

Third-party fraud
A fraudster uses another person's (likely stolen) identity but may also falsify financial details to enhance their creditworthiness.

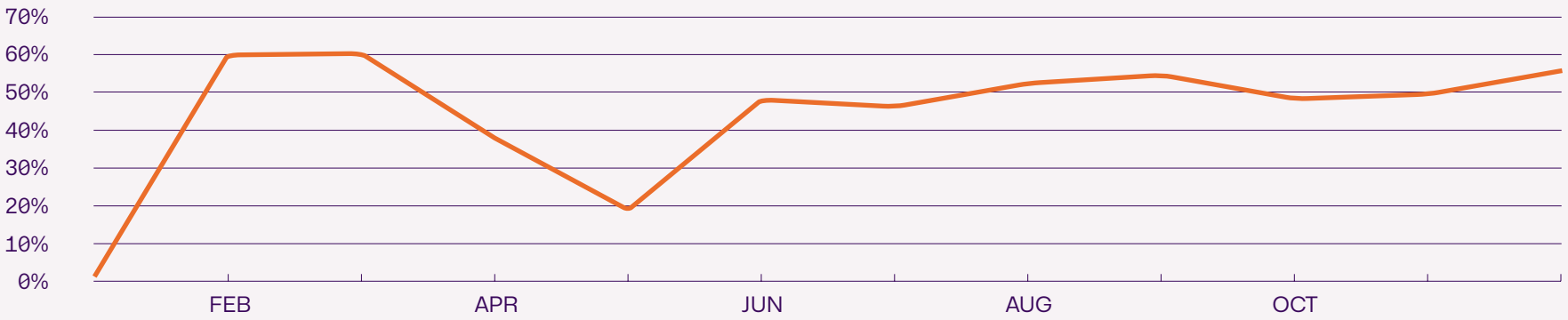
Synthetic identity fraud
A fraudster uses a fabricated identity (with entirely false details or piecemeal details from the identities of real people).

Detecting document fraud is critical for underwriters because there is often a direct link between falsified documentation and early payment default. First-party fraud has become a hidden fraud loss for many financial institutions because these credit losses are actually a consequence of document fraud during the application process.

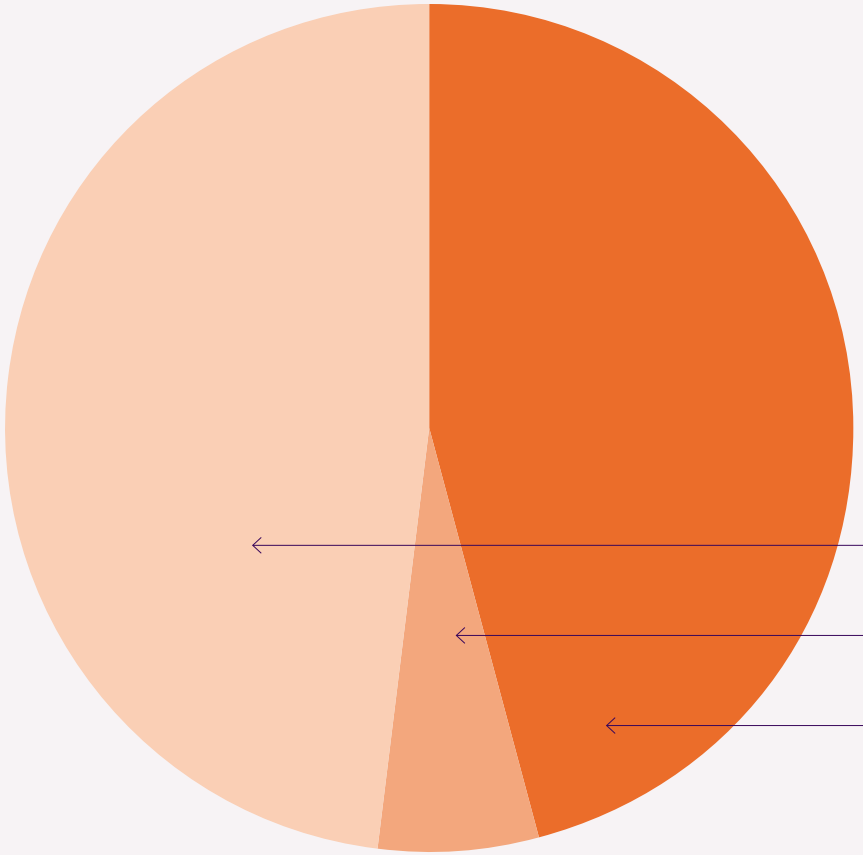
More and more, risk leaders have come to ask: Are fraudulent documents the source of many of my credit losses? Our data confirms their suspicions. 46% of fraudulent application documents don't include any alterations to identity details, meaning applicants are likely applying with their true identity. But those documents contain alterations to financial details such as income, bank balance, transaction amounts, and transaction descriptions (a sign of first-party fraud). And this problem is only getting worse – we saw a 4% increase in fraudulent documents with alterations to just financial details since last year.

Interestingly, we saw a rise in first-party fraud during the first part of 2023, a dip in May, and then an increase back to higher rates. A similar pattern was seen in 2022. This could be a signal that first-party fraud tends to peak during the first half of the year, potentially due to tax season or a desire to move to a new apartment or house.

Percentage of fraud docs in 2023 where financial details were edited, by month



What's even more interesting is that the percentage of fraudulent documents with only identity details edited is quite small (6%), while the largest group of fraudulent documents include alterations to both identity and financial details (48%).



Distribution of edited details in documents

48% Identity and financials edited

6% Only identity edited

46% Only financials edited

Here's the challenge for risk teams: While ID verification solutions can help mitigate third-party fraud (by identifying forged or counterfeit IDs), 94% of fraudulent documents include alterations to both identity and financial details. So, in 2024, income verification, in addition to name and address verification, is critical for protecting your company from fraud and credit losses.

When we look at first-party fraud risks by industry, other concerning trends emerge:

Consumer underwriting

60% of fraudulent personal loan application documents match the pattern of first-party fraud rather than third-party fraud – and this has doubled since last year. These individuals are inflating their salaries or hiding evidence of bad spending habits. They present a much higher risk of delinquency.

Business underwriting

46% of fraudulent SMB loan application documents match the pattern of first-party fraud rather than third-party fraud. This means SMB lending businesses are approving customers who may attempt repayment, but have a significantly elevated risk of delinquency.

How to fight first-party fraud

Detecting and preventing first-party fraud may be a notoriously difficult task, but not impossible. With the right strategy, tools, and partners, your organization can be on its way to reducing risk in a significant way. Our Risk Intelligence platform identifies where each piece of information is on a digital, scanned, or photographed bank statement (name and address of the document owner, balance information, document dates, full transaction history for the statement period, etc.). That means Inscribe can not only tell you if an alteration has been made, but also whether the alterations were made to the applicant's identity, finances, or both. This creates a safeguard to ensure your applicants are legitimate and eligible.

Some signals Inscribe uses to detect first-party fraud

Amount format anomaly

Determines if anomalous formatting is associated with amounts, including balances and transactions on bank statements and pay stubs.

X-ray

Shows the differences between the document submitted and the document recovered so you can see exactly how it was altered.

Transaction data

Surfaces risky transactions, including self-transfers used to inflate balances, absence of typical business spend, and large deposits.

EXPERT SPOTLIGHT

Frank McKenna

Co-founder of PointPredictive and
Author of Frank on Fraud

Mitigating the risk of first-party fraud sometimes requires a culture change within your organization

"Nobody wants to believe that your actual customers can be committing fraud against you," said Frank McKenna, co-founder of PointPredictive and Author of Frank on Fraud. "It's very difficult to get an organization to accept that it happens and then to invest in tools and technology to stop it."

"99% of companies don't have any understanding of how big first-party fraud is," he continues. "They tend not to invest in the problem because they don't differentiate those losses. However, we know that if companies define the problem, identify the scope, and then use a targeted anti-fraud technique to combat those cases, those credit losses can be averted. And the reward for doing so is large."

Frank recommends companies conduct an assessment to calculate the specific cost of first-party fraud. The company could then assign that dollar amount to risk mitigation tools and technologies. Over time, this investment will be offset by the avoided losses, as well as efficiency gains through automation.

Get more advice from Frank ↗

"We know that if companies use a targeted anti-fraud technique to combat first-party fraud, those credit losses can be averted and the reward for doing so is large."

Frank McKenna

RISK #3

Fraudulent templates (and fraud advice) are rampant

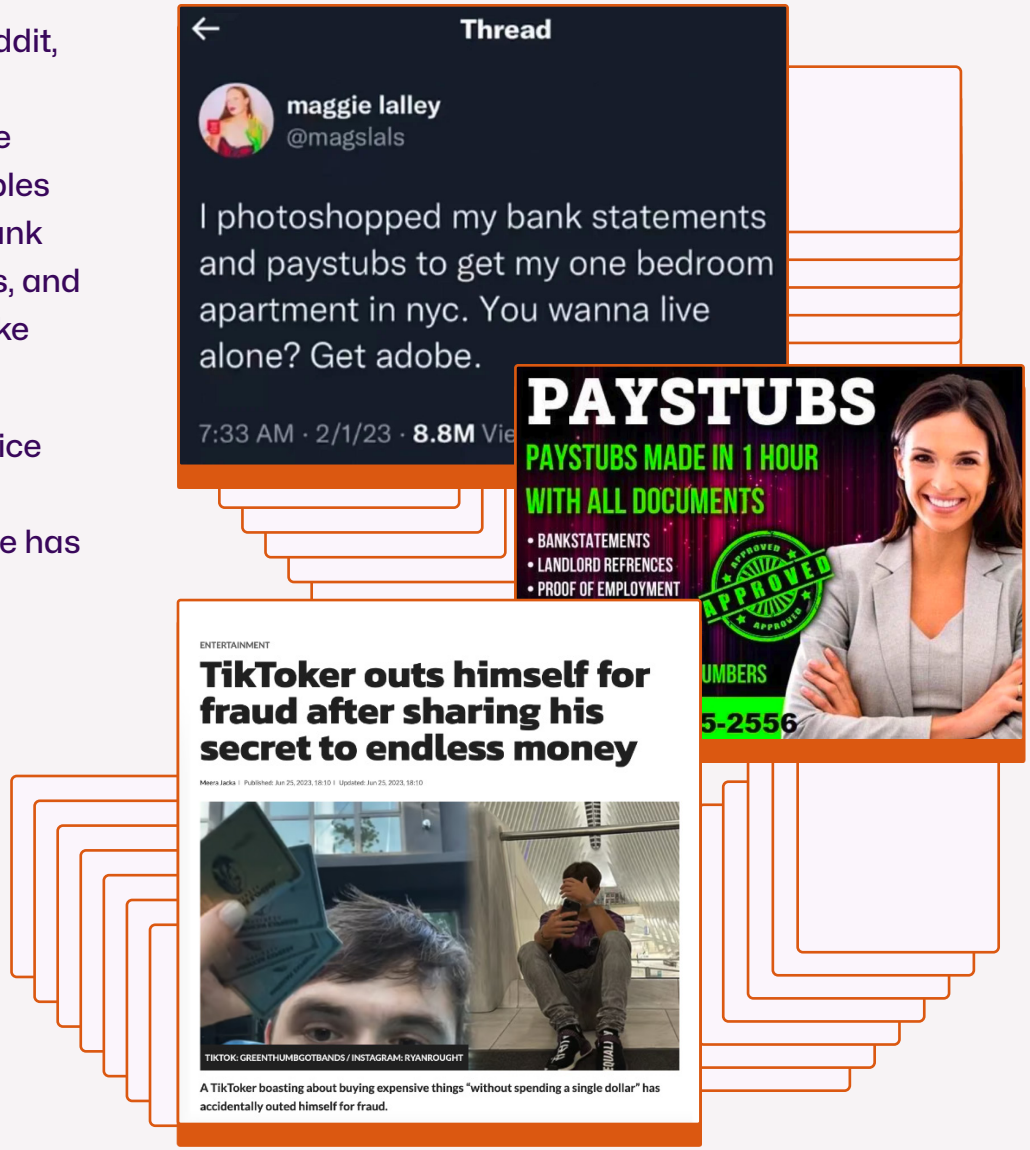
Bank statement templates detected increased by 69%, while pay stub templates detected increased by a whopping 512%.

Document templates (legitimate-looking documents that are sold and purchased online) have become an increasingly popular tool for fraudsters. A quick Google search for a fake W-2, fake utility bill, or fake Bank of America statement will generate thousands of results. You can even find fake bank statement generators and websites that sell “novelty” financial documents.

03

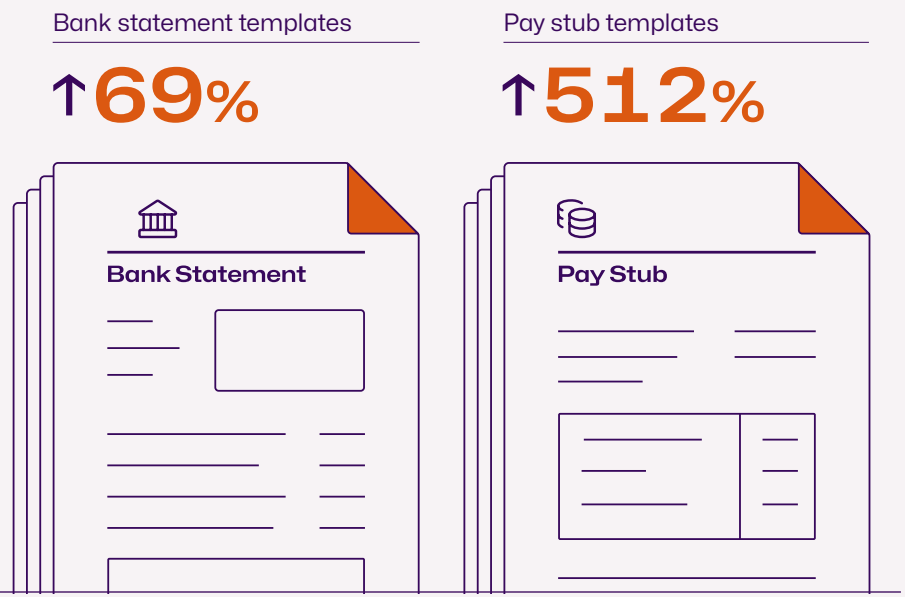
But that's not all: Social media platforms like Reddit, Telegram, and TikTok have made it easier for fraudsters to sell document templates and share forgery techniques. We've seen countless examples where consumers are asking how to edit their bank statements when applying for loans, credit cards, and housing. We've even seen fraudsters offer to make fraudulent edits for a small fee.

This almost effortless access to fraud-as-a-service makes it easy to understand how the number of unique document templates detected by Inscribe has increased by nearly 20% since last year.



What's more concerning is the types of templates that Inscribe detected in 2023. In 2022, the vast majority of the templates we detected were proof of address documents, like utility bills. However, in 2023, we saw an alarming shift in the types of templates detected: Bank statement templates detected increased by 69% and pay stub templates detected increased by 512%.

These templates are likely used to falsely demonstrate employment or inflate income. The danger here is that this fraud is almost impossible to spot with just the human eye and, as we mentioned before, and it's easily accessible to bad actors. While a less sophisticated fraudster may use Microsoft Paint to change the name on a utility bill or to add an extra $10,000 to a bank balance, these document templates are designed so that they are easily editable and almost indistinguishable from originals, using all the correct fonts and alignments.



Change in template types detected by Inscribe in 2023

How to fight document template fraud

A manual reviewer may not be able to recognize that the bank statement they are looking at today has the same 100 transactions with the same dates, same descriptions, and same amounts as another bank statement they looked at six months ago, but a computer can. Machine learning models reap the benefits of network effects – the more data they ingest, the smarter they get, and they can remember millions of data points. Because Inscribe has utilized the most sophisticated technology since our inception, we can deliver the safest and most usable AI solution for financial services to protect you from increasingly sophisticated fraudsters.

Some signals Inscribe uses to uncover document templates

Fingerprint

Indicates if a document deviates from the expected characteristics of the bank Inscribe identified on the document.

Name & address format anomaly

Finds outlier discrepancies between the name and address in the submitted document and similar documents.

Copycat image

Compares the document submitted to identical documents in our database that have a different identity associated.

EXPERT SPOTLIGHT

Rohan Sriram

Product Manager,
Plaid

Network effects can help you catch more fraud, faster

Because Inscribe has the largest database of fraudulent documents, we're able to use the power of network effects to identify fraud that's occurring at multiple institutions and proactively protect the rest of our customer base from that fraudster.

Rohan Sriram, Product Manager at Plaid, further explains the benefits of network effects: "At Plaid, our customers also get the benefit of network effects because one in three Americans have connected a bank account through Plaid. We have relationships

with many financial institutions and we also power thousands of fintech apps. So this enables us to see trends across our entire network – and that's a very powerful thing to think about, especially when it comes to things like fraud where a lot of times you're blind because a lot of the data is in silos."

"So for example, fraudsters typically attempt the same fraud on multiple companies at the same time. So, if you see a particular device for the first time, you don't really know if it's fraudulent," he continued. "But when you work with a vendor that has a large network like Inscribe or Plaid, you can see fraudulent behavior across multiple customers to identify bad actors. I think that's where the network effect gets really powerful."

Hear more from Rohan ↗

"When you work with a vendor that has a large network like Inscribe or Plaid, you can see fraudulent behavior across multiple customers to identify bad actors."

Rohan Sriram

RISK #4

When it comes to fraud, expect the unexpected

Fraud attempts are constantly evolving — risk teams must band together and learn from one another.

Fraudsters are always evolving their techniques. When one approach doesn't work, they try another. One reason why fraudsters have become more effective in recent years is because they're working together – sharing tips, techniques, and information (see Risk #3).

That's why industry collaboration is so important. Risk teams should assume the same collaborative mindset to fight fraud effectively, banding together, learning from each other's experiences, and sharing best practices. In doing so, it becomes more difficult for fraudsters to launch the same attack across multiple targets successfully.

04

In the spirit of collaboration, we've compiled the top fraudulent document types, high-risk fraud signals detected, and days of the week with the most fraud attempts we saw in 2023. While this information doesn't mean you shouldn't accept certain document types or documents submitted on certain days, it may help you think about fraud trends to investigate within your own company.

TOP 5 FRAUDULENT DOCUMENT TYPES

Watch those tax forms

There are many document types detected by Inscribe, but these make the list for having the most cases of fraudulent alterations or templates caught.

1. Tax forms
2. Utility bills
3. Pay stubs
4. Bank statements
5. Business filings

TOP 5 HIGH-RISK FRAUD SIGNALS

Beware of software used

Inscribe uses document forensics and network-based detectors to uncover fraud, and these are the most common high-risk fraud signals detected.

1. Suspicious software
2. Edited text
3. Inconsistent fonts
4. Document anomalies
5. X-ray

TOP 5 DAYS WITH THE MOST FRAUD ATTEMPTS

Keep an eye on Wednesdays

While companies experience document fraud every day, the middle of the week has higher fraud rates – a signal that fraudsters are trying to blend in.

1. Wednesday
2. Tuesday
3. Thursday
4. Monday
5. Friday

How to fight document fraud — together

There are several fraud-fighting communities and resources available to help you learn from others in similar roles. We've compiled a few that fraud, risk, and ops leaders have shared with us.

Some helpful fraud-fighting communities fraud

Frank on Fraud blog
frankonfraud.com ↗

About Fraud
about-fraud.com ↗

ACFE
acfe.com and fraudweek.com ↗

Fraud Lab
fraudlab.com ↗

Financial Services Information Sharing & Analysis Center
fsisac.com ↗

EXPERT SPOTLIGHT

Rajat Bhatia

Sr. Director & Head of Risk Management,
Navan

Keep evolving to stay ahead of fraudsters

Rajat Bhatia, Sr. Director & Head of Risk Management at Navan, was looking for a solution that his team could use to check documents for fraud.

Out of all the solutions he reviewed, Inscribe was the only one they would be able to use right out of the box. That meant they could get started right away using Inscribe's web app while they waited for their engineering team to integrate the API.

"We had a team of risk management and operations people who needed to be able to screen customer

documents immediately," Rajat said. "And Inscribe gave us the flexibility to do that. Because we were able to use the web app for those customer documents, Inscribe was able to help us prevent fraud on day one."

Now, Rajat's team uses Inscribe as part of the KYC and KYB process to ensure that prospects coming through the door are valid business entities. If a customer is deemed legitimate during the onboarding process, then the underwriting team begins reviewing documents to assess credit risk. If a bank statement wasn't collected during onboarding, they'll ask for one during the underwriting process and use Inscribe to verify the document's authenticity.

"Everyone in the industry needs to keep evolving because the adversary – the people trying to commit fraud – are smarter, better resourced, and more creative than we can even imagine," he said.

Read Rajat's full story ↗

"Everyone in the industry needs to keep evolving because the adversaries are smarter, better resourced, and more creative than we can even imagine."

Rajat Bhatia

ABOUT INSCRIBE

AI-powered Risk Intelligence for fraud, credit, and compliance

Instead of relying on tedious, subjective, and error-prone manual document reviews, teams that use Inscribe's AI-powered Risk Intelligence platform are equipped with instant access to fraud and credit intelligence that eliminates uncertainty and makes risk decisions easier. And because Inscribe created the document fraud detection category using AI and machine learning almost a decade ago, we have the best-performing models in the industry, so you can count on us to detect fraud in documents that other solutions simply can't.

99% precision rate
to reliably catch fraud and credit abuse

150%+ ROI
in the first 3–6 months

30 minutes
saved on manual document review per application

30 seconds
to return document results and enable a decision

PLAID · NAVAN · VIVA FINANCE · gigwage · Lendflow · Petal · coast · MERCARI · bluevine · ramp

Want to learn more?

Speak with an expert from our team to see how you can minimize risk and maximize efficiency.

Get Started ↗

inscribe