ALLOY

2023

State of Fraud Benchmark Report

2022 fraud trends and predictions for 2023

How did fraud affect financial institutions in 2022, and what can we start planning for in 2023?

- **100%** of respondents have experienced fraud
- **96%** have lost money to fraud over the past 12 months
- **91%** said that fraud increased YoY
- **71%** of respondents have increased their spending on fraud prevention YoY

Fraud is a growing problem for financial institutions (FIs), large and small.

Fraudsters have gotten increasingly sophisticated over the past few years and are showing no signs of slowing down. They're operating like "startups" — they are technologically savvy, well-funded, innovative, nimble, and growth-oriented. At the same time, customers are demanding reduced friction and more digital options, opening the door for these fraud startups to attack.

Alloy surveyed more than 250 decision-makers working in fraud-related roles at financial institutions ranging from startup fintech companies to enterprise banks. We asked them about fraud and its effects on their institutions.

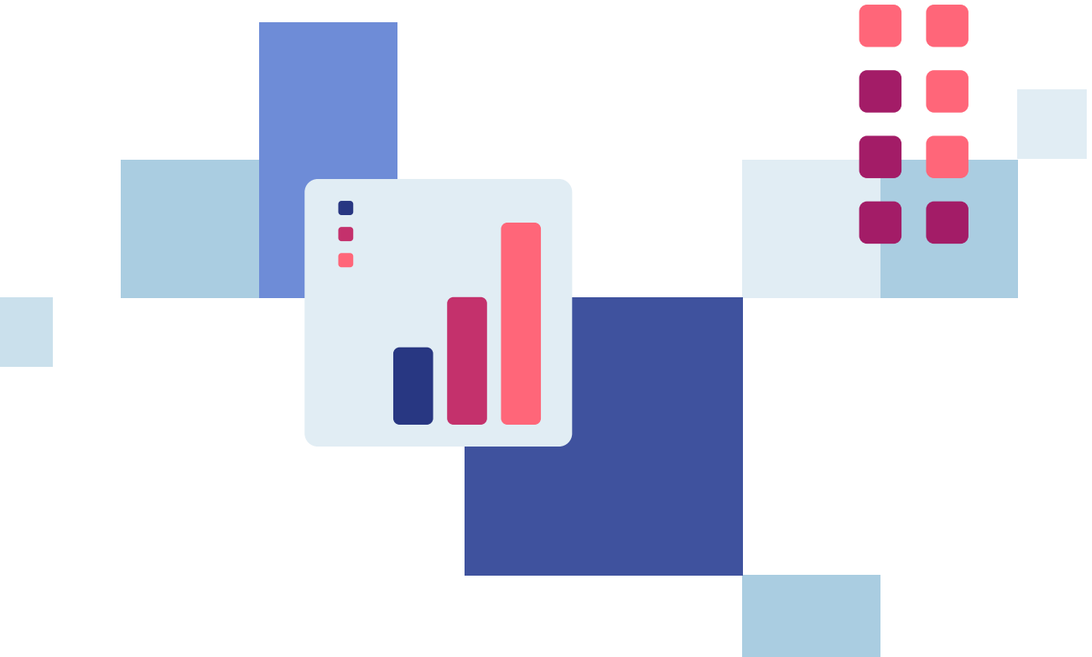


Table of contents

About the survey

Methodology

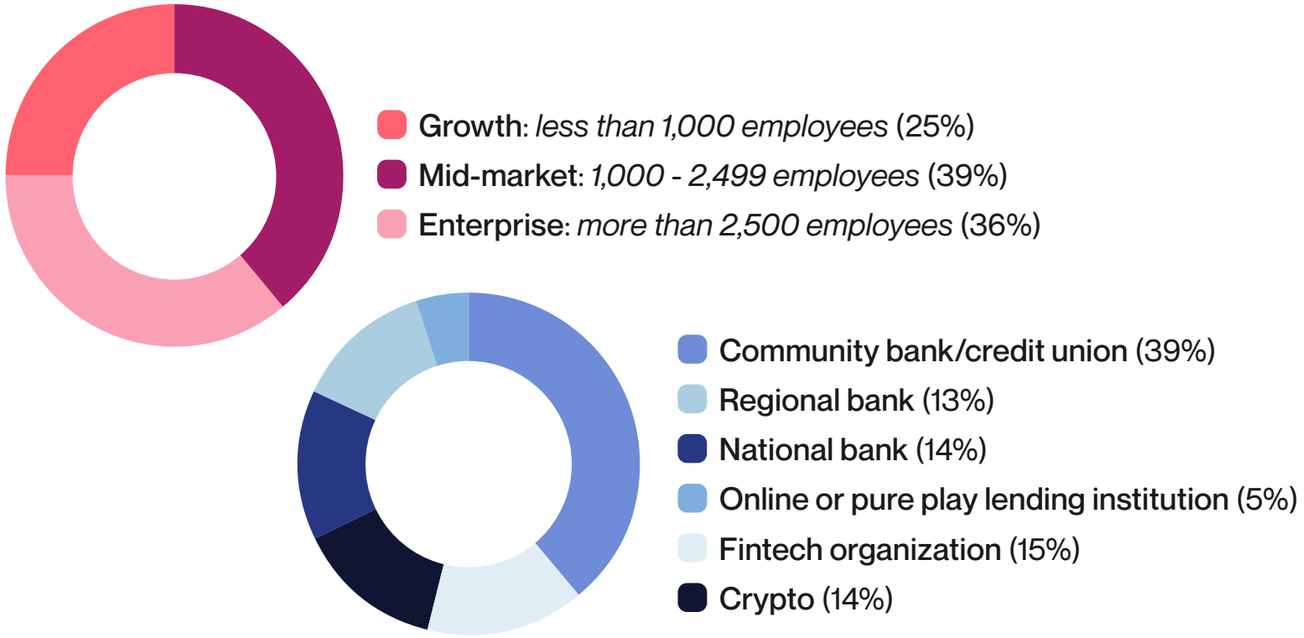
The survey ran from **September 8-20, 2022.**

Respondents included 251 decision-makers working at financial institutions in:

- **Fraud**
- **Compliance**
- **Risk technology procurement**
- **Digital banking strategy**
- **Account opening**

The survey was conducted by **Qualtrics**, a leading survey platform that powers +1B surveys every year.

Demographic segments

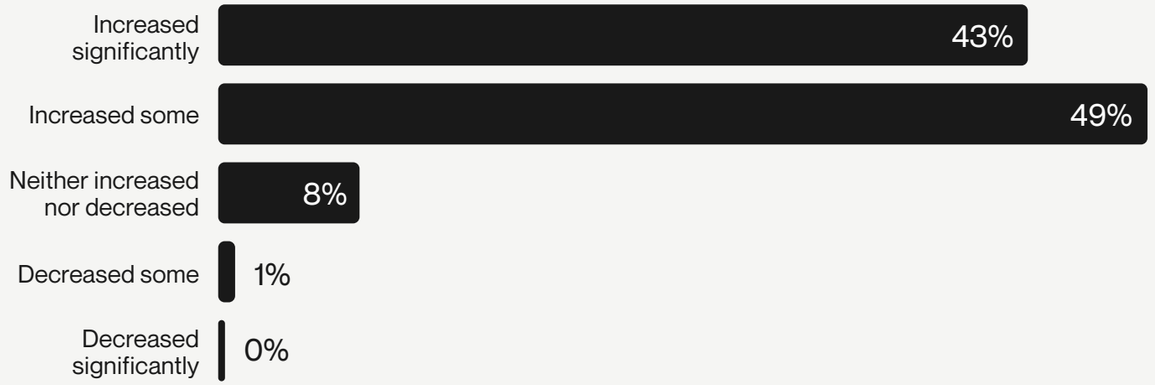


Fraud is a growing problem

91% of respondents said fraud increased year-over-year since 2021.

Only **1%** saw a decrease in fraud.

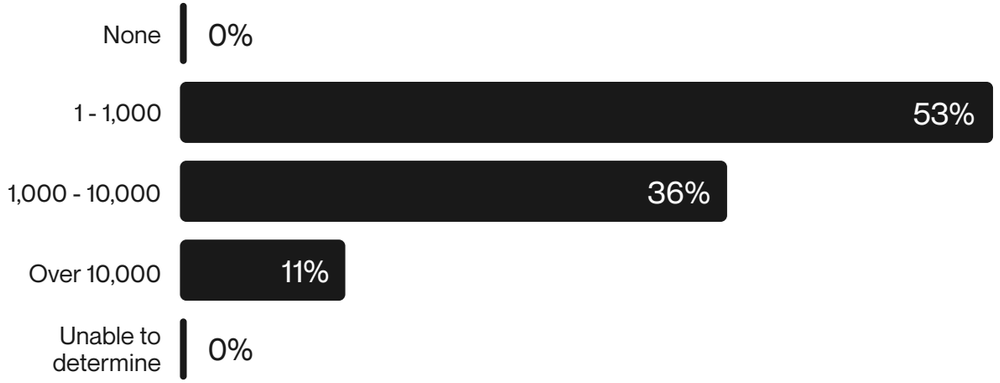
Have fraud rates increased or decreased at your organization in the past 12 months?



All respondents experienced fraud; however, fraud volumes vary by company size

One-third of respondents said they experienced between 1,000 and 10,000 fraud attacks in the last twelve months. 11% of respondents reported over 10K fraud attacks in the last twelve months.

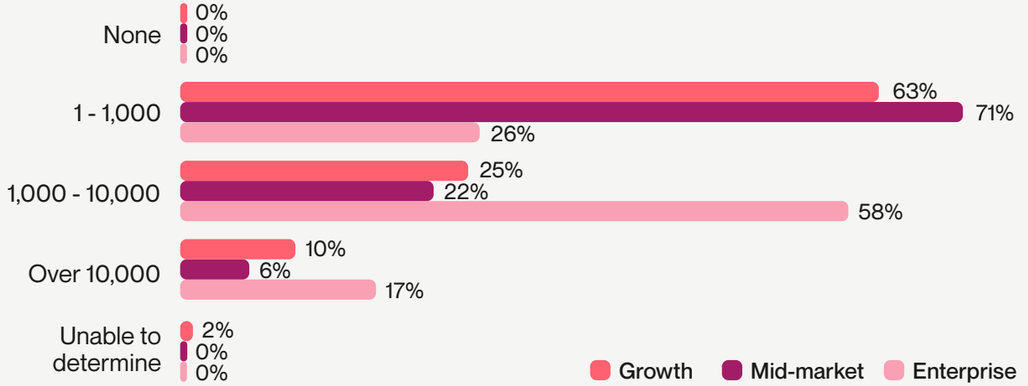
How many people or businesses attempted to defraud your organization in the past 12 months?



BENCHMARK

Larger companies are more likely to experience higher volumes of fraud — 75% of enterprise companies reported seeing over 1K fraud attacks over the last twelve months. In contrast, only 35% of growth companies and 29% of mid-market companies reported seeing over 1K fraud attacks in the past twelve months.

How many people or businesses attempted to defraud your organization in the past 12 months?



First-party fraud is perceived as the most prevalent type of attack

Fraud types defined:

First-party fraud

An individual misrepresents their own identity, financial situation, or intention to repay a financial institution

Second-party fraud

A fraudster convinces another person to use their identity or personal information to perform fraud

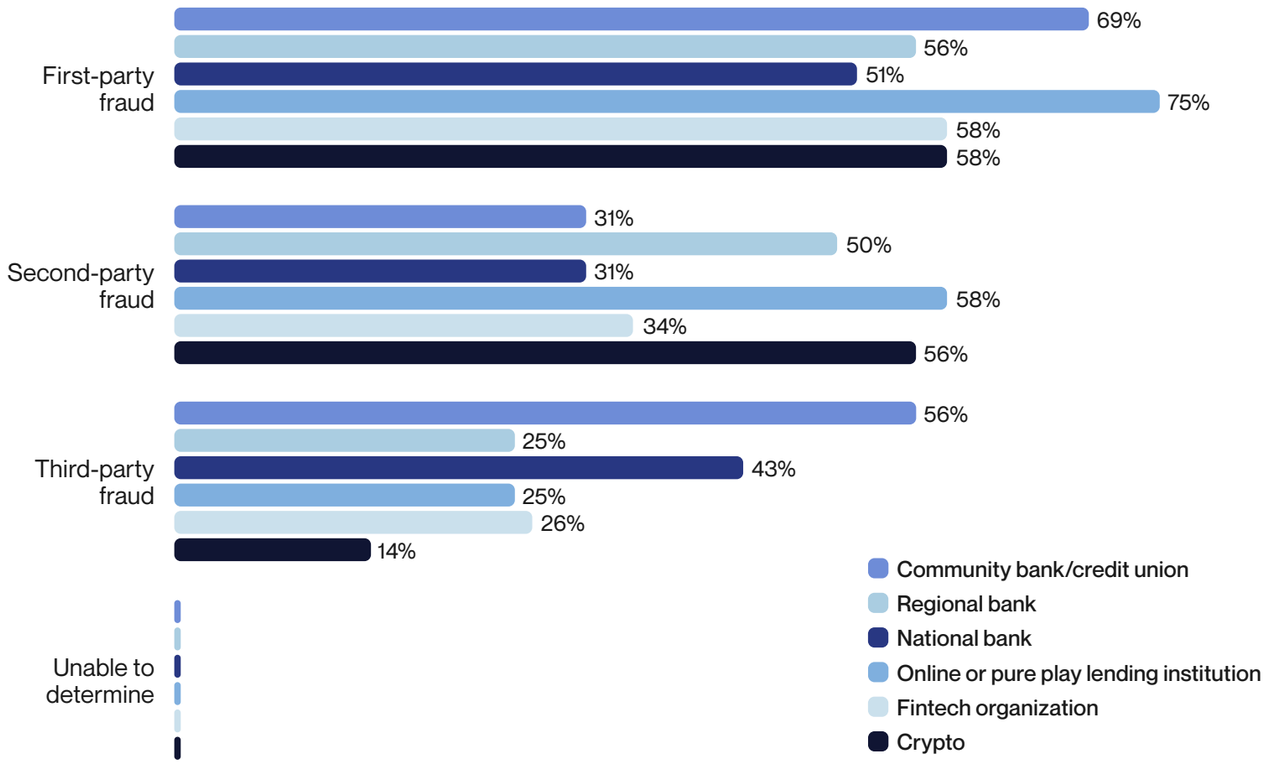
Third-party fraud

Financial crimes that are committed while using someone else's (stolen) identity

Which of the following fraud types have you experienced at your organization? Select all that apply.

Most common fraud types by industry segment

Which of the following fraud types have you experienced at your organization? Select all that apply.



BENCHMARK

First-party fraud is the most prevalent across all types of FIs.

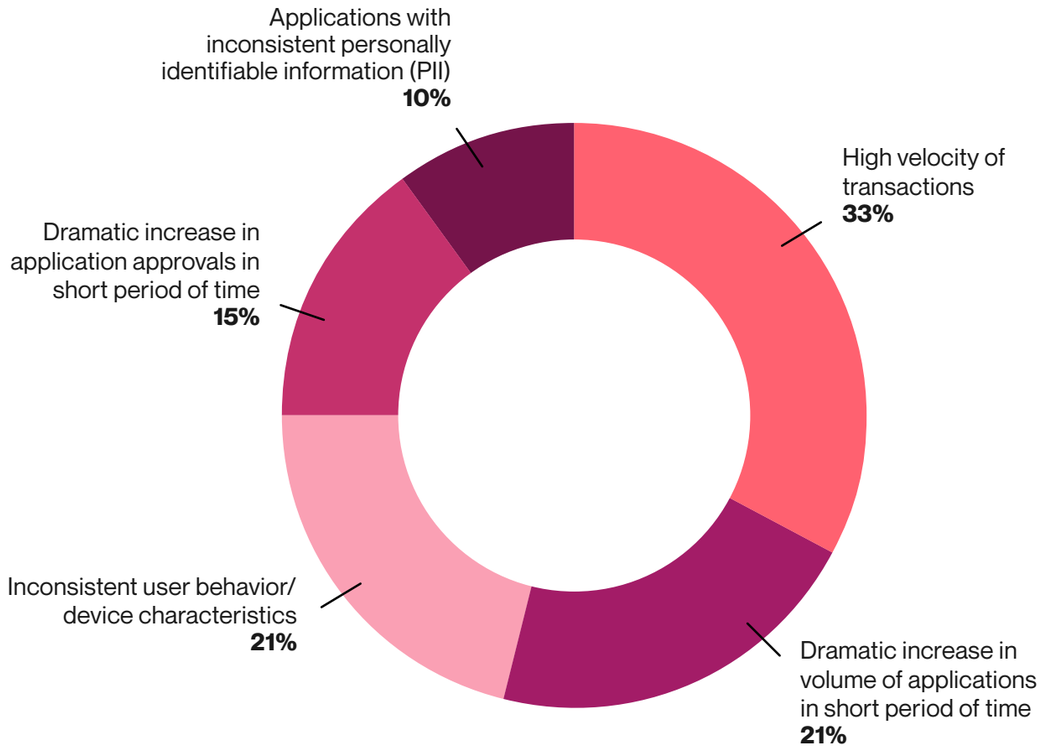
Second-party fraud is more common for online lending institutions, crypto, and regional banks.

Third-party fraud is more prevalent for community banks and national banks.

How are financial institutions catching fraudsters?

Survey respondents reported seeing first-party fraud most frequently. However, flags for high velocity of transactions are typically indicative of a third-party fraud attack in which a large group of fraudsters all target a financial institution at the same time.

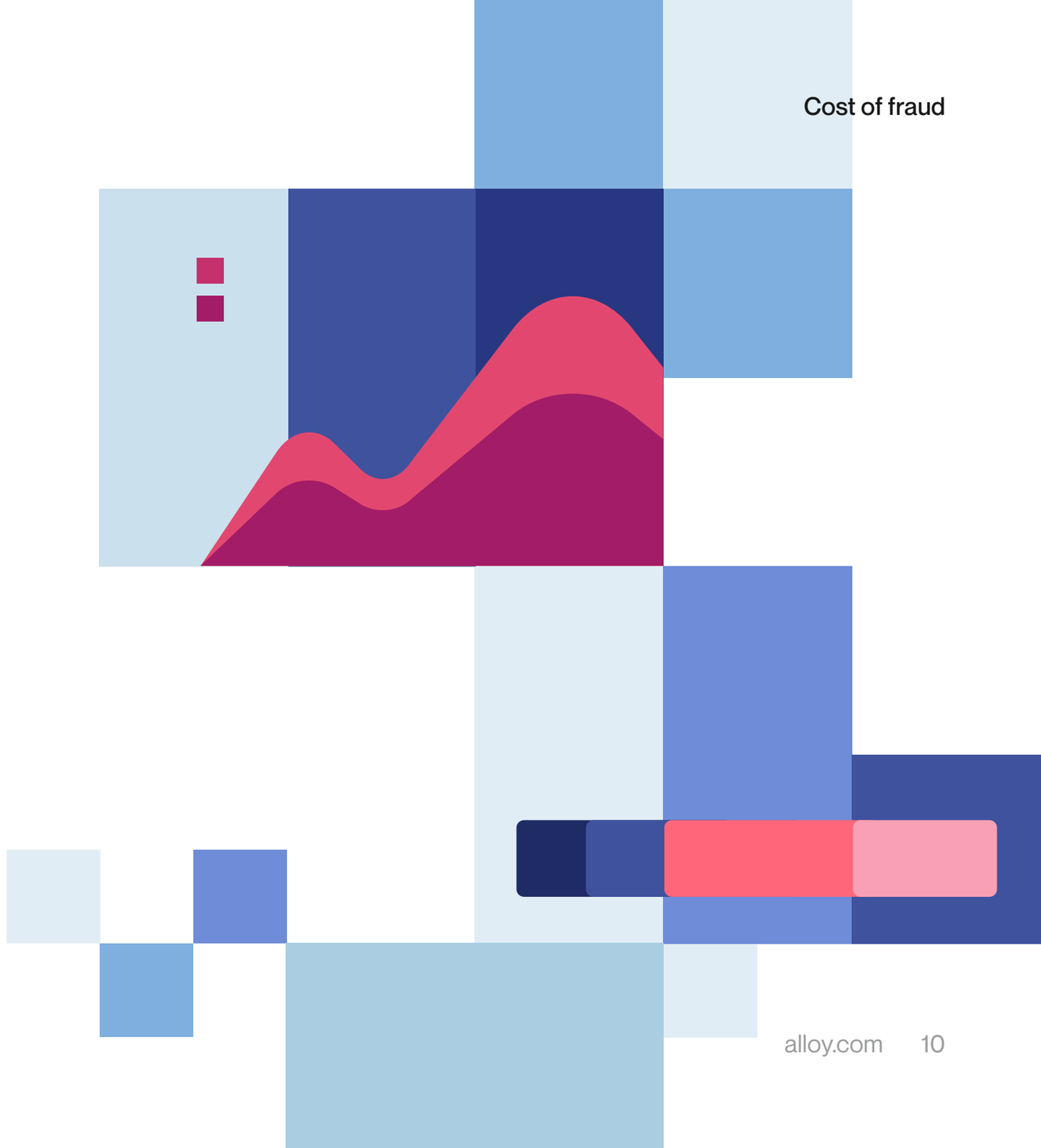
What is your organization's most common flag for fraud?



The cost of fraud runs deep

Many dimensions make up the total cost of fraud for a financial institution. There is a direct cost — i.e., the dollar amount successfully taken by a fraudster — and indirect costs, such as investigations to determine where the fraud is coming from, resources spent recovering fraud losses, and the budget allocated to fraud prevention. There are also longer-term consequences to consider, such as legal repercussions, regulatory fines, reputational damage, and loss of customers.

When you add all of these factors up, the stakes are high.

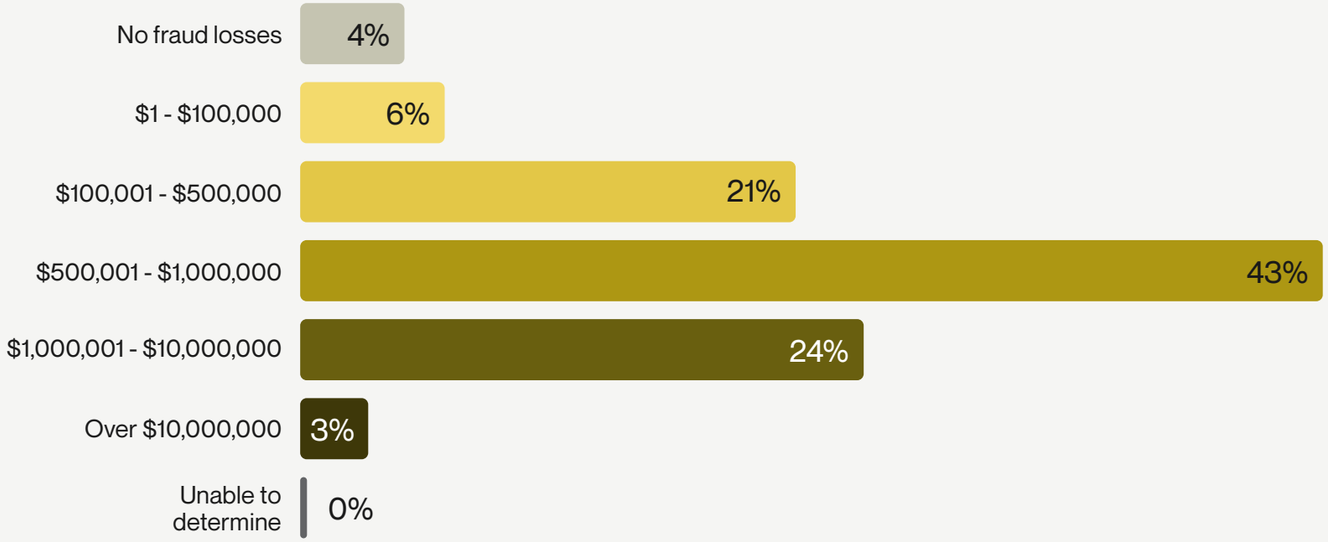


The direct cost of fraud

70% of respondents have lost over $500K in the last twelve months, and 27% of respondents lost over $1M to fraud last year.

And this is just the tip of the iceberg. These estimations only represent fraudulent transactions where their FIs took a monetary loss, not the total fraud their organization was exposed to. It does not include any bad actors they stopped at onboarding, fraudulent transactions detected and loss averted, and bad actors that made it through their onboarding funnel and have not yet defrauded them.

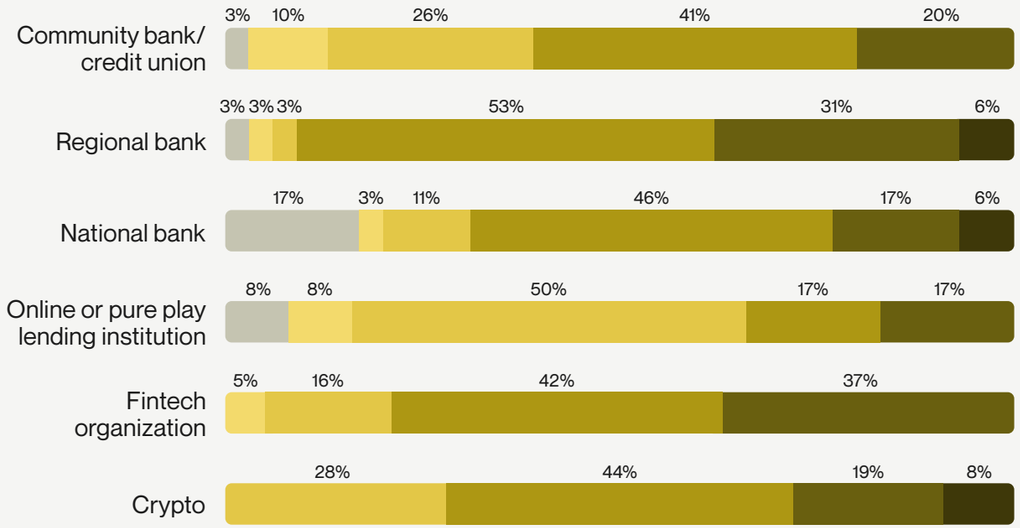
How much do you estimate your organization lost through fraud over the last 12 months?



The direct cost of fraud by segment and size

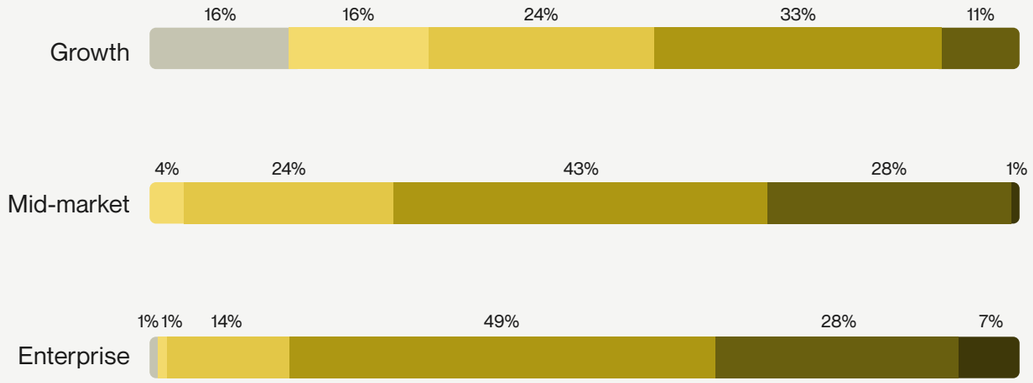
BENCHMARK by segment

How much do you estimate your organization lost through fraud over the last 12 months?



BENCHMARK by size

How much do you estimate your organization lost through fraud over the last 12 months?

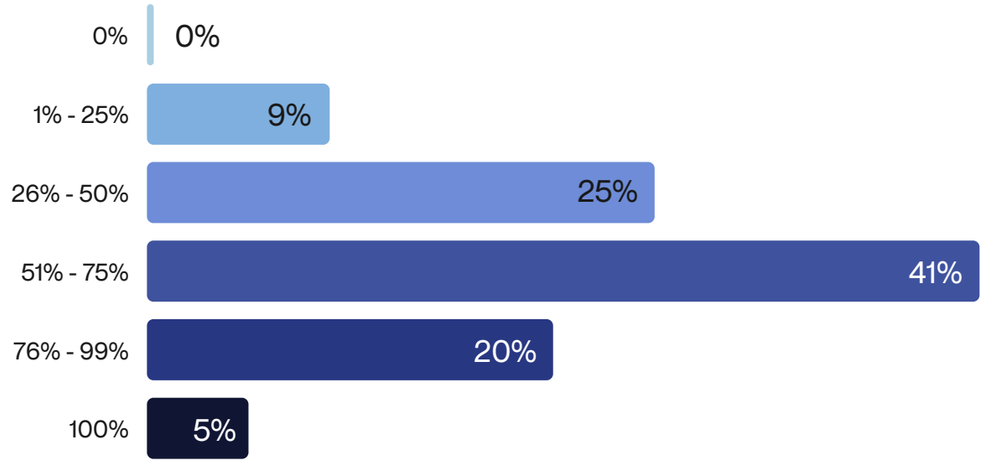


No fraud losses | $1 - $100,000 | $100,001 - $500,000 | $500,001 - $1,000,000 | $1,000,001 - $10,000,000 | Over $10,000,000 | Unable to determine

Investigating and recovering fraud funds is an uphill battle

Respondents were generally optimistic about recovering their fraud losses. Over half of respondents said they were able to recover most (51-100%) of fraud losses. Still, recovering fraud losses is a resource-consuming process.

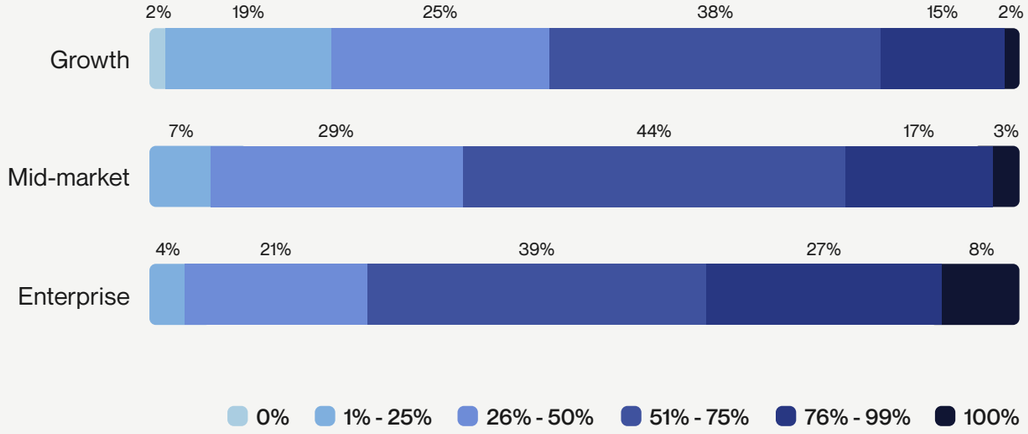
About what percentage of these fraud losses were recovered?



BENCHMARK

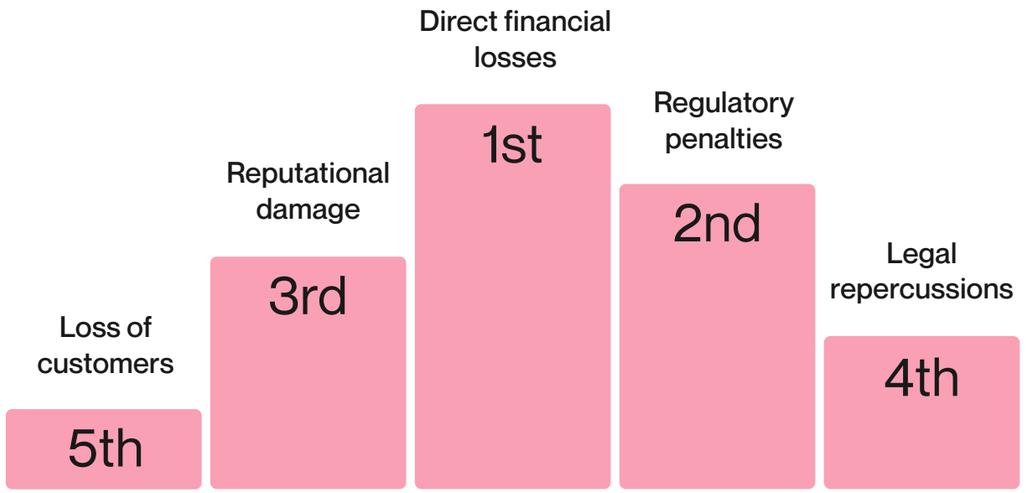
Your chances of recovering fraud losses correlate to how many resources your organization has. Enterprise organizations were more likely to recover most of their fraud losses (74%), compared to 64% of mid-market organizations and 55% of growth companies.

About what percentage of these fraud losses were recovered?



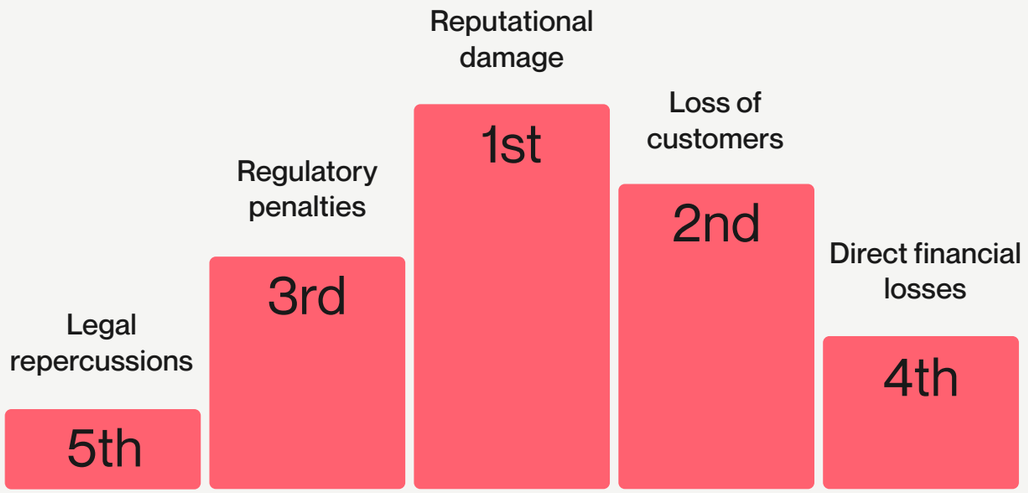
Not all costs are treated equally

Respondents ranked direct financial losses as the cost they care most about, with loss of customers being the consequence they care least about.

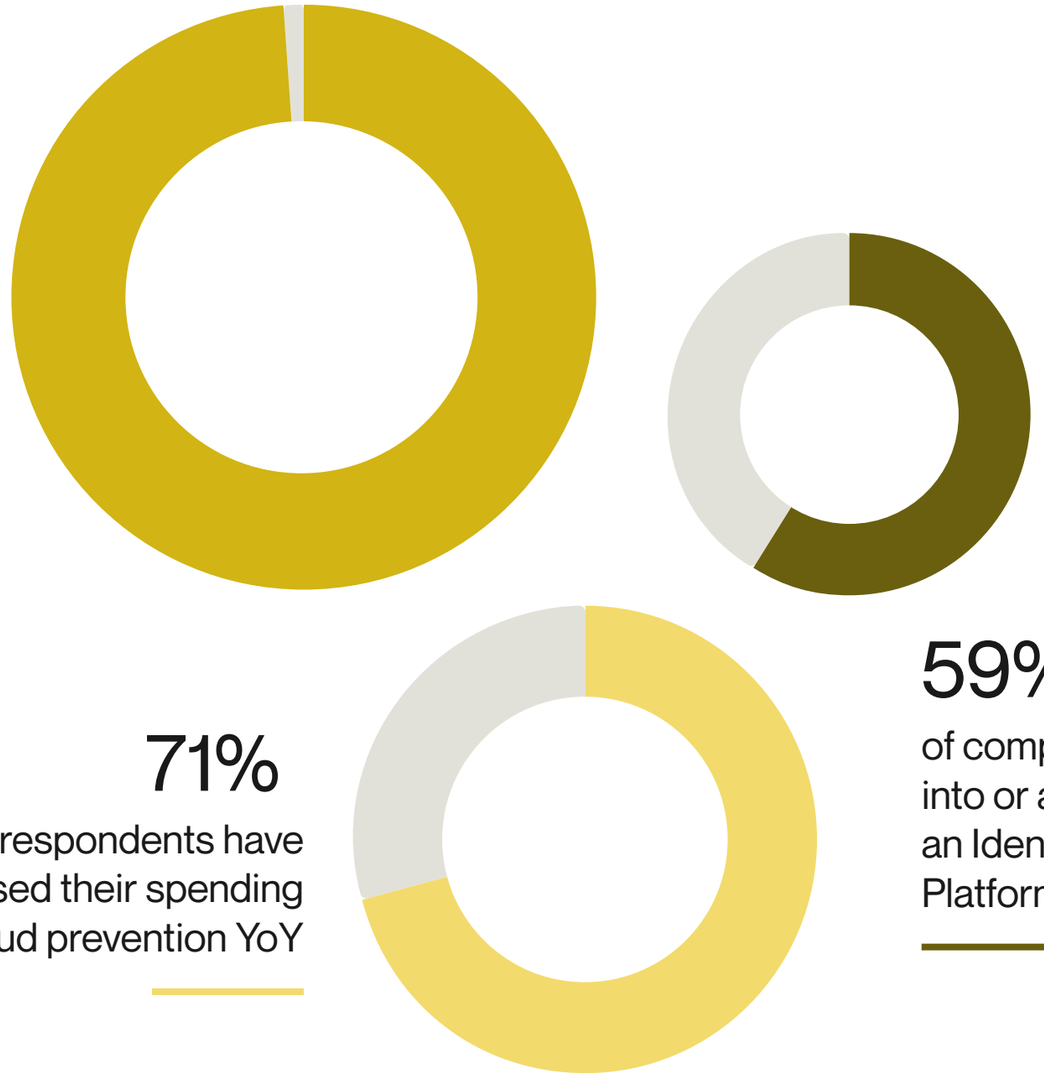


BENCHMARK

However, when you look at how **C-suite respondents** answered this same question, you see more interest in the “hidden” indirect costs of fraud than the general respondent population.



How are FIs responding to increased pressure from fraudsters?



99%

have made changes to their policies and controls for fraud prevention in light of the evolving fraud landscape

71%

of respondents have increased their spending on fraud prevention YoY

59%

of companies are looking into or are already using an Identity Decisioning Platform (IDP)

Automation is the leading barrier to fraud preparedness

Even though 95% of respondents said their organizations could sufficiently manage fraud in-house, they still identified some significant areas for improvement.

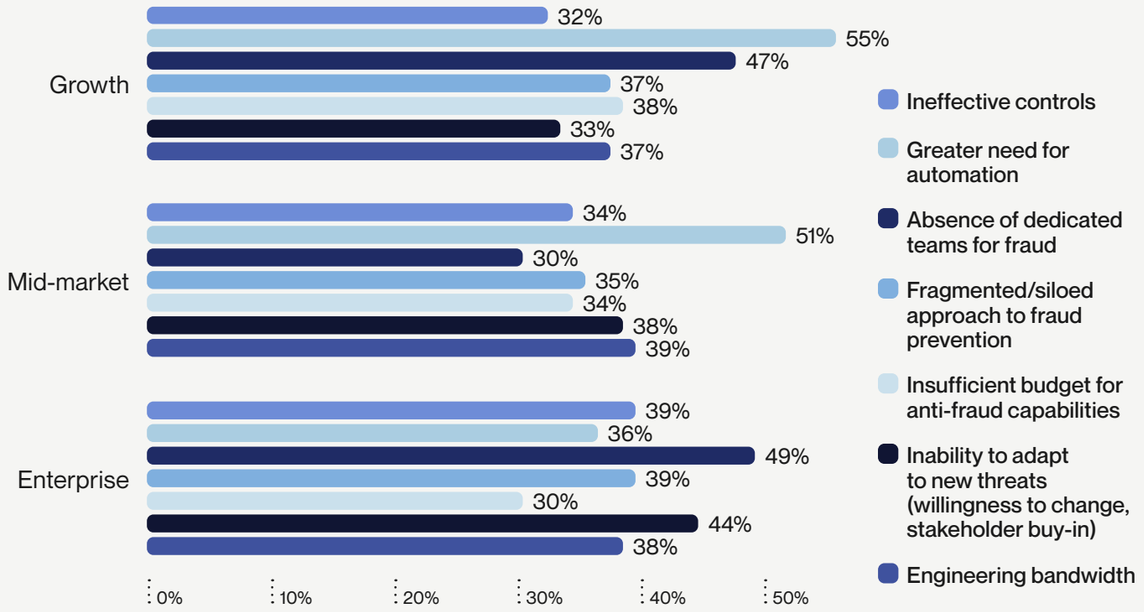
46% of respondents cited a greater need for automation as the most common barrier to being prepared to combat fraud, followed by an absence of dedicated teams for fraud (41%) and the inability to adapt to new threats (39%).

Why do you believe your organization is not prepared? Select all that apply.

BENCHMARK

Smaller companies are looking to automate manual work to optimize resourcing, while larger organizations are more likely to build dedicated teams to solve fraud.

Why do you believe your organization is not prepared? Select all that apply.

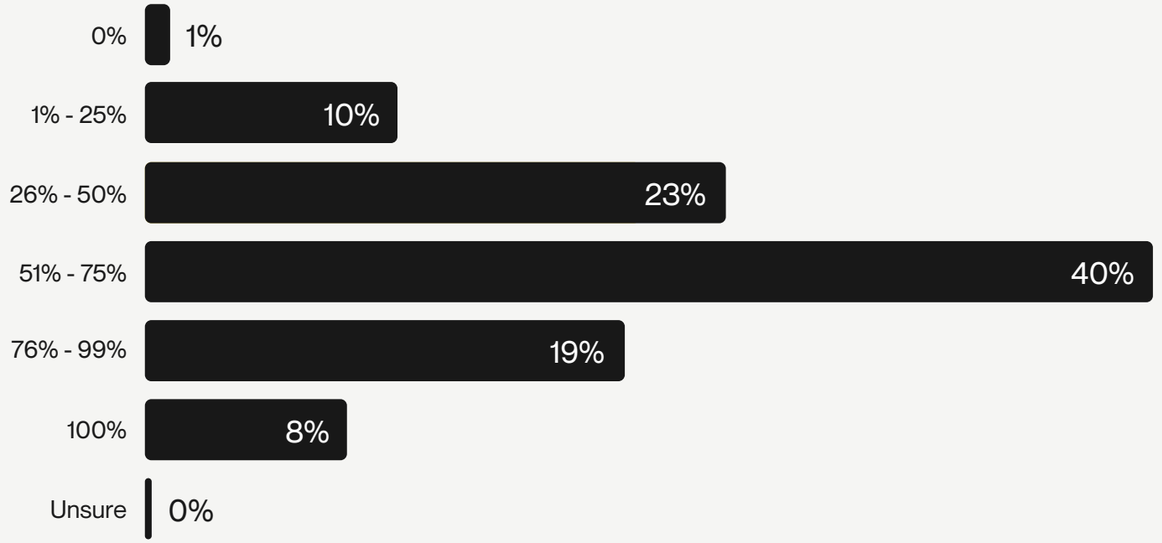


How many employees does it take to solve fraud?

There are a lot of cooks in the kitchen when it comes to working on fraud-related projects.

Two-thirds of respondents have over half their workforce working on fraud-related activities.

At your organization, what percentage of employees are working on fraud-related projects/activities?

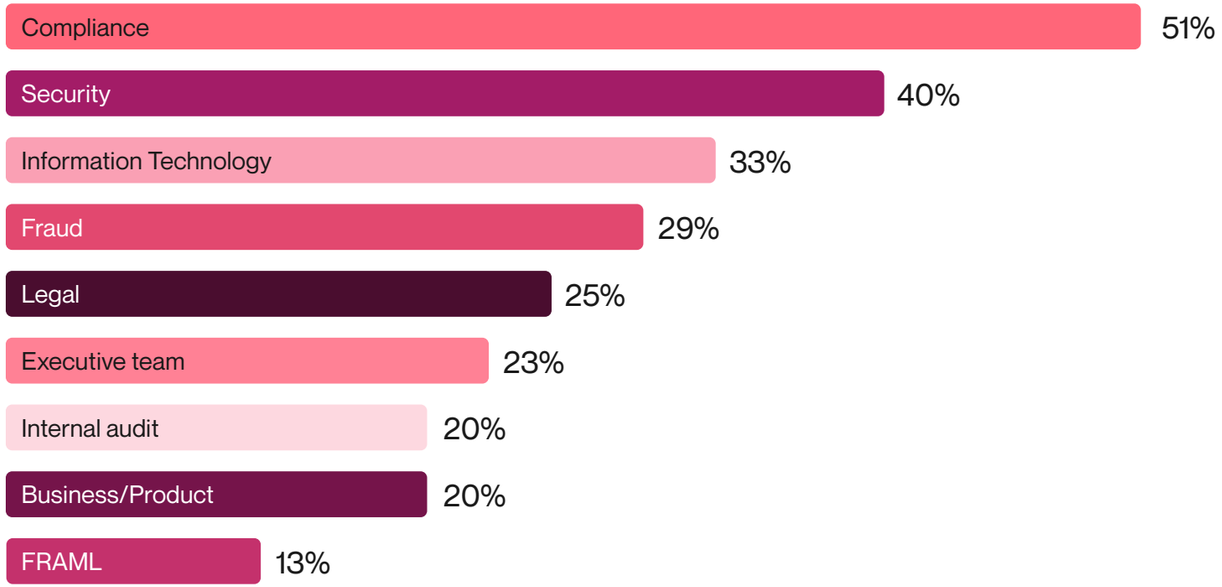


Who's who in fraud prevention

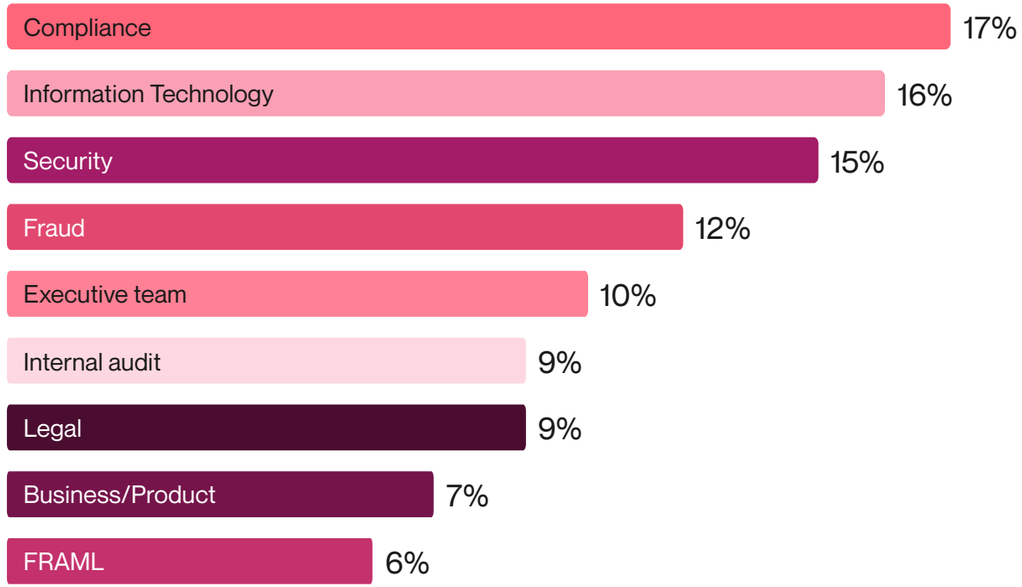
More than half of respondents said their Compliance teams are **involved** in fraud prevention efforts (51%), followed by Security (40%) and Information Technology (33%).

Those three groups were also most commonly named the **owners** of fraud — Compliance (17%), Information Technology (16%), and Security (15%).

At your organization, which of the following teams/functions are involved in fraud prevention? Select all that apply.



At your organization, which of the following teams/functions are owners of fraud prevention?

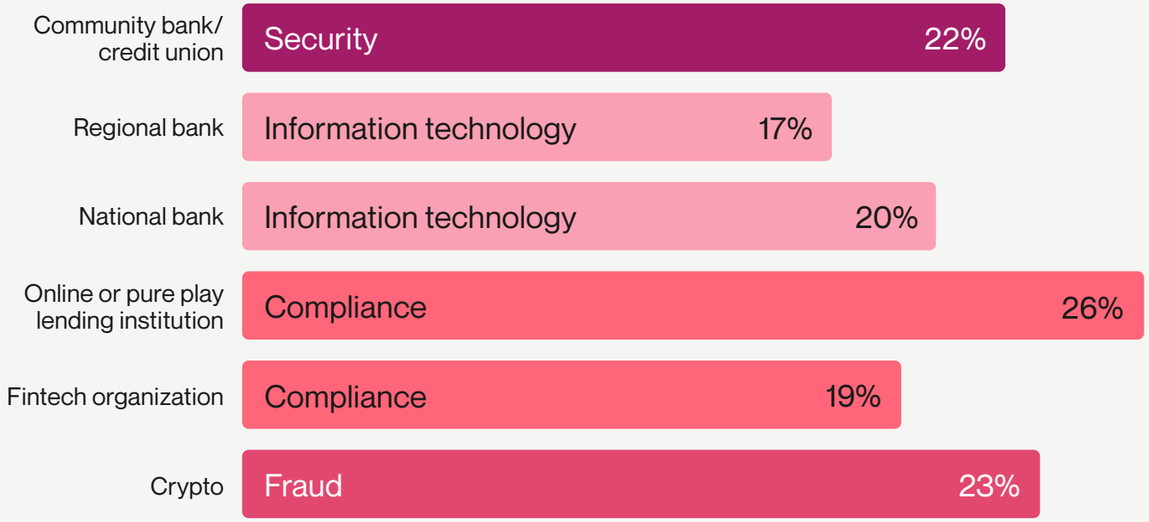


Fraud prevention ownership varied significantly across different segments

Crypto companies were more likely to name their fraud team as the owner of fraud prevention.

BENCHMARK

At your organization, which of the following teams/functions are owners of fraud prevention?

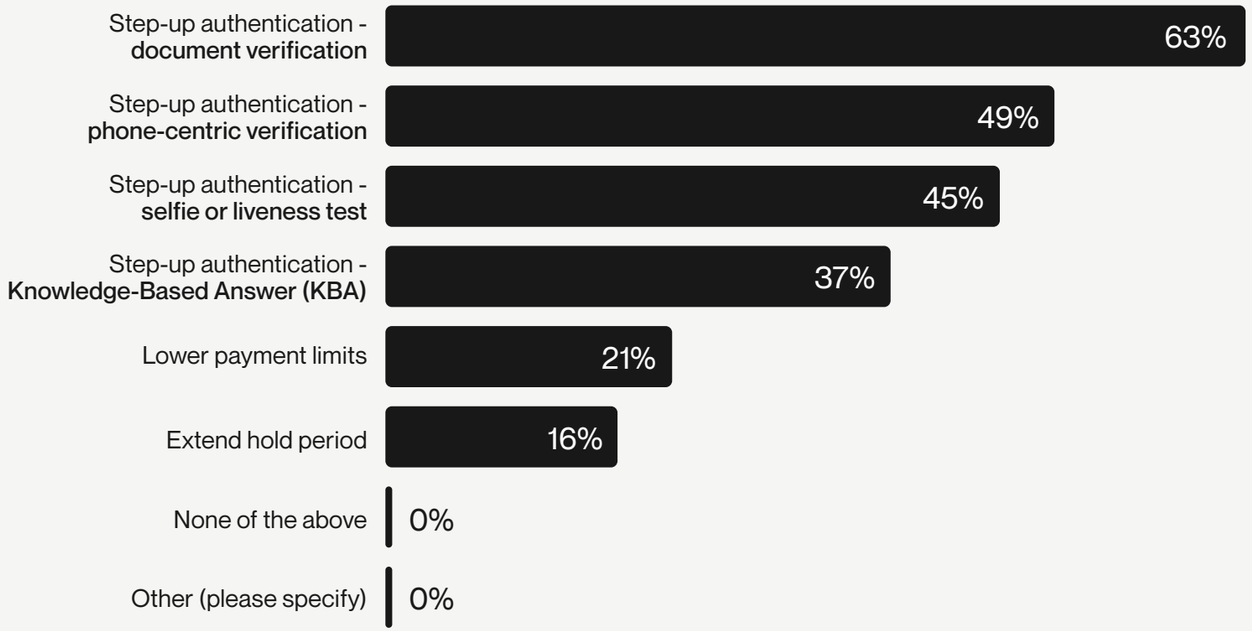


Step-up verification is a common next step once fraud is detected

Even while experiencing fraud, customer experience is paramount.

Few FIs hold payments (16%) or lower payment limits (21%) after fraud is identified. Instead, they lean heavily on step-up document verification (63%) and step-up phone-centric verification (49%) once fraud is detected.

Once suspected fraud is identified, how does your organization respond? Select all that apply.

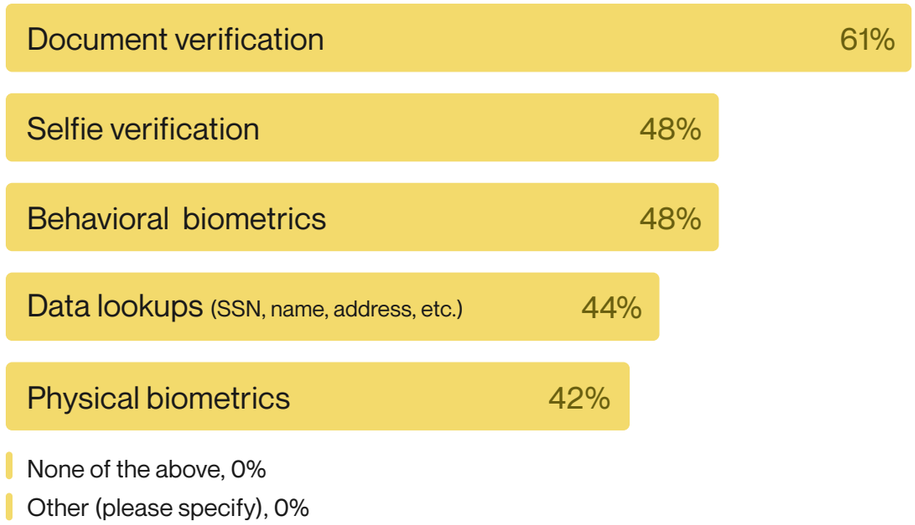


What's in your fraud prevention toolkit?

Managing and preventing fraud at onboarding can be a whole different ball game from managing and preventing fraud on an ongoing basis.

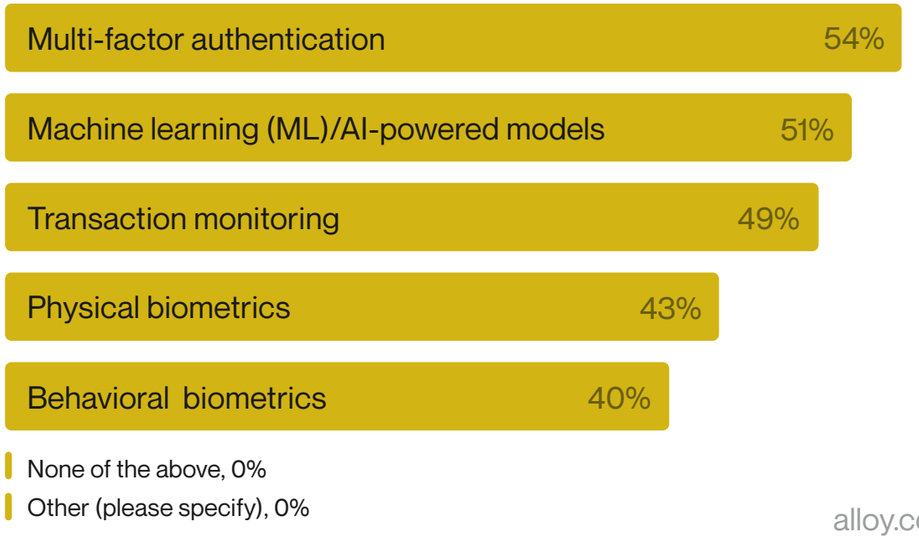
Document verification (61%), behavioral biometrics (48%), and selfie verification (48%) are the top tools for preventing fraud at onboarding.

Which of the following controls does your organization use when onboarding new customers? Select all that apply.



Multi-factor authentication (54%), ML & AI (51%), and transaction monitoring (49%) are top tools for monitoring fraud on an ongoing basis.

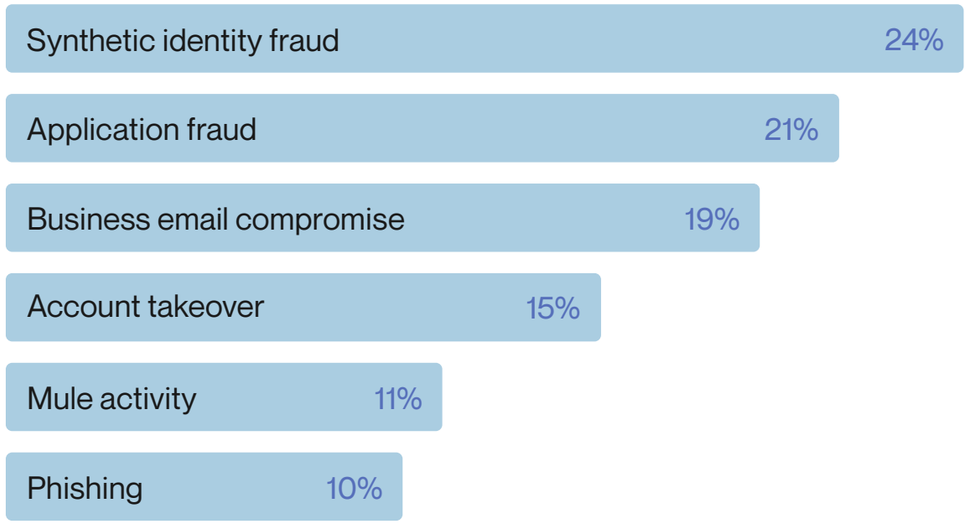
Which of the following controls does your organization use to monitor ongoing risk? Select all that apply.



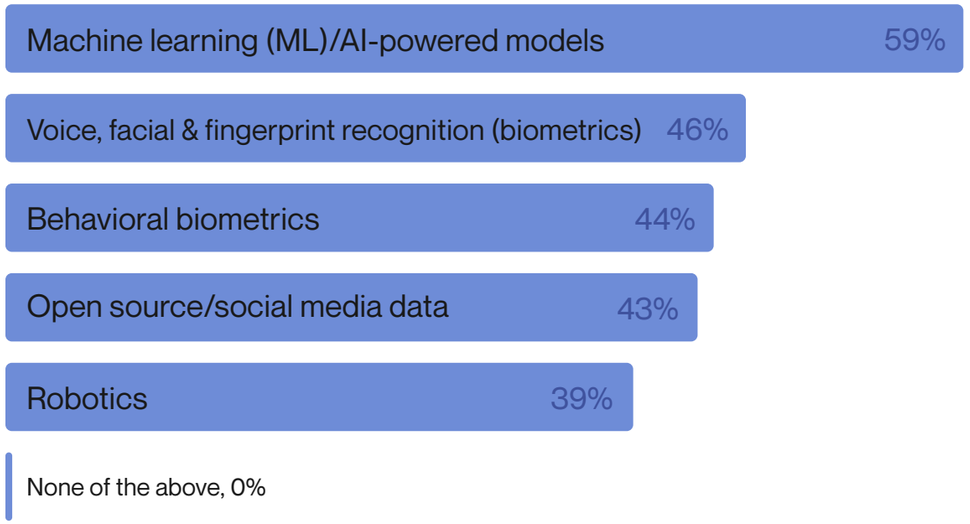
Respondent predictions for 2023

Synthetic identity fraud and application fraud will remain top of mind for FIs in 2023, while FIs leverage more machine learning/ artificial intelligence models and biometrics data to improve their fraud controls.

In the next 12 months, which type of fraud are you most concerned about?

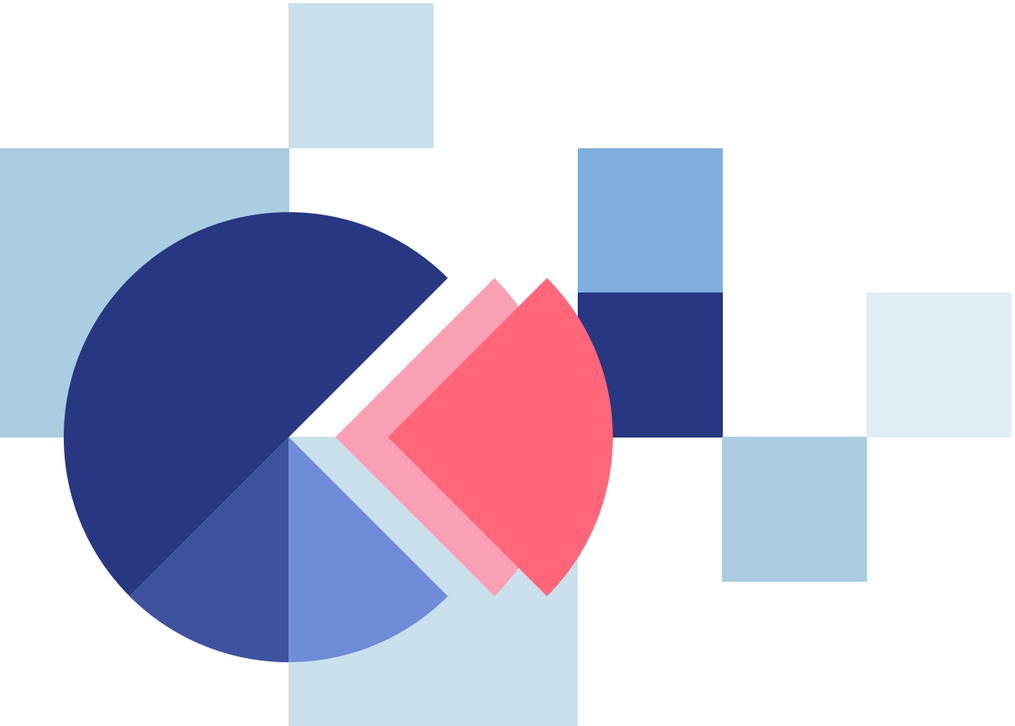


Which of the following emerging technologies will your organization be looking to invest in over the next 12 months? Select all that apply



Where will fraud go next?

Predictions for 2023 from Alloy's fraud analyst, Caroline Lu:



"Synthetic fraud will continue to rise because of the continued digitization of payments. Synthetic fraud identities are usually built over the span of multiple years as fraudsters build their fake identities' credit history. Fraudsters typically wait 3-5 years to "warehouse" the stolen information before they start using it to apply for accounts. We expect a lot of the PIIs that were stolen in early 2020 when the pandemic started to surface in 2023-24 (exactly three years after the leaks).

We should also expect a rise in employment-based fraud and other various scams due to the macroeconomic conditions and volatile stock market we're seeing right now. Scammers know many people are uncertain and struggling and will use it to their advantage.

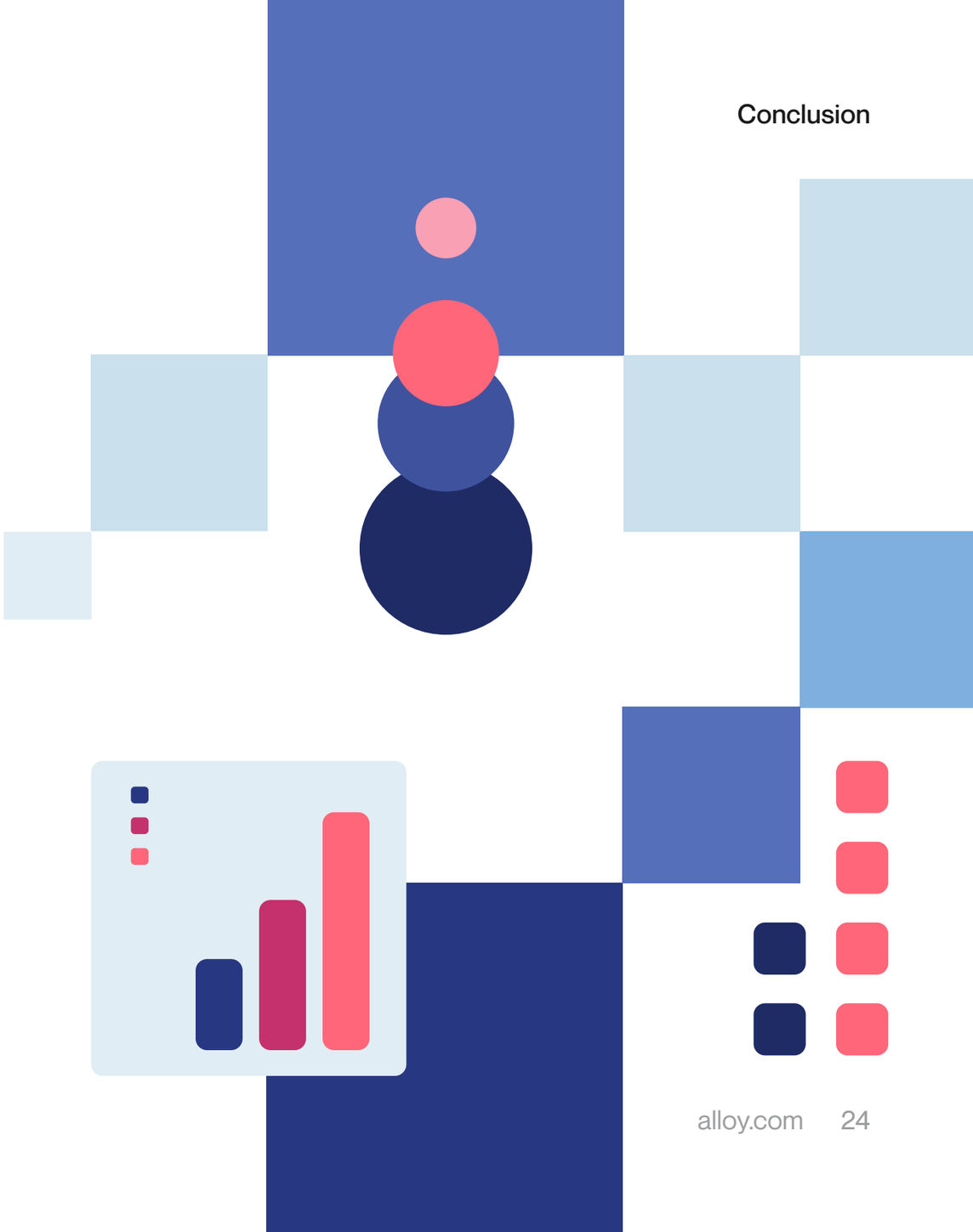
Fraudsters might offer assistance in helping improve your credit, recoup investment losses, file social security or unemployment claims, or even offer victims fake job opportunities. In exchange, one would have to give away their social security number, bank account information, and other PII data. Then, the fraudsters will use the information to open up new bank accounts or apply for new credit cards without the knowledge of the actual person."

Conclusion

Fraud has been on the rise for years, and 2022 was no exception, with 91% of respondents agreeing that fraud rates increased over the past twelve months. At the same time, fraudsters are becoming more sophisticated in their methods of attack. Respondents across the board recognize the growing threat, which they acknowledge can lead to significant financial losses that are challenging to recover. C-suite respondents, however, are also looking big picture. They are particularly concerned about the “hidden” costs of fraud, such as legal repercussions, loss of customer relationships, and reputational damage.

In response, financial institutions are putting more resources towards the problem. For enterprise businesses, that’s in the form of building out dedicated fraud teams to analyze fraud trends and optimize their fraud controls. For mid-market and growth businesses, it’s in the form of increasing automation so their leaner teams can focus on other business objectives.

Despite most respondents increasing their spending on fraud prevention resources YoY (71%), they are likely missing some critical pieces to the puzzle. As we look ahead to 2023 and beyond, investments should be focused on improving agility to future-proof fraud controls. Financial institutions with a flexible fraud tech stack will be uniquely positioned to fight the fraudsters of today, while adapting to the fraudsters of tomorrow.



About Alloy

Alloy solves the identity risk problem for companies that offer financial products. Today, nearly 500 banks and fintechs turn to Alloy's end-to-end identity risk management platform to take control of fraud, credit, and compliance risk, and grow with confidence. Founded in 2015, Alloy is powering the delivery of great financial products to more customers around the world.

Learn more at alloy.com