2023

DOCUMENT FRAUD REPORT

MUST-KNOW TRENDS FOR TEAMS WHO FIGHT FRAUD

inscribe

Fraud Fact

Less than 10% of document fraud is visible to the human eye.

The enduring role of documents in fraud prevention

Frank Abagnale, famously portrayed by Leonardo DiCaprio in "Catch Me if You Can," counterfeited checks. Bernie Madoff forged financial statements and accounting records. The fake German heiress Anna Sorokin (also known as Anna Devley) said it took "surprisingly little time" to produce counterfeit bank statements, which were never questioned.

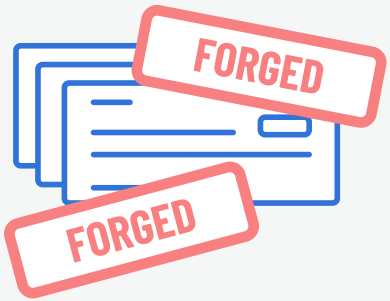
Document fraud has been around for centuries, and the methods used to create fraudulent documents have become more sophisticated over time. It's easy to accomplish, but hard to catch, because so much of it is hidden in the metadata, embedded text, and file history — details that are invisible to the human eye.

Types of fraudulent documents

Document fraud can take many forms, and can be perpetrated for a variety of reasons. Some of the most common types of document fraud include:

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

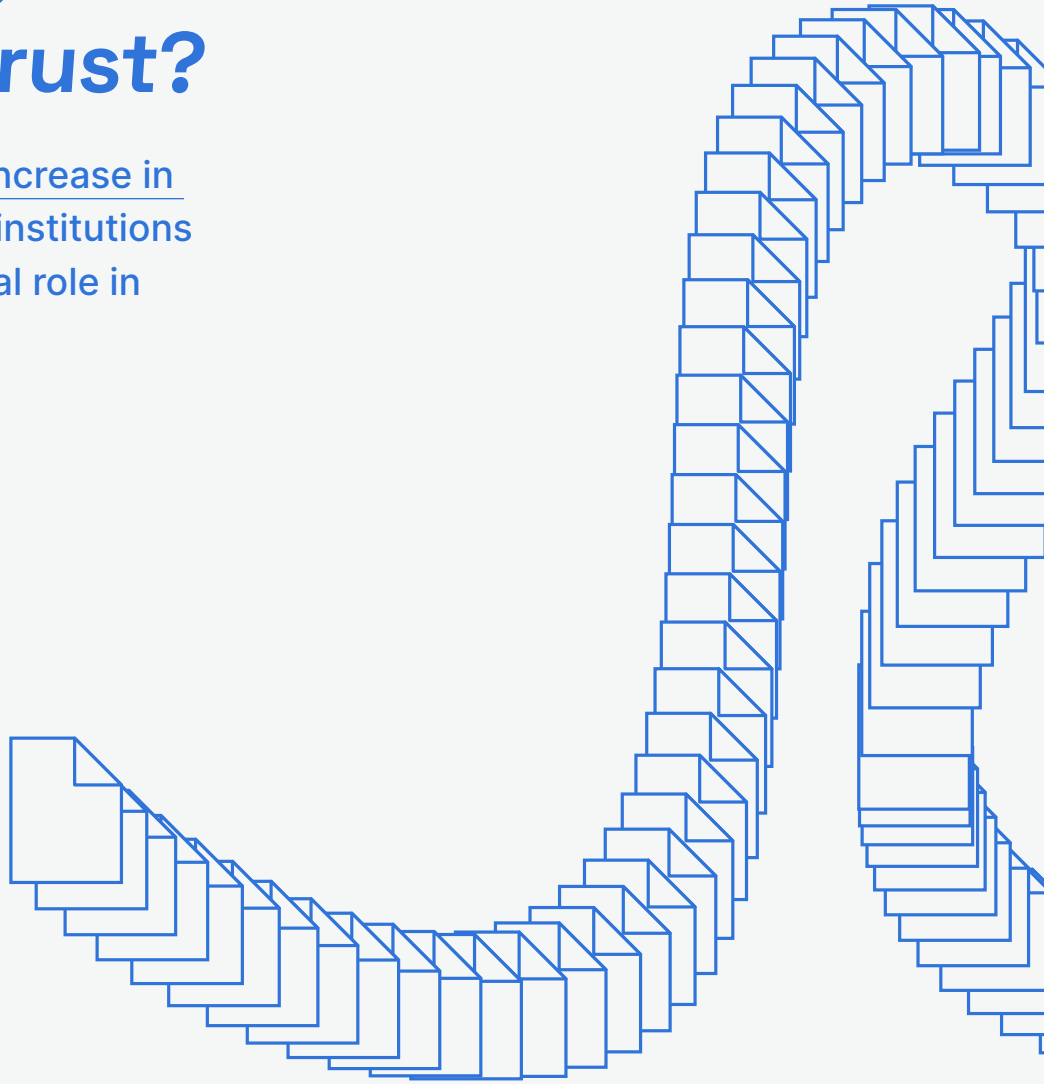
Fake documents are documents that are created to deceive or mislead someone. They may be entirely fabricated or contain some truthful information mixed with false information. For example, a fake W-2 may have a person's real name, but a false address.

Why are documents so effective for building trust?

In 2022, financial services companies saw a 79% increase in document fraud. So why do fintechs and financial institutions still accept documents? Because they play a pivotal role in building 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 based on trustworthiness (Is the customer who they say they are?) and creditworthiness (Can the customer afford this financial product?)

Documents enable you to verify someone's identity, their proof of address, borrowing power, and more by showing you that the information has been verified by another reputable institution (a bank, utility provider, government, etc.). They create borrower transparency, and as a result, trust.



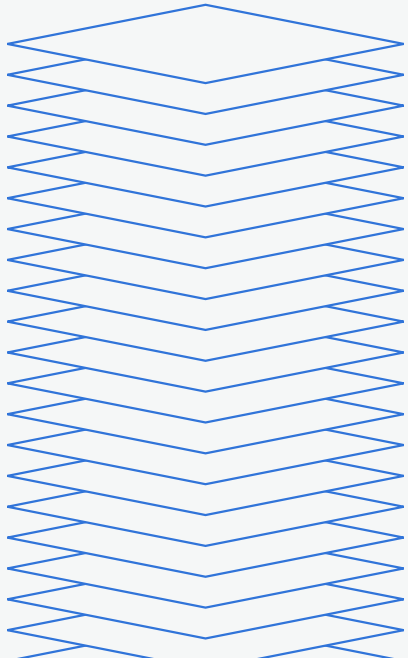
But fake documents that can be purchased online and sophisticated image-editing software like Adobe Photoshop make document fraud almost impossible to detect. And relying on manual reviews can cost your company a lot: Because investigators can't see what's been altered in a document — or if it looks exactly the same as a template they reviewed two months ago — it increases the risk of human error and takes a toll on your team.

With the power of AI and machine learning, however, you can arm your team with the ability to uncover a document's paper trail ... or rather, its file history. True PDFs are digitally native documents (like bank statements, utility bills, or W-2s) downloaded directly from certified institutions. Each document has metadata that can tell you who created it, when it was created or modified, and what software was used to create it. True PDF documents also have embedded text, which provides information such as font style, space, coloring, and placement.

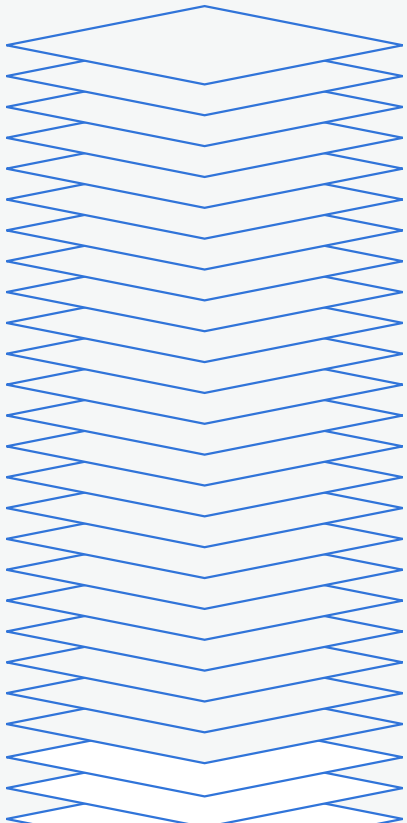
At Inscribe, we've combined the heuristics used by manual review teams with the power of artificial intelligence in order to analyze billions of document data points with a high degree of accuracy — making the invisible, visible.

Inscribe will not only tell you if there's suspicious evidence in the metadata, but you can use our X-ray feature to compare what the document looked like before it was tampered with. You'll see things like the original name, date, address, and bank balance of a document before a fraudulent manipulation. Our proprietary "fingerprint"

WITH THE POWER OF AI AND MACHINE LEARNING, YOU CAN UNCOVER A DOCUMENT'S PAPER TRAIL ... OR RATHER, ITS FILE HISTORY.



WHEN WE'RE ARMED WITH KNOWLEDGE, WE CAN OUTSMART FRAUDSTERS.



detector quickly compares the embedded text in a document provided by an applicant with what the embedded text should look like in a True PDF from specific banks and other institutions.

All of this makes it possible for us to uncover trends in how fraudsters are evolving their document manipulation techniques.

We believe that knowledge is power. So we're embarking on an initiative to empower the fintech and financial services industry with Risk Intelligence by regularly surfacing the fraud trends revealed by our data.

Because when we're armed with knowledge, we can outsmart fraudsters.

From first-party fraud to fake documents that can be purchased online, we've packaged up the most important trends we think teams who fight fraud should be aware of in 2023 (as well as some best practices for detecting it).

Document fraud trends to know for 2023

Fraud fact

There were 27% more fraud incidents on business bank statements than personal bank statements in 2022.

TREND 1

First-party fraud is often behind credit losses

For many companies in the financial services industry, credit losses are a fact of life.

Typically, they are presumed to be a result of honest customers who intended to pay back a loan in full, but for one reason or another, simply weren't able to. Fraud losses, on the other hand, are immediately associated with someone who has applied for a loan under false pretenses (typically a manipulated or fabricated identity as part of a third-party fraud scheme) with no intention to ever pay.

Much attention has been paid to the rise of third-party and identity fraud since 2020, and understandably so: Synthetic identity fraud (a type of third-party fraud) resulted in $20 billion in losses for U.S. financial institutions in 2020, and large companies like PayPal have since discovered millions of illegitimate accounts within their customer base.

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 identity, but may also falsify financial details to enhance their creditworthiness

Synthetic identity fraud

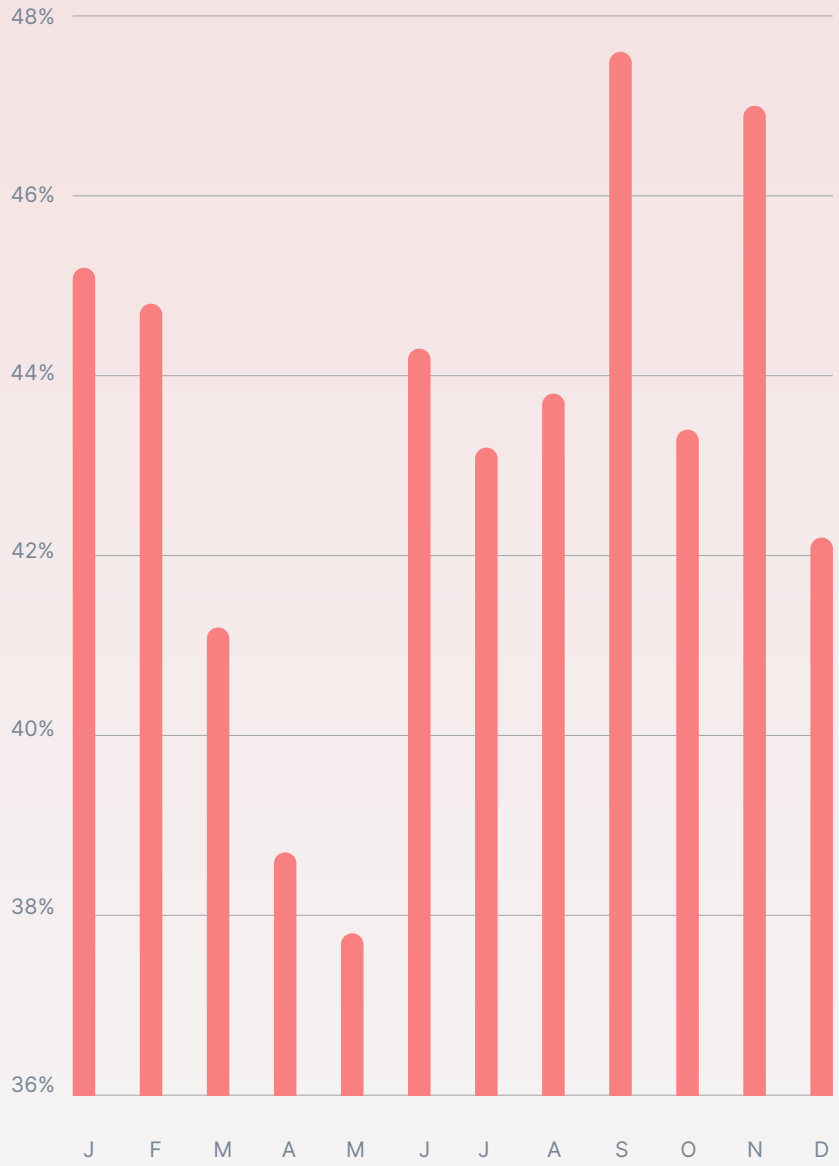
A fraudster uses a fabricated identity (with entirely false details or piecemealed details from the identities of real people)

But lately, many of our customers have had hunches about their credit losses being due to first-party fraud (where someone applies under their real identity, but falsifies information like income or cash flow, to gain access to a larger amount of funds). Most organizations simply don't have the data to prove it.

After processing millions of loan applications, our data confirms their suspicions: A significant proportion of credit loss can be traced to fraud during the application process — meaning that first-party fraud is more rampant than previously thought.

According to the 2023 Identity Fraud Report, more than half (51%) of all incidents in financial services fraud were categorized as identity fraud — meaning false identity details were used by fraudsters.

Our data at Inscribe supports this analysis: On average, slightly less than half (around 42%) of the fraudulent documents we detect do not include altered identity details. Instead, they contain alterations to financial details such as income, bank balance, transaction amounts, transaction descriptions, etc.



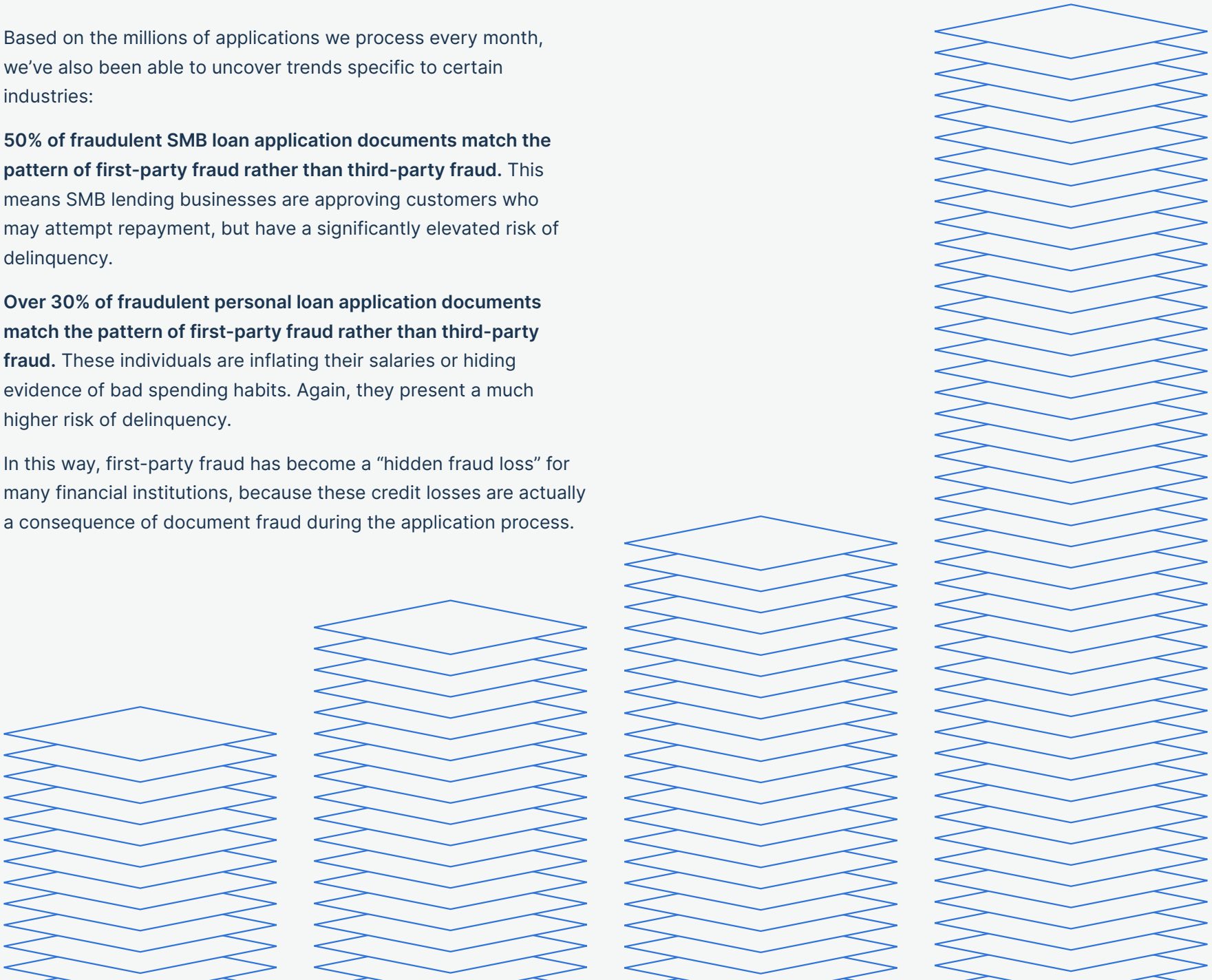
Percent of fraudulent documents in 2022 where the identity was not edited

Based on the millions of applications we process every month, we've also been able to uncover trends specific to certain industries:

50% 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.

Over 30% of fraudulent personal loan application documents match the pattern of first-party fraud rather than third-party fraud. These individuals are inflating their salaries or hiding evidence of bad spending habits. Again, they present a much higher risk of delinquency.

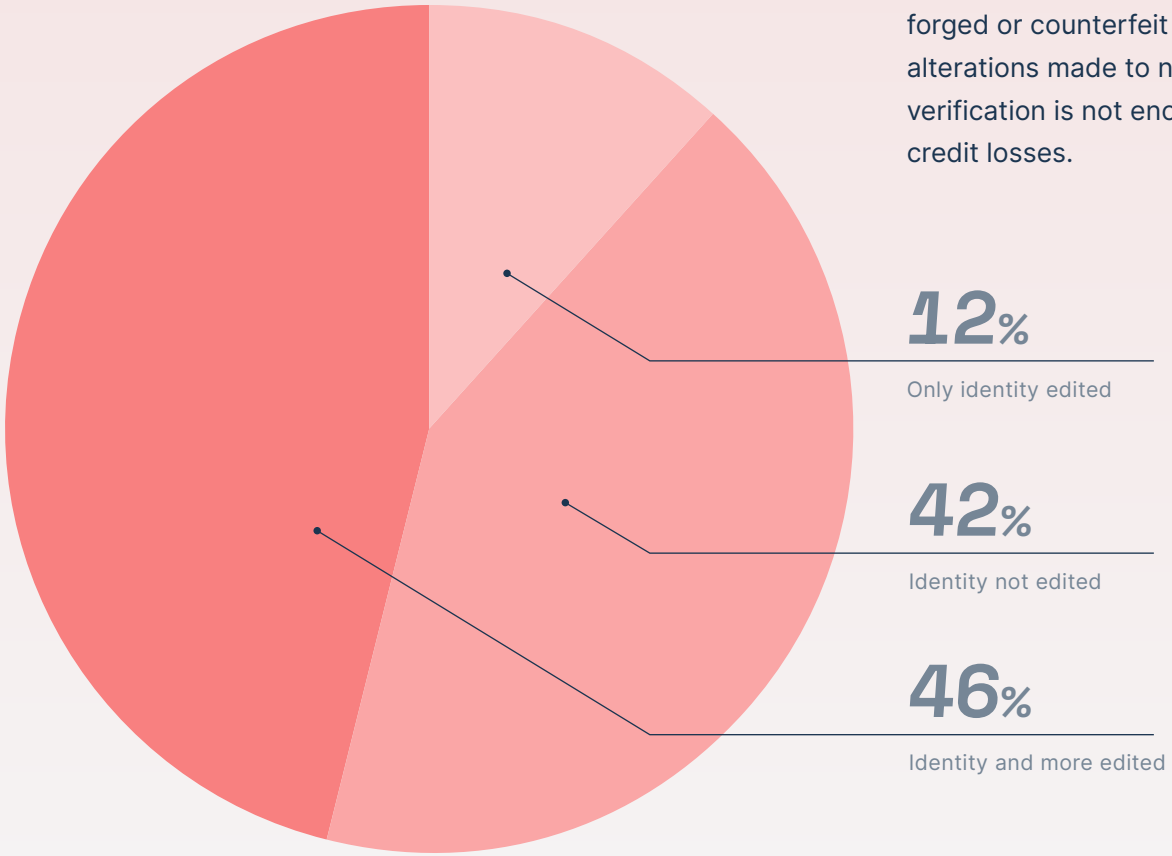
In this way, first-party fraud has become a "hidden fraud loss" for many financial institutions, because these credit losses are actually a consequence of document fraud during the application process.



What's even more interesting is that the percentage of fraudulent documents with only identity details edited is quite small (around 12%). And the largest group of fraudulent documents are ones where both identity details and financial details were falsified.

Here's the challenge for fraud and risk teams: While ID verification solutions can help mitigate third-party fraud (by identifying forged or counterfeit IDs), 88% of fraudulent documents include alterations made to non-identity details. So in 2023, identity verification is not enough to protect your company from fraud and credit losses.

Distribution of documents with edited identity details



How to fight this fraud

The first step in mitigating these credit losses is not to force additional income requirements onto your applicants — as that may result in you rejecting worthy customers or preventing underserved communities from accessing finances — but rather confirm that your existing requirements are actually being met today.

In the past, first-party fraud was notoriously difficult to detect. But Inscribe is able to identify 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 our software 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.

Tools Inscribe uses to uncover first-party fraud

Parsing
Extracts and returns key document details in just seconds.

Verification
Checks that identity details in the document match what an applicant provides.

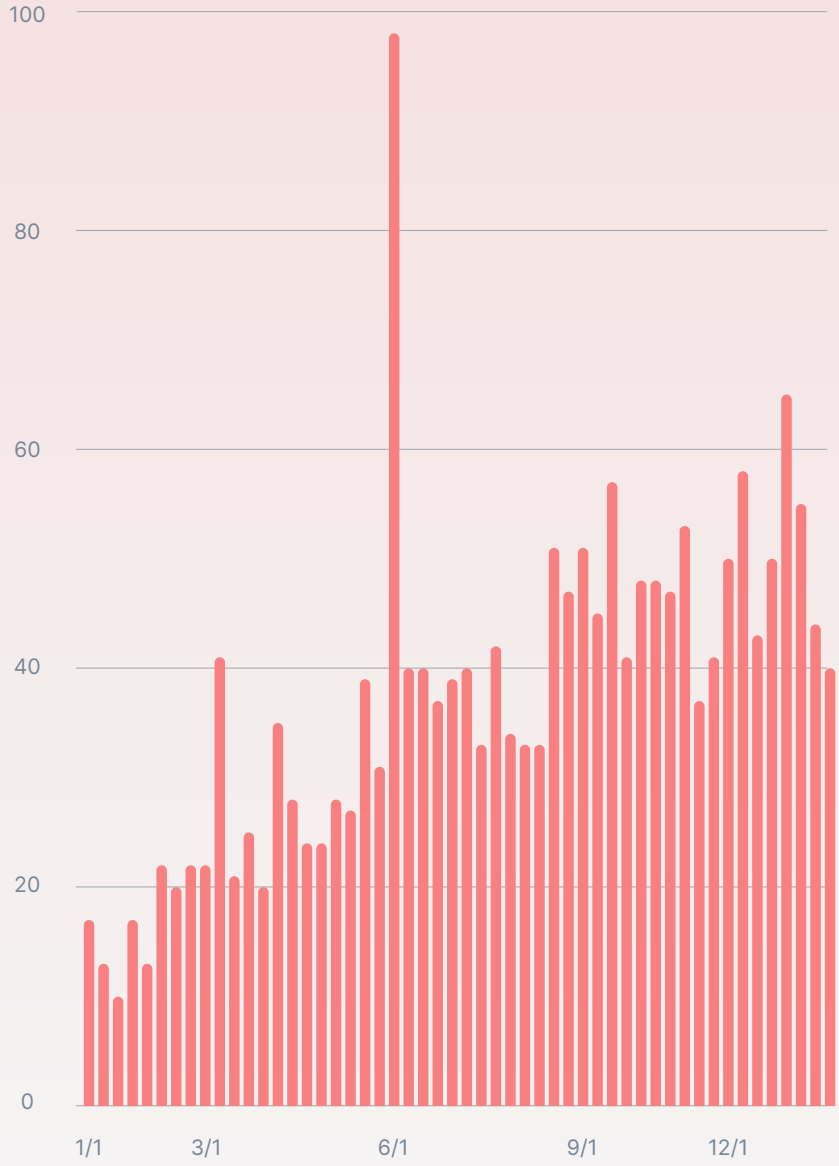
Detection
Uncovers if details in a document have been altered and how.

TREND 2

Fraudulent documents are easier than ever to acquire

Document templates (counterfeit, fake, or forged documents that are 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.

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. This almost effortless access to fraud-as-a-service makes it easy to understand how the number of document templates detected by Inscribe tripled in 2022.



The chart on the left shows a month-by-month analysis not of the volume of document templates, but rather the number of different, distinct document templates Inscribe detected — meaning that in the summer of 2022, there was a week where we flagged almost 100 different unique templates that were being used by multiple customers across numerous documents.

The danger here is that this fraud is almost impossible to spot with just the human eye and, as we mentioned before, 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.

Unique document templates flagged by Inscribe in 2022

How to fight this fraud

Machine learning models are able to reap the benefits of network effects — the more data they ingest, the smarter they get. And they can remember millions of data points. 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 transaction descriptions, same transaction amounts as another bank statement they looked at six months ago. But a computer can.

What's the risk of detecting document fraud with AI? Using models that aren't sophisticated enough or don't have enough data points to decide in seconds.

At Inscribe, fraud detection is in our DNA. We're helping teams who fight fraud by processing millions of documents each month — meaning we have the industry's most innovative fraud models (trained on hundreds of millions of data points from a wide range of document types) and they keep evolving.

Detectors Inscribe uses to flag document templates

Fingerprint
Indicates if a document deviates from a typical bank statement.

Anomaly detection
Finds outlier discrepancies between the document and similar documents.

Copycat
Compares the submitted document against our database of documents.

TREND #3

The most common fraudulent documents

When we started looking at the types of documents with the highest fraud rates in 2022, we expected to see small regional banks or credit unions topping the list; our hypothesis was that it would be easier for instances of fraud to get by undetected because investigators would not be as familiar with those documents.

But when we ran our analysis, the highest fraud rates were found in very common documents from well-known institutions: tax forms (W-2s and CP-575s) and bank statements from Bank of America, Wells Fargo, TD Bank, and others. Interestingly, our data also found the most common days of the week for fraudulent documents to be submitted.

Keep reading to learn about the most common fraudulent document categories, types, and days of the week.

TOP FRAUDULENT
DOCUMENT CATEGORIES

Watch those utility bills

There are many document categories, but these nine make the list for having the most cases of fraudulent documents.

- Utility Bill
- Tax Form
- Business Filing
- Bank Statement
- Invoice
- Social Security Card
- Pay Stub
- Driver's License
- Check

TOP FRAUDULENT
DOCUMENT TYPES

Get a clue about W-2s

Within each document category are different types of documents. Here are the nine with the most instances of fraud.

- W-2
- CP-575
- Navy Federal Credit Union
- Bank of America
- Wells Fargo
- TD Bank
- PNC Bank
- Chase Bank
- U.S. Bank

TOP FRAUDULENT
DOCUMENT DAYS

Don't sleep in on Sundays

While it's true that companies experience document fraud every day, Sunday sees the most activity. Here's the breakdown for the rest of the week.

1 Sunday
2 Saturday
3 Monday
4 Wednesday
5 Friday
6 Thursday
7 Tuesday

How to fight this fraud

Document fraud is in the details. While this information doesn't mean you shouldn't accept W-2s, certain bank statements, or documents submitted on Sundays, it does mean that they're more likely to be manipulated by fraudsters — so if you see something suspicious, give those documents a closer look in 2023.

It's hard for humans to spot something that is one or two pixels off. But with a document fraud detection solution like Inscribe, you'll know with certainty if a document is fraudulent and why, all within seconds. Inscribe returns a trust score of 0–100 based on the severity of fraud results and will highlight any fraudulent activity found, so you can protect your organization from inflated loans or credit lines.

If you want to investigate exactly what details have been altered, Inscribe's web app makes it easy to see the differences between the document provided and the document recovered. You can also see what's been uncovered in the metadata, including any software used to make edits to pay stubs or bank statements.

Document forensics Inscribe uses to detect fraud

X-ray
Shows the previous version of a document if it exists.

Software used
Determines if Adobe Photoshop or other software was used on the document.

Inconsistent fonts
Indicates if more than one font was used in a word.

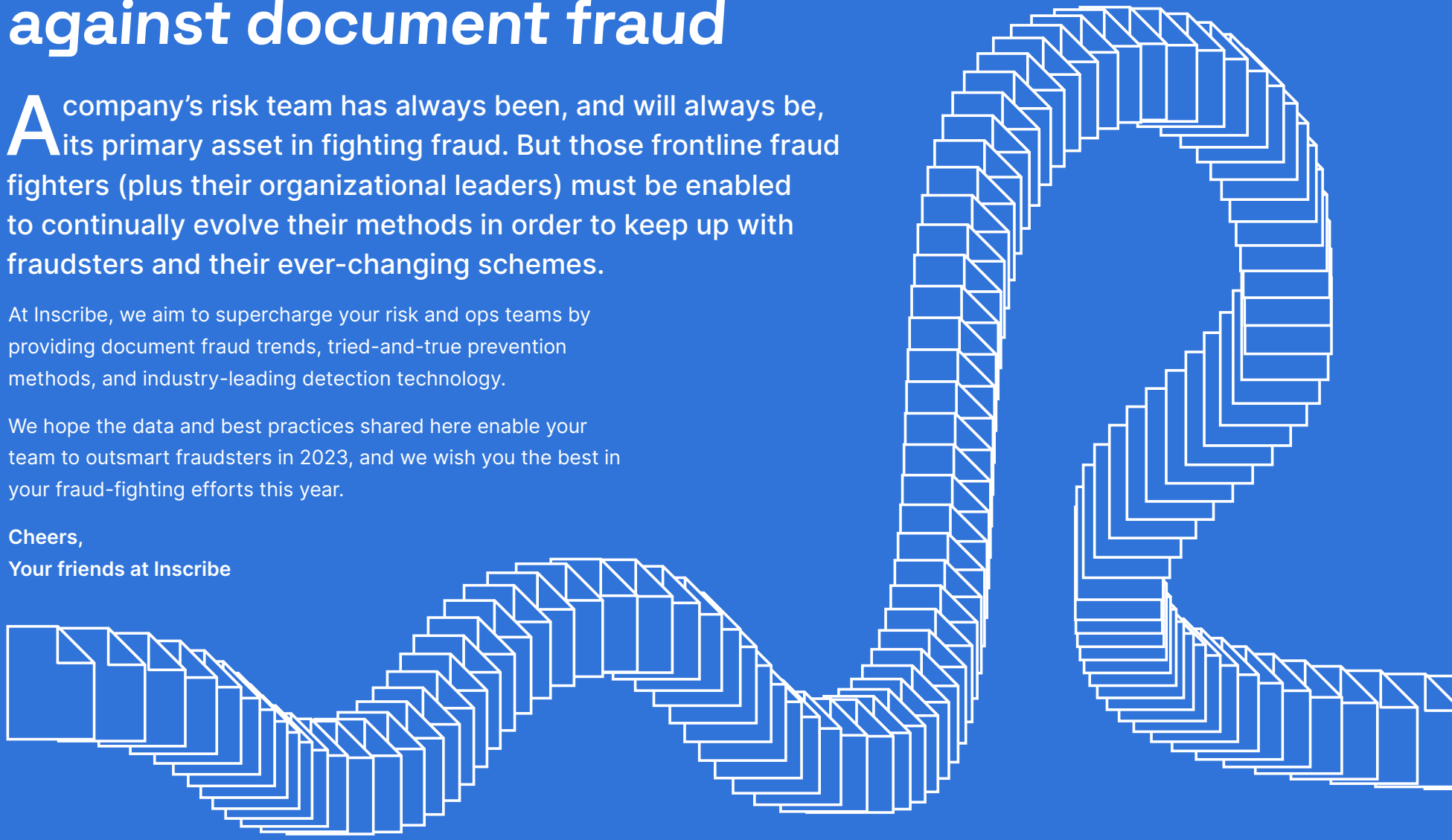
Arming your team in the fight against document fraud

A company's risk team has always been, and will always be, its primary asset in fighting fraud. But those frontline fraud fighters (plus their organizational leaders) must be enabled to continually evolve their methods in order to keep up with fraudsters and their ever-changing schemes.

At Inscribe, we aim to supercharge your risk and ops teams by providing document fraud trends, tried-and-true prevention methods, and industry-leading detection technology.

We hope the data and best practices shared here enable your team to outsmart fraudsters in 2023, and we wish you the best in your fraud-fighting efforts this year.

Cheers,
Your friends at Inscribe



ABOUT INSCRIBE

We help companies fight document fraud with AI

Fraud tactics are constantly evolving, but Inscribe stays ahead by using the most sophisticated AI models in the industry. Unlike other fraud vendors focused on emails, device info, or transactions, Inscribe is dedicated to solving document fraud. We combine the latest AI methods with analysis on 6M+ documents to provide the most reliable and cost-effective solution in the industry. Because we've spent years working with such a wide range of customers, we have the largest document network in the industry.

50%
reduction in application review time

$80M+
fraud caught per month

25X
return on investment

200+
hours saved per week

PLAID MERCARI bluevine ramp AMOUNT SHIFT Petal TripActions Lendflow


Want to learn more?
Reach out to speak with an expert from our team, get a personalized demo, and see if Inscribe is a fit for your business.
Get Started →
inscribe