REPORT | VOLUME 02

State of Fraud and AML

Unit21

Table of Contents

Foreword

Jason Mikula
Publisher, Fintech Business Weekly

If there's one constant of the last several years in banking and Financial Technologies (FinTech), it's change.

The near-manic environment of the early pandemic, powered by near-zero interest rates, surging levels of venture capital, and government stimulus for businesses and consumers alike has left some in the industry with a bit of a hangover.

But problems that were easier to ignore (or throw bodies at) a few years ago, including fraud and Anti-Money Laundering (AML) risk, haven't gone anywhere.

In fact, as this report will lay out, 65% of industry professionals surveyed believe instances of fraud and money laundering are likely to grow in 2024. But, as experienced fraud and AML professionals no doubt know, identifying and mitigating these risks is a constant game of "whack-a-mole." Bad actors are constantly probing for weaknesses to identify new opportunities.

Emerging technologies, like the recent launch of FedNow, bring new capabilities to banks and FinTechs and new products and services to consumers, but are also likely to pose new fraud and AML risks as bad actors find novel ways to take advantage of them. And, like any

business, bad actors respond to incentives. While PPP and unemployment fraud represented alluring, lucrative targets during the height of the pandemic, fraudsters always follow the money. Likewise, AML requirements and risks are constantly evolving as regulations change, as geopolitical situations develop, and as regulators and law enforcement pursue offenders.

As the operating environment continues to shift, FinTechs are navigating the abrupt change in priorities from "growth at any cost" to a focus on unit economics and plausible routes to profitability – making getting a handle on costly fraud more important than ever.

Government regulators continue to step up their scrutiny of banks and the FinTechs they work with, as recent regulatory actions and pronouncements have demonstrated. This all adds up to the need for companies in the space to drive better outcomes, often with fewer resources at their disposal.

The theme of "doing more with less" is one that clearly resonated with many survey respondents, with 71% saying a top priority for the next year includes reducing reliance on manual processes by improving automation. But, despite industry players spending billions on "digital transformation" and data management solutions, information silos remain a major problem – an astonishing 55% of respondents admitted to having trouble locating and integrating data.

As everything in the world seems to continue speeding up, manual processes, whether asynchronous, look-back transaction monitoring, or suspicious activity report filing, are increasingly no longer fit for purpose. Moving from detecting fraud and AML issues to preventing them requires a paradigm shift in how FinTechs and banks think about planning, building, and operating their risk management frameworks and tech stacks.

> *"I continue to believe that openly discussing the state-of-play of fraud and AML in banking and FinTech – the good, the bad, and the ugly – is a critical necessity to achieve progress in making advancements in mitigating these threats, both at a company-level and at an industry-wide one."*

This report, based on input from over 250 industry Risk & Compliance professionals, offers a snapshot of challenges facing practitioners today and opportunities for improvement in the future.

This report wouldn't be possible without the industry professionals who took the time to contribute to it (and to Unit21 to compile and analyze their responses) – so, to everyone who took the time, thank you! ■

Jason Mikula
Publisher, **Fintech Business Weekly**

Executive Summary

Risk & Compliance professionals are expecting more fraud and money laundering instances to occur in the next year, but companies aren't investing in growing their Risk & Compliance teams to combat these threats. Ultimately, this leaves fraud and AML teams with limited access to critical resources like engineering support, making it harder to adapt to growing transaction volumes and a variety of threats.

Organizations are trying to do more with less, and they need a system that cost-effectively supports their needs. Unsiloing data, automating manual tasks, and empowering teams to move from fraud detection to prevention are their top priorities in the foreseeable future.

- **65%** believe instances of fraud and money laundering will grow in 2024
- **55%** admit to having trouble locating and integrating their data
- **71%** said adding automation to manual processes was a priority in the next 12 months

In the subsequent sections, we delve deeper into these insights, interspersed with real-world data from our survey.

By the end of this report, you'll discover:

1. **The top priorities for today's Risk & Compliance professionals**
2. **The biggest challenges facing Risk & Compliance teams**
3. **What it takes to build a successful Risk & Compliance program**
4. **The main reasons why software solutions are purchased (or not)**
5. **What's coming in the future of fraud and AML**

Who We Surveyed

Methodology

We surveyed a total of 264 Risk & Compliance professionals from organizations of all different sizes and at various stages to draw insights on how fraud and AML teams view the current state of the market. We explore their biggest pain points, their core objectives, and top priorities for the near future.

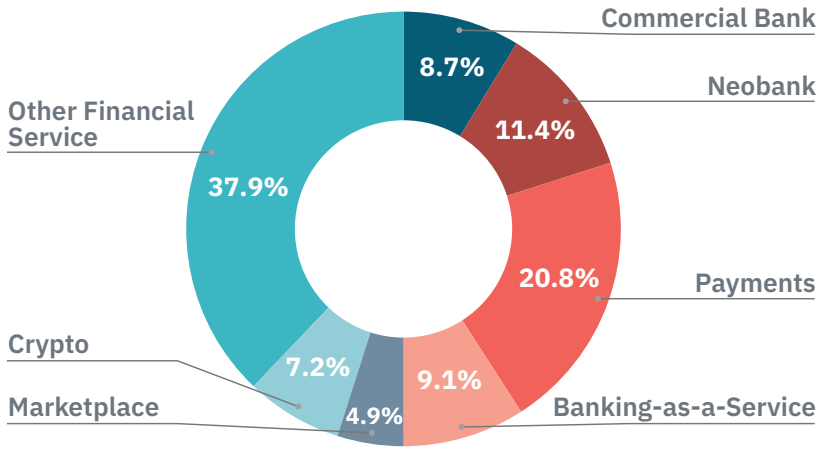
- *Survey Dates: July 2023*
- *Survey Size: 264*

All participants must also:

- Be a part of the financial services landscape
- Be responsible for fraud and/or AML within their organization

Risk & Compliance Organization Breakdown

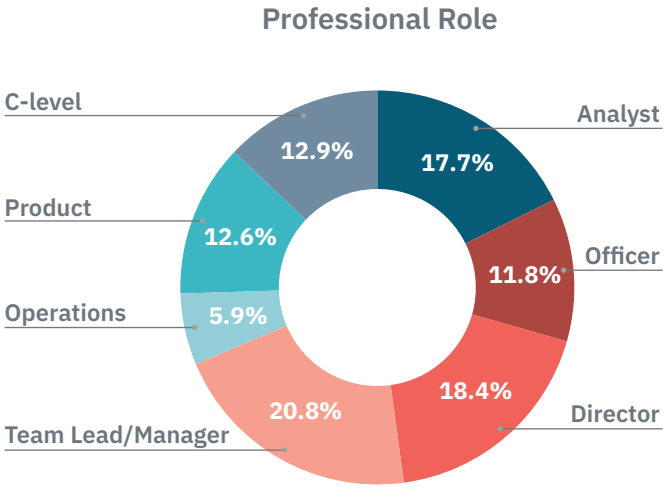
By Industry Type

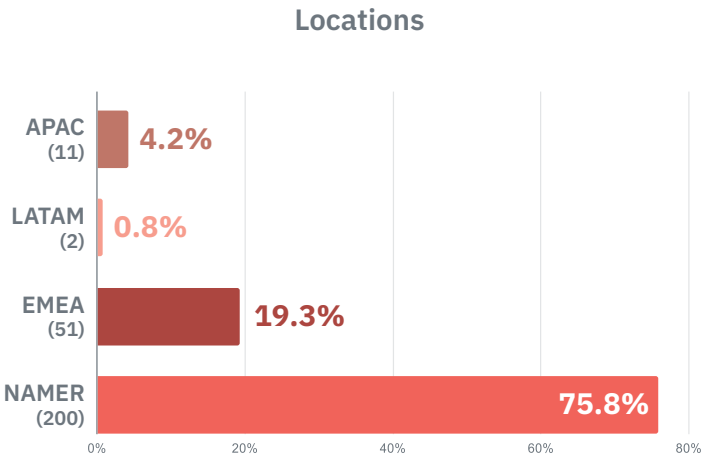


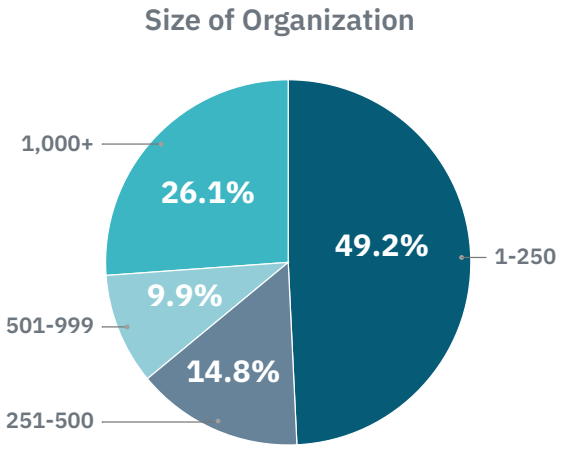
Respondent Firmographics

This survey aimed to understand how those responsible for fraud and/or AML view the current state of these programs at their organization and the industry as a whole. All survey participants are responsible for one or more of these areas at their respective companies.

Participants were from companies of varying sizes, industries, and locations, and respondents held a myriad of roles within their respective organizations.





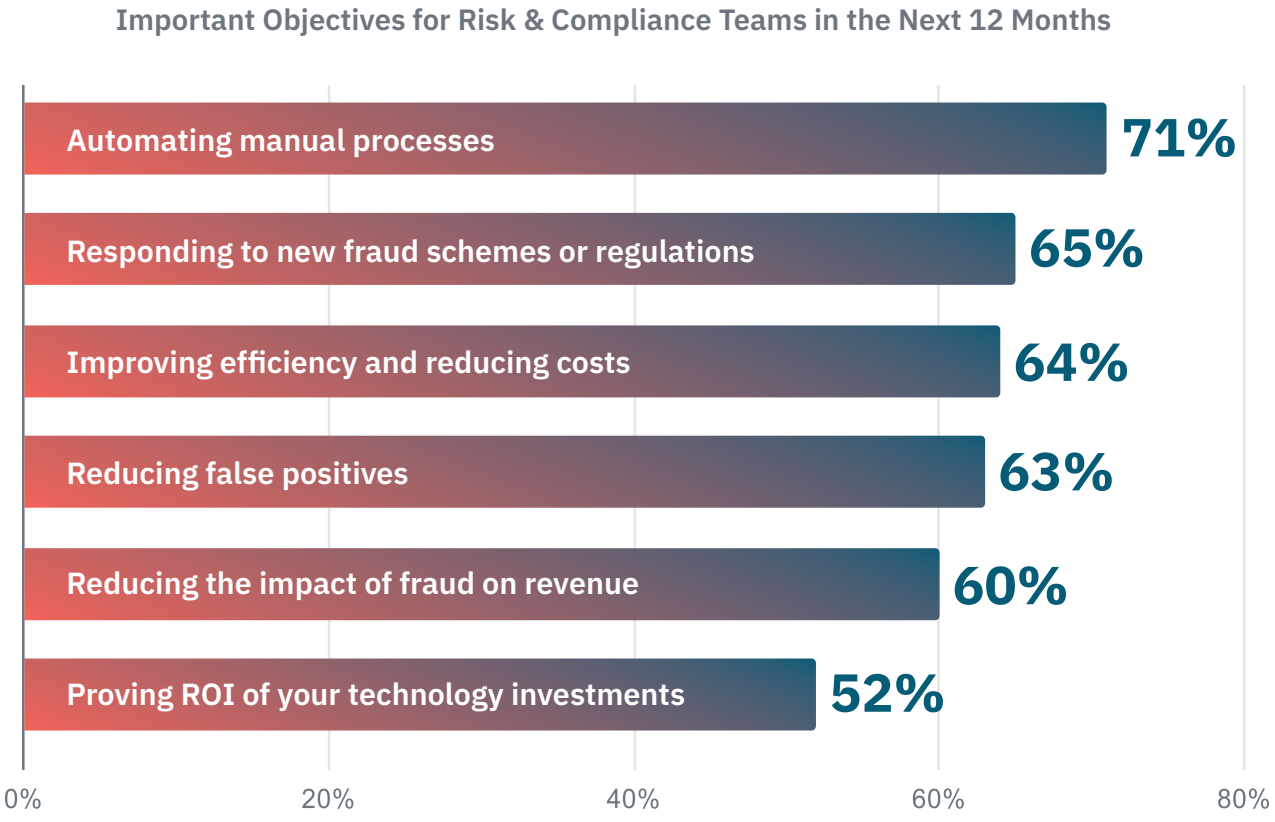


Top Priorities for Risk & Compliance Professionals

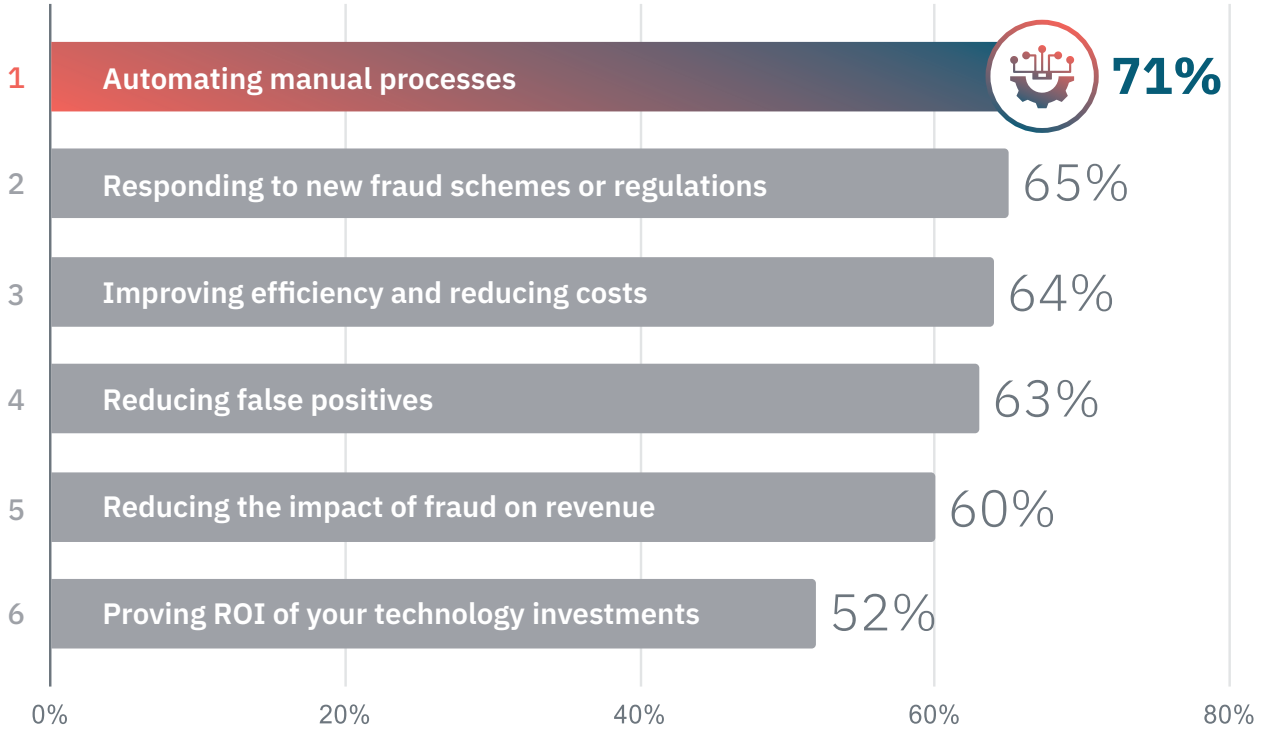
Based on survey results, the following stand out as pivotal priorities for Risk & Compliance professionals over the next year:

1. **Integrating automation into manual tasks (71%)**
2. **Adapting to evolving financial crimes and regulatory changes (65%)**
3. **Enhancing efficiency & trimming the cost of fraud + compliance programs (64%)**

Let's dive into what respondents had to say about each of these areas.



1. Adding Automation to Manual Processes



71% of respondents rated automating manual processes as a top objective for the next 12 months.

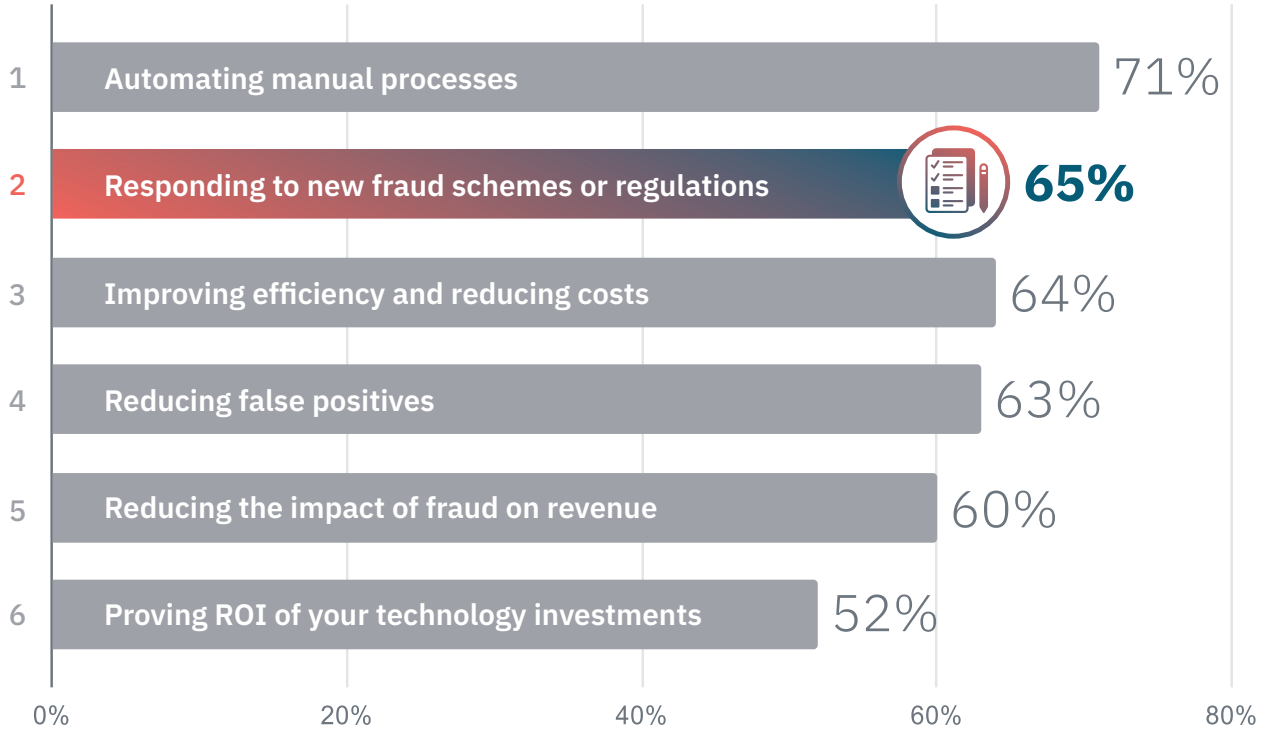
In 2022, reducing manual work for analysts and automating processes like alert resolution and filing were some of the top priorities for fraud and AML professionals, but this year, automating manual processes is even more prominent.

Despite stagnant growth rates in Risk & Compliance teams (28% reported zero growth and 23% reported less than 10% growth), transaction volumes soared.

To top it off, there are ever-increasing ways to transact, including new payment rails like FedNow and various service offerings trying to keep pace with consumer appetites. The increase in transactions and ways to transact, coupled with limited headcount expansion, means teams are pressed to do more with less.

To manage these challenges, financial organizations are compelled to optimize operations and target the automation of processes that are currently manual.

2. Addressing Evolving Fraud Schemes and Regulations

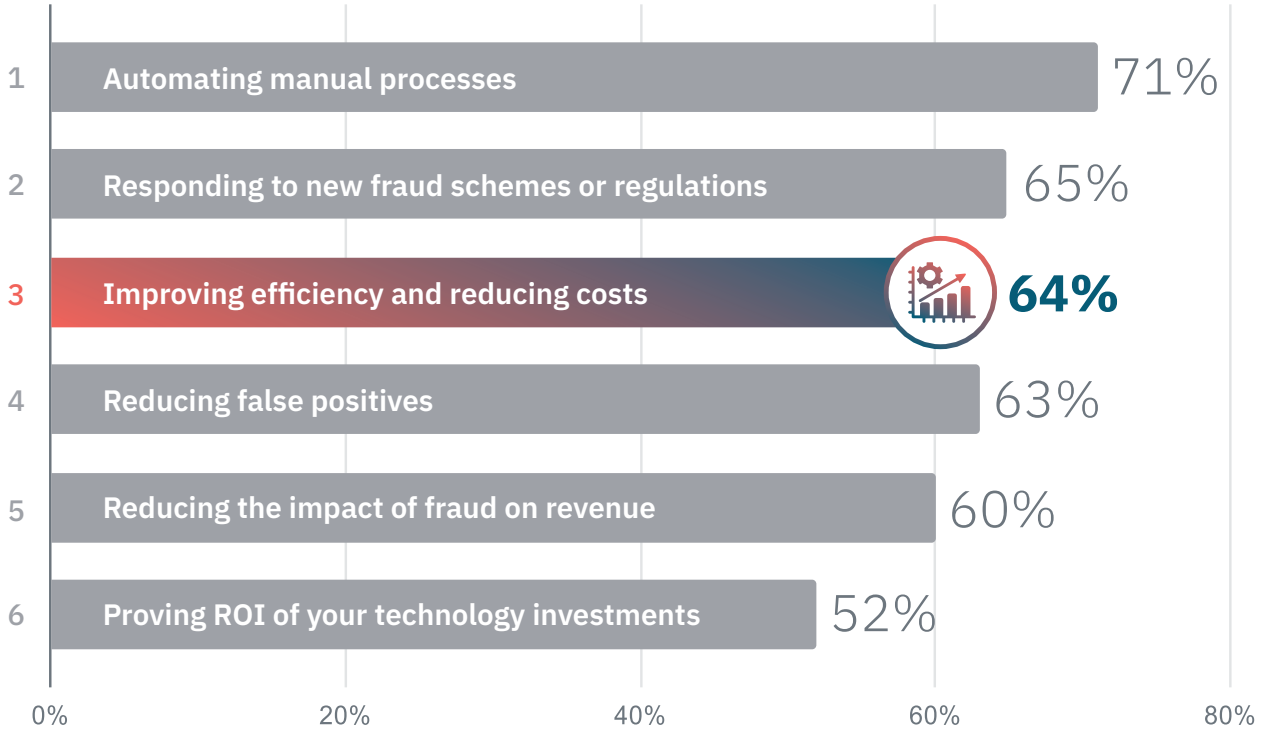


In 2022, identifying new fraud schemes was the top pain point for Risk & Compliance professionals. Turning that knowledge into preventative measures was also relatively important, ranking as the 4th largest pain point.

This year, **65% of respondents said that the ability to respond to changing financial crime schemes and new regulations was critical to their teams in the following year**, making this the second most important priority.

With a continuously evolving fraud landscape and AML regulatory market, professionals are concerned about identifying—and quickly responding to—emerging fraud threats and changes to AML regulations. Therefore, the priority isn't just identification—it's transforming that knowledge into preventive measures to minimize future financial crime.

3. Improving Efficiency and Reducing the Cost of Fraud & Compliance Programs



It's understandable that professionals prioritize enhancing efficiency, given the importance of automating tasks. For many, the ultimate goal is to streamline processes, thus saving costs.

Having a system that streamlines workflows, increases productivity, and does so without adding manpower is an ideal solution for fraud and AML teams—and upper management!

Since the aim of Risk & Compliance is to mitigate fraud losses and increase revenue, the more teams need to spend on these solutions, the less chance they have to actually achieve their goal of reducing monetary losses. Teams must trust a solution that allows them to optimize operations and reduce costs associated with fighting fraud, money laundering, and other financial crimes.

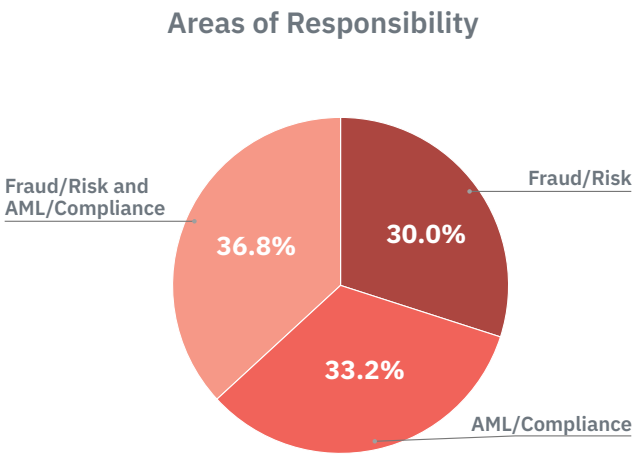
Biggest Challenges for Fraud and AML Teams

1. Varied Priorities for Different Teams

Fraud teams, AML teams, and FRAML teams, while working within the same broad domain of Risk & Compliance have slightly different primary concerns and challenges based on the nature of their functions.

Fraud Teams

Their primary focus tends to be on identifying and preventing unauthorized or fraudulent activities. This might involve monitoring for suspicious transaction patterns, flagging potentially compromised accounts, and integrating real-time anti-fraud measures. They often grapple with the rapid evolution of fraud strategies and the need for real-time response mechanisms.

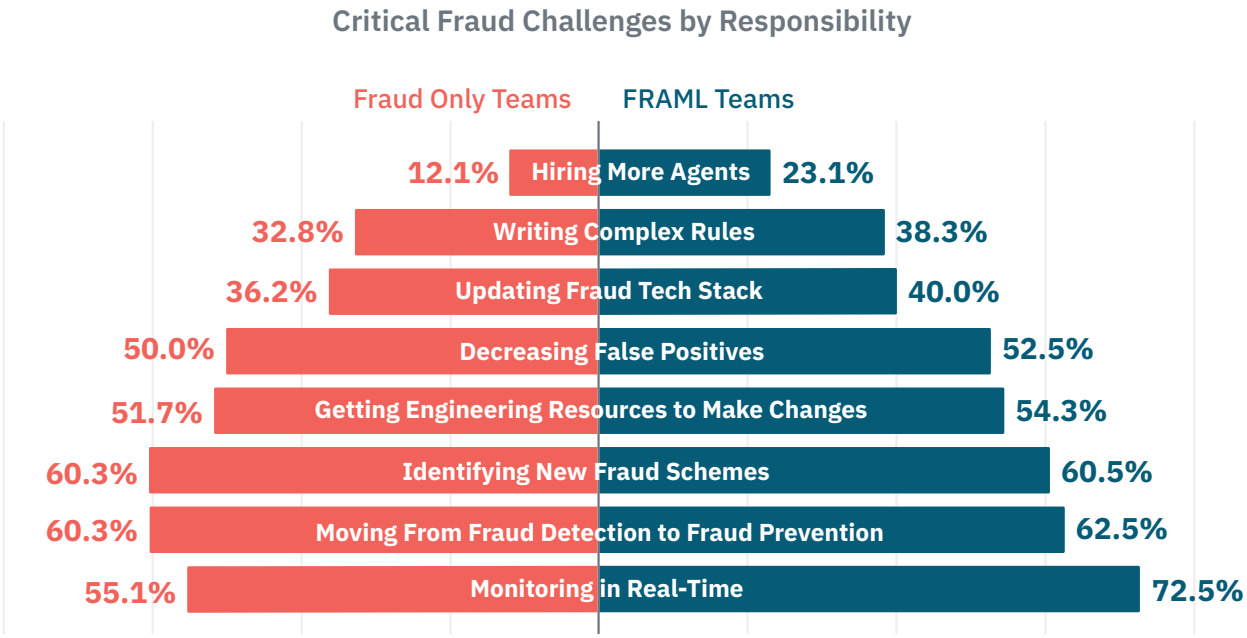


AML (Anti-Money Laundering) Teams

AML teams primarily ensure that financial transactions are not being used as a medium for money laundering activities. This involves tracking large or suspicious transactions, ensuring proper customer due diligence, and reporting to regulatory bodies when necessary. They often face challenges in tracking complex transaction chains, staying updated with ever-evolving regulatory requirements and ensuring accurate reporting.

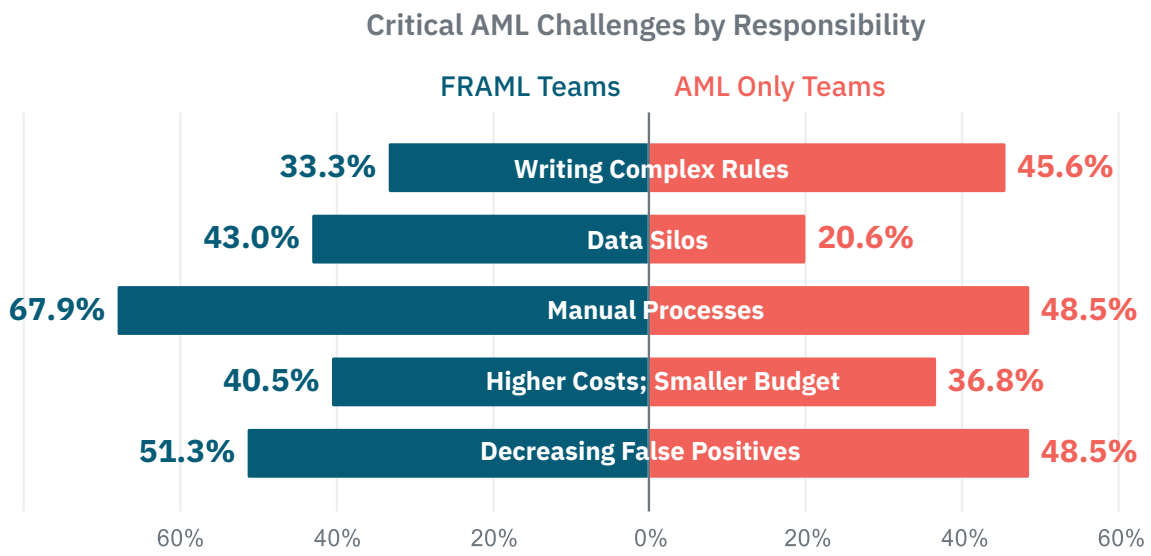
FRAML (Fraud, Risk, and Anti-Money Laundering) Teams

FRAML teams, being a confluence of both fraud and AML focuses, have a dual mandate. Their unique challenge lies in striking a balance between proactive fraud prevention and stringent AML compliance, often requiring a more integrated system that can cater to both requirements simultaneously. Data silos are particularly problematic for FRAML teams because they need a unified view of data to combat both fraud and money laundering effectively. They also emphasize the need for systems that can adapt quickly to both evolving fraud strategies and changing AML regulations.



Teams responsible for Fraud and FRAML list the same top three challenges but in slightly different orders. Notably, across the board, these three responses received 60% of votes from respondents, showing they are relatively equal in importance to both teams.

The key difference is that monitoring in real-time was the third highest challenge for fraud teams, while it ranked as the overall most important challenge for FRAML teams—and by a big margin (nearly 20%).



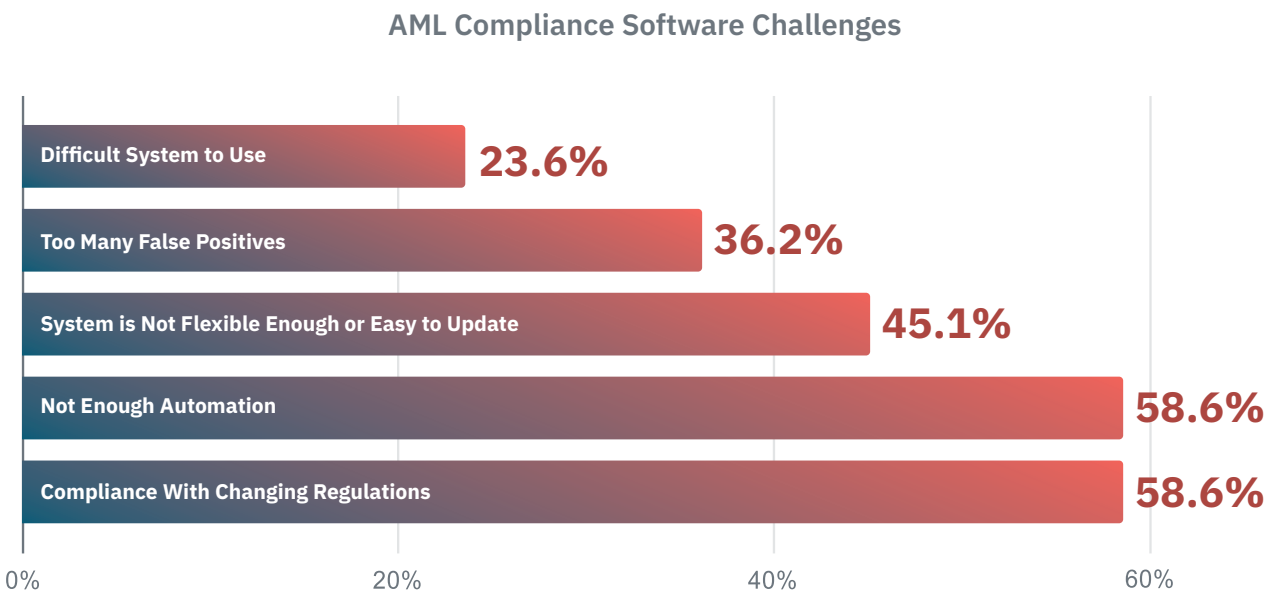
Teams responsible for AML and FRAML both listed manual processes and decreasing false positives as their top two challenges, although teams responsible for FRAML placed much more importance on both—especially manual processes.

Data silos are important to FRAML teams because those responsible for Risk & Compliance management care deeply about reducing investigation times, streamlining workflows, and improving the overall efficiency of how these AML tasks are carried out.

Ultimately, while there are overlapping challenges between the teams, the nuanced differences in their core functions result in varied priorities. For optimal efficiency, organizations must understand these distinctions and equip each team with tailored tools and strategies.

2. Keeping Pace with Growth and Regulatory Evolution

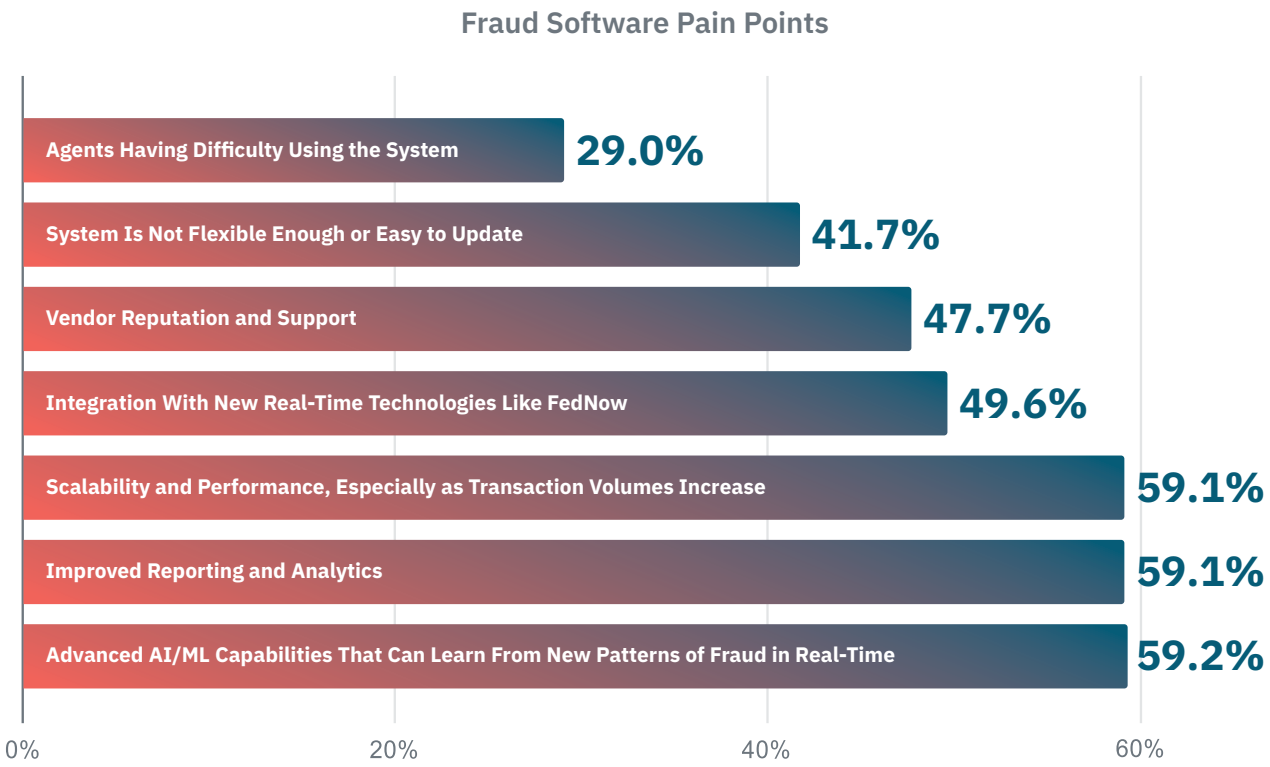
The contemporary financial landscape places enormous demands on companies' Risk & Compliance infrastructure, underlining the importance of adeptness in fraud and AML operations. Yet, most companies struggle with challenges when honing these tools to achieve optimal results.



Compliance Dynamics: AML regulations are in perpetual flux. A staggering 59% of respondents identified compliance with these ever-changing regulations as a major challenge. Not only do these shifts make adherence strenuous, but they also necessitate a flexible solution that can swiftly adapt its rules to mirror the current compliance landscape.

Efficiency and Timeliness: Time is of the essence. Delays in adapting to new regulations or inaccuracies in refining software rules can expose organizations to hefty fines and penalties. A software's inability to adjust rapidly may inadvertently bypass new AML regulations or, worse, spew a barrage of false positives.

Productivity through Automation: Manpower is valuable. The ability to automate, especially in alert management, is a cornerstone to improving productivity. With alert automation, suspicious activities can be swiftly flagged, and alerts can be prioritized, scored, and escalated with urgency. This ensures that efforts are channeled effectively into the investigation and resolution of genuine threats.

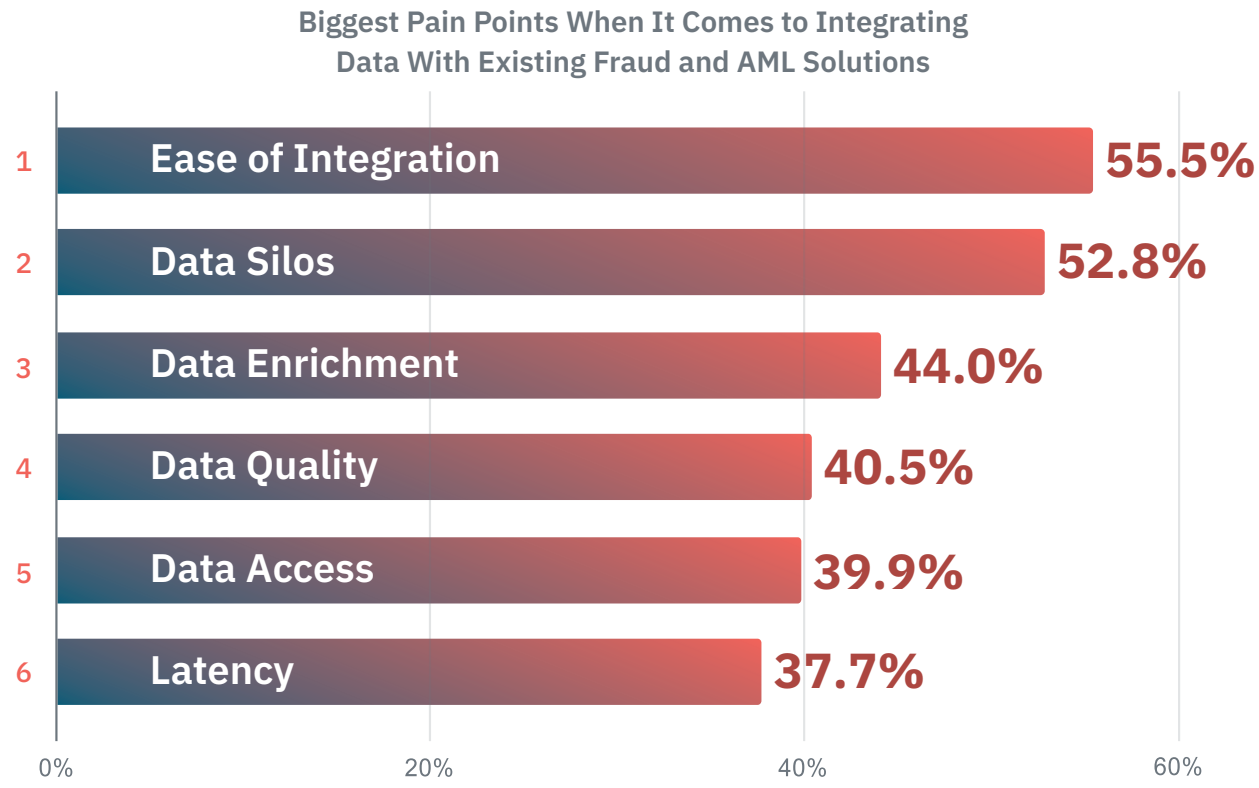


Scalability and Growing Pains: Growth should be liberating, not stifling. As companies expand and transaction volumes surge, many feel shackled by the fraud systems meant to protect them. This issue is magnified when these systems are bespoke creations. Last year's data revealed that 51% of organizations employ in-house built systems, often rigid and difficult to revamp as the operational landscape evolves and the enterprise proliferates.

Shifting Behavioral Patterns: As companies balloon, customer behavior isn't static. Previously efficient rules with high fraud catch rates can suddenly become counter-productive, churning out false positives due to shifts in user behaviors. This necessitates an ongoing recalibration of the rule sets. Fresh rules must be introduced, while outdated ones need phasing out.

Efficiency through Rule Automation: A superior risk management framework not only thwarts fraud but also scales seamlessly alongside company growth. By automating rule management—including the inception, discontinuation, and optimization of rules—teams can boost their efficiency. This redirection of resources ensures that the focus remains on investigating and acting upon legitimate threats.

3. Navigating Fragmented Data Systems



The modern Risk & Compliance arena poses a pivotal challenge: unifying fragmented data for actionable insights. While data quality remains essential, it's the accessibility and integration of data that are currently at the forefront of professionals' concerns, with 55% of respondents acknowledging that ease of integration and siloed data are key problem areas.

The Challenge of Data Silos

Beyond Data Quality
Today, having impeccable data isn't the sole requirement. The utility of accurate and detailed data diminishes if it's trapped within isolated silos, forcing analysts on a wild goose chase across multiple systems.

Unifying Data for Clarity
For teams to harness the full potential of their data, it's imperative to have a consolidated repository. This centralized approach not only streamlines analysis but also empowers professionals to derive actionable insights by painting a comprehensive picture.

The Essence of Integrated Solutions in Fraud and AML

The Quest for the Right Tool
Financial establishments need solutions equipped with ready connectors for various data types, adeptness in using APIs for fluid data exchange, and transparent guidelines for accurate data mapping and transformation.

Diverse Data Sources
AML and fraud solutions thrive on multiple data sources, spanning transaction data, customer profiles, and external third-party data. The crux is in seamlessly amalgamating this information and presenting it in an intuitive format to aid decision-making.

The Gap Between Vendor Promises and Reality

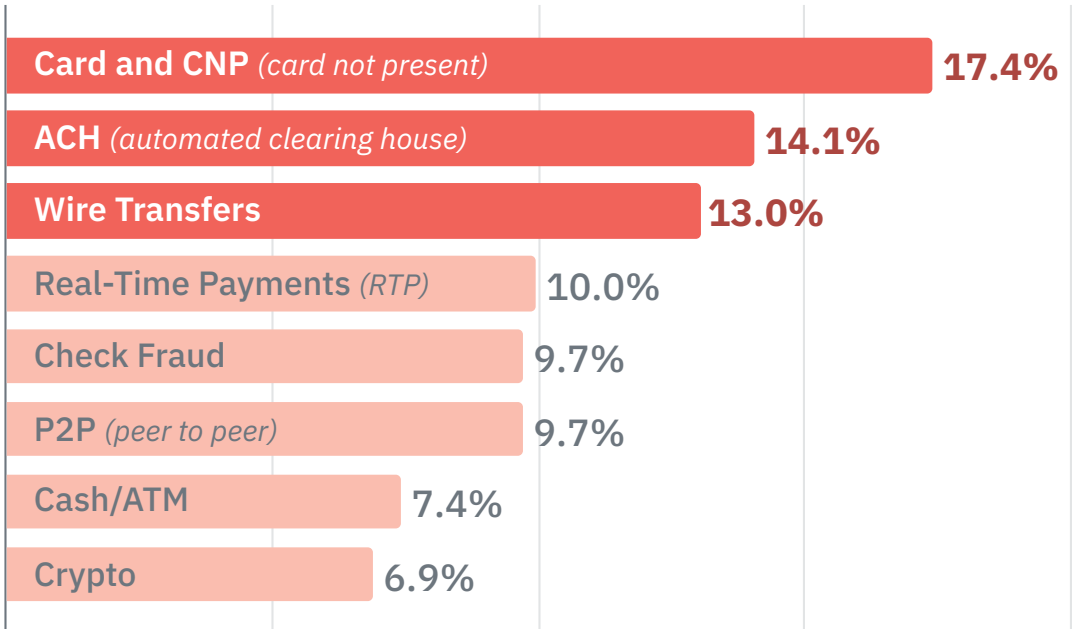
The Mirage of Data-Agnostic Systems
A while many vendors say their platforms are data agnostic with user-friendly integration, the reality often paints a different picture. Many of these solutions falter regarding custom data integrations, saddling users with prolonged, cumbersome setup processes.

Translating Data for Readability
Even if some systems can wrangle custom data, they often stumble in converting this into user-friendly formats. Given this landscape, it becomes paramount to prioritize customization capabilities, ensuring that the chosen software can genuinely cater to an organization's unique data integration requisites.

4. Addressing Fraud Across Varying Payment Rails

It's extremely challenging for teams to prevent fraud and money laundering if they don't know where that suspicious activity occurs. Since fraud often occurs at the point of the transactions themselves, pinpointing the most affected payment methods is essential. This not only helps in detecting the primary areas of fraud but also aids in devising effective strategies to counteract and reduce it.

Top Payment Rails Where Fraud Occurs



- **Card and CNP** *(card-not-present)* were the most common payment rails that experienced fraud; which is no surprise considering payment cards are one of the most common (and trusted) payment methods.
- **ACH** and **wire transactions** are also popular rails for fraudsters, who likely exploit the settling period used for clearing these transactions.

- **P2P** and **real-time payments** are appealing to fraudsters because the transaction is often irreversible, but they aren't quite as favored because it's much harder to actually exploit these systems without gaining direct access to someone's account.
- Despite adopting more modern (and often digital) payment methods like **RTP, P2P,** and **CNP, check fraud** is still a popular option, as the system still has some of the same weaknesses it's always had, such as forgery.

As consumers lean more towards quick, digital payment methods, real-time transaction monitoring becomes crucial. Recognizing the most exploited payment methods is essential in devising counter-strategies.

5. Lack of Engineering Support

Engineering support is often a critical component of any team's Risk & Compliance infrastructure, as it is required to ensure systems are up-to-date and operating at peak efficiency. Overall, we saw positive movement where now 91% of teams are getting some form of engineering support (as opposed to the 82% reported last year)...

However, 58% of organizations still can't offer more than 15 hours of internal engineering support for their Risk & Compliance teams, which is woefully under what's required to meet demands.

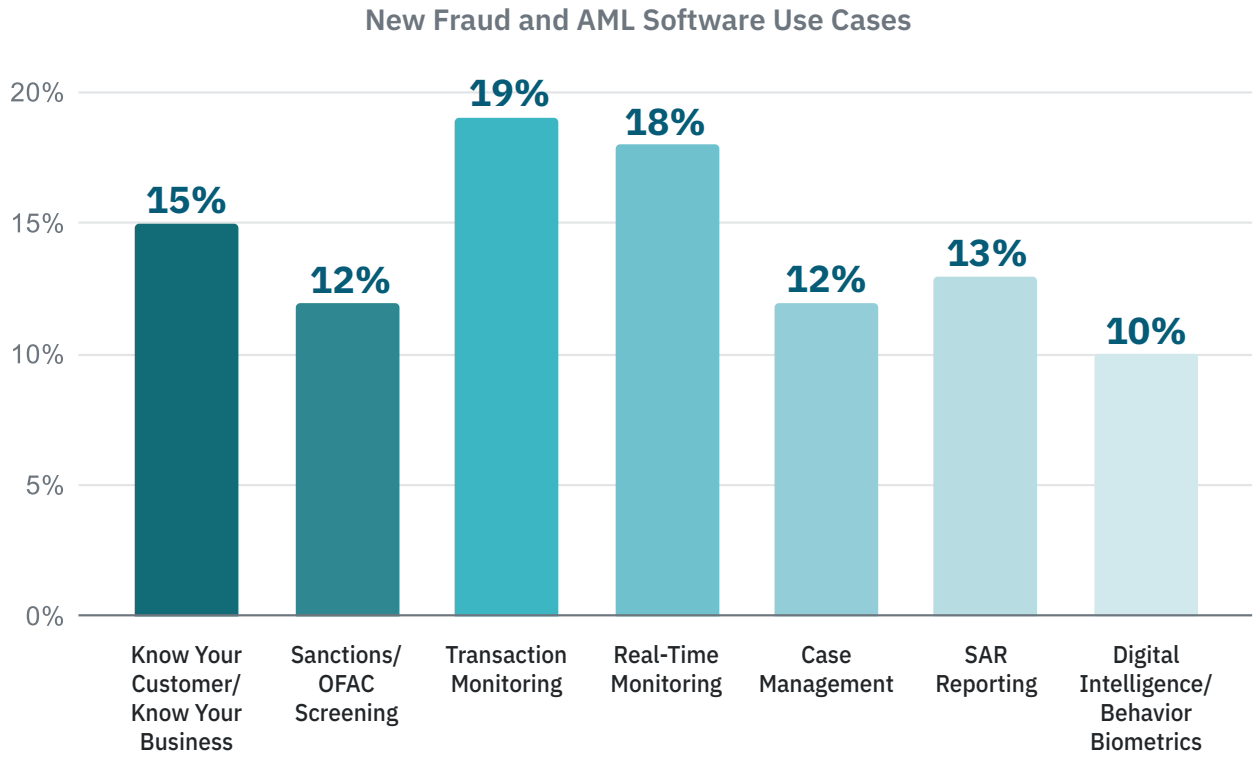
After all, once fraud schemes and money laundering threats are identified, Risk & Compliance teams need to develop new rules and update their system to check for—and act on—these threats properly. As noted earlier, this challenge is greatest for organizations with complex, internally built solutions or for those using inflexible legacy software that cannot be updated without the use of code.

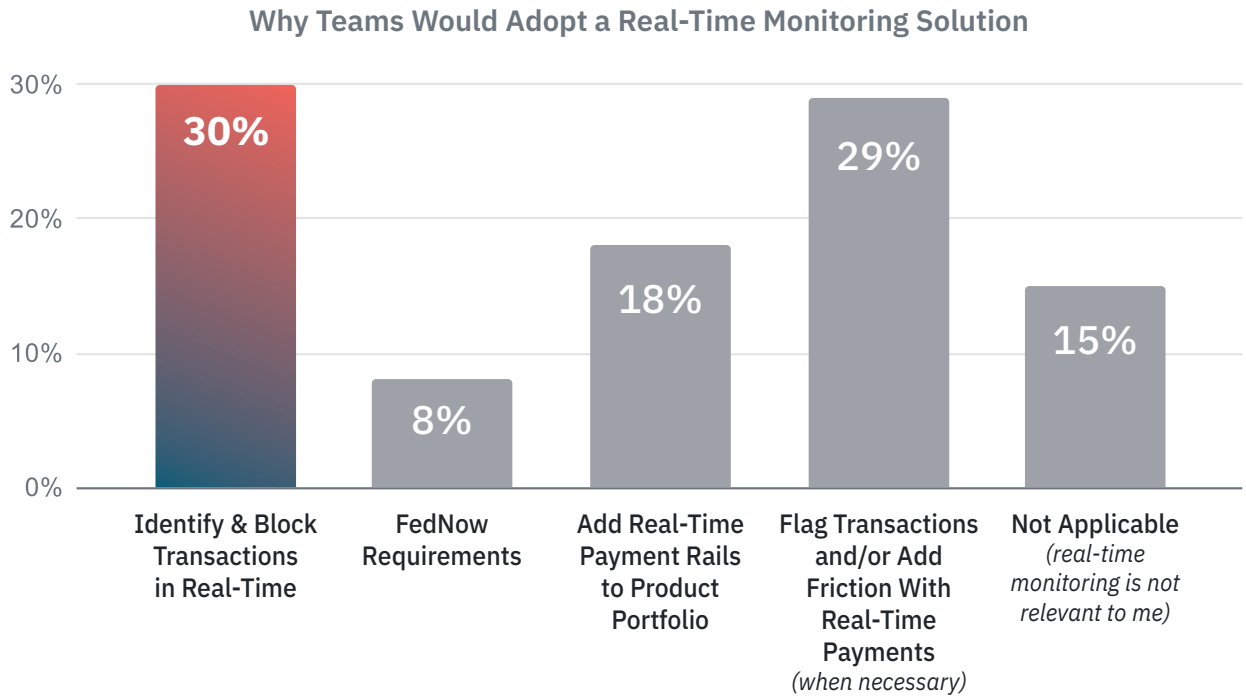
Two potential solutions exist: either invest more in manpower or transition to a system requiring minimal engineering involvement.

Use Cases for Software

Real-time Monitoring: A Top Priority in Risk & Compliance

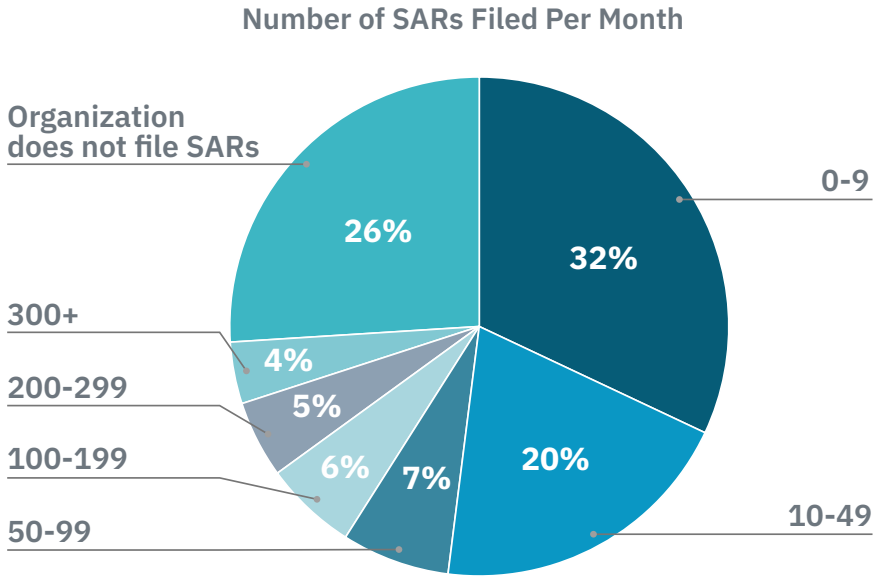
In today's rapidly advancing digital landscape, the urgency of monitoring and acting upon suspicious transactions as they occur cannot be overstated. Real-time transactions are essentially irreversible. Once a fraudulent activity has been processed, the chances of recovering those funds diminish significantly. This has led transaction and real-time monitoring to stand out as the most vital features of a fraud and AML solution.



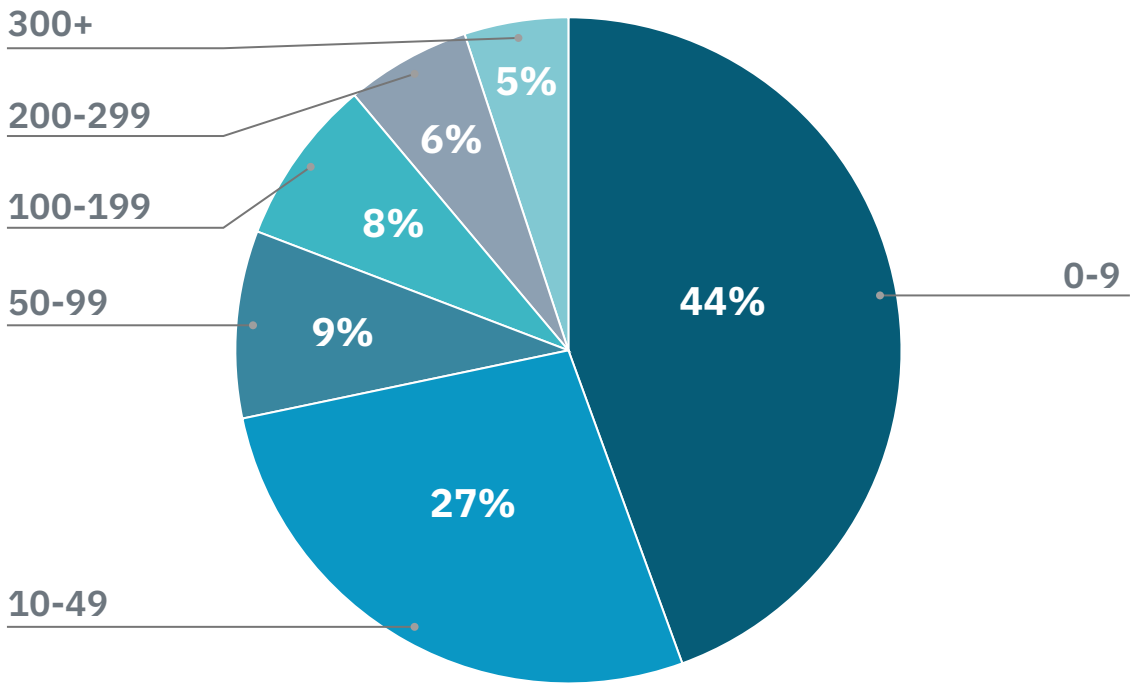


Addressing Repetitive Tasks with Automation

The reality of the current financial landscape is illustrated by the fact that a substantial portion of Risk & Compliance teams have to file numerous Suspicious Activity Reports (SARs) every month. The sheer volume of this activity—some organizations filing 300+ SARs monthly—indicates the high level of suspicious activities being flagged.



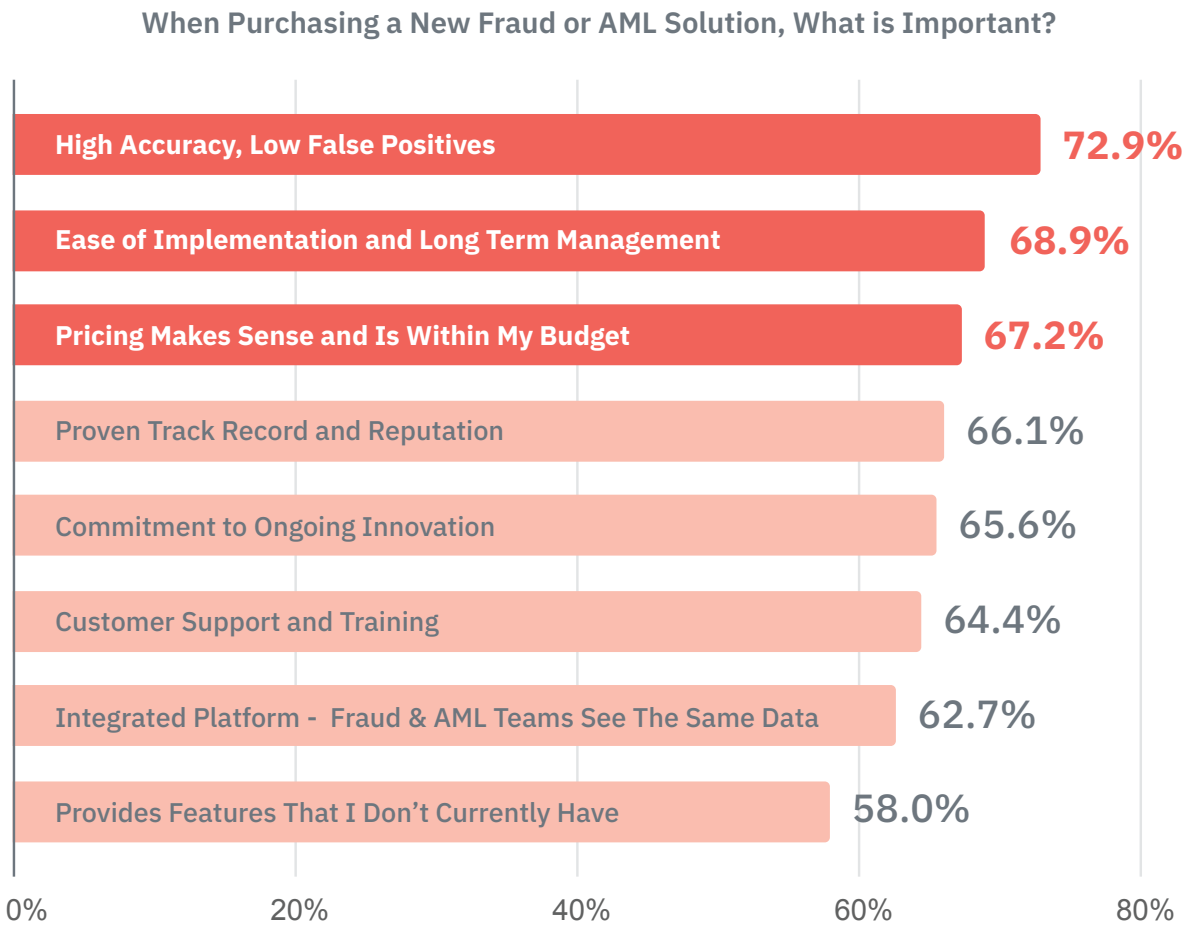
Number of SARs Filed Per Month by Organizations That File SARs



Of those who file SARs with their organizations, 29% file 50 or more SARs per month.

The repetitive nature of tasks like sanctions screening and SAR reporting can drain resources. If your organization is filing 50 or more SARs each month, then automating this process can lead to significant time and cost savings. The time conserved can then be redirected towards investigating and addressing legitimate cases of suspicious activity.

Choosing the Right Solution: What Matters Most?



When venturing into the market for a new fraud or AML solution, three major considerations come into play:

Accuracy & Efficiency: The system should offer data precision combined with low false positive rates. This not only streamlines operations but also optimizes resource allocation.

Ease of Setup & Maintenance: A seamless implementation process, paired with hassle-free long-term management, is critical. No organization wants to be bogged down by complicated integration processes or continuous rule updates.

Cost Consideration: It's a myth that top-tier fraud and AML systems are only about high costs. While there's an investment involved, the repercussions of fraud and compliance failures can overshadow this initial outlay. The right system can offer returns many times over its price.

It's a balancing act, but teams often lose more to fraud and compliance failures than they realize because they don't want to invest in the upfront costs of having a high-quality fraud and AML system.

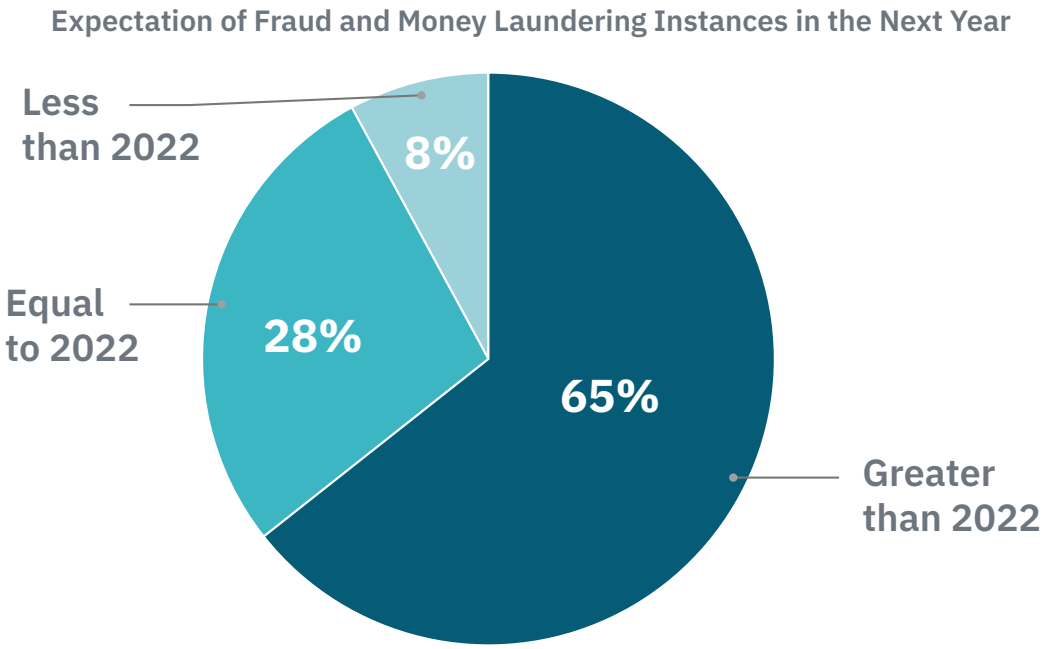
A Fraud Prevention Success Story: PrizePool

It's not all theoretical. PrizePool's experience showcases the tangible benefits of effective transaction monitoring. By leveraging advanced features, the company managed to thwart over $500,000 in fraudulent transactions. Given that every dollar of fraud can cost U.S. financial institutions $4.23, the savings from a robust Risk & Compliance infrastructure are evident.

The challenges of the modern financial world demand sophisticated, real-time solutions. While the upfront costs of such systems might seem daunting, the long-term savings, both in terms of finances and resources, make the investment worthwhile.

Future of Fraud and AML

Rising Challenges in Financial Crime

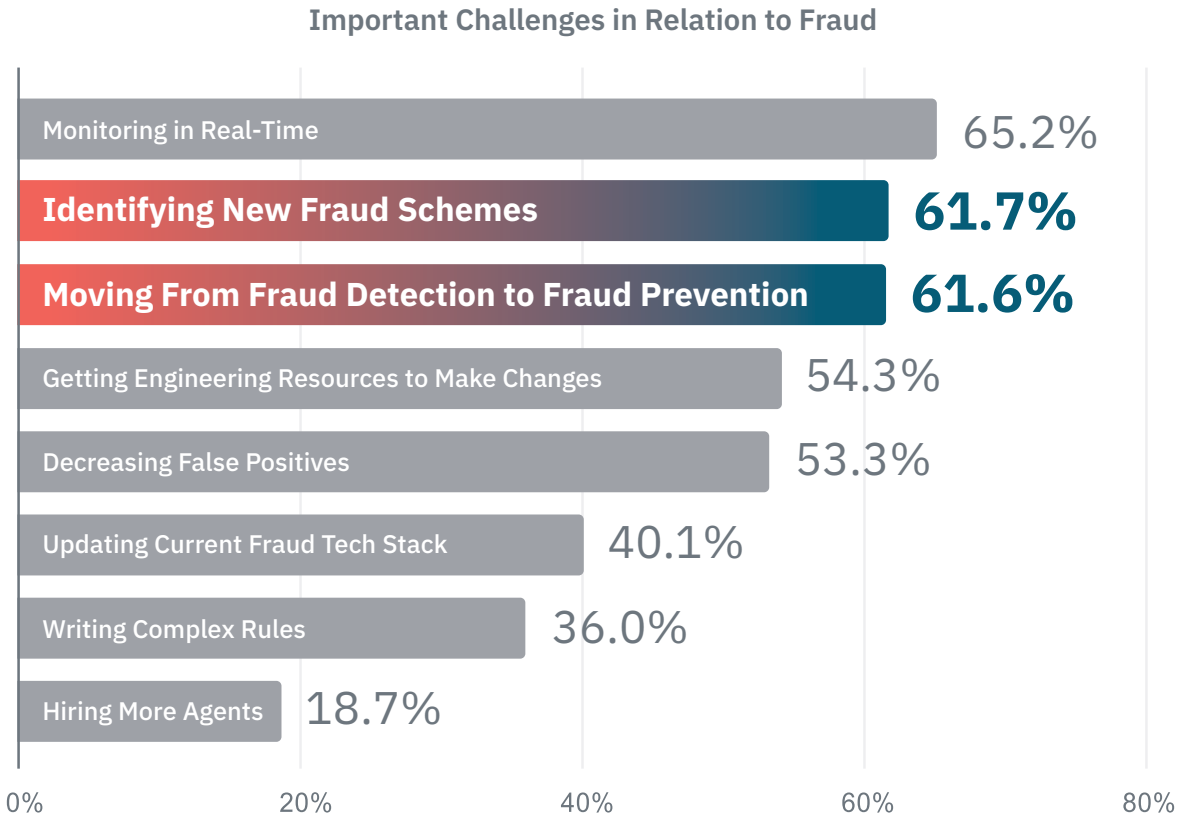


65% of respondents expect fraud and money laundering cases to increase in the next 12 months.

Growth Expectation: A majority of industry experts anticipate an uptick in financial crime in the next 12 months. As technology advances, so do the techniques and methods adopted by nefarious actors.

Adapting to Tech Changes: With the advent of P2P and real-time payment solutions, there's a burgeoning opportunity for fraudsters to exploit these innovations.

Shift From Fraud Detection to Prevention



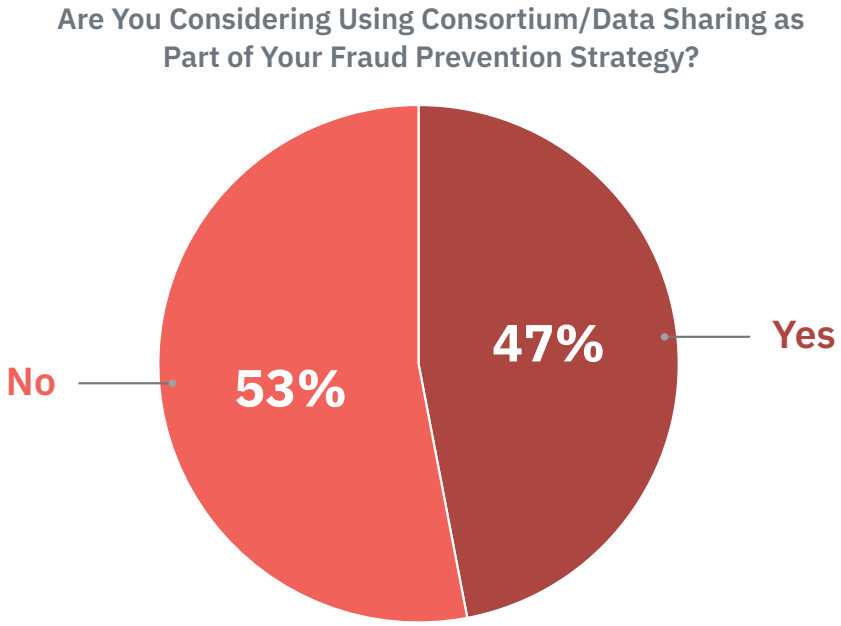
61.6% of respondents said moving from detection to prevention was one of the most important challenges for them.

Instant payment methods are in demand, but they bring challenges. The swifter these methods, the trickier it becomes to prevent fraud.

A reactive approach isn't enough. The emphasis is on proactive prevention by understanding customer behaviors, spotting inconsistencies, and then using this data to build controls to block actions related to this anomalous behavior. It's also critical to be able to think like a fraudster. Knowing their motives and the strategies they might deploy to commit crime can help fraud teams anticipate threats before they occur.

However, as we've discovered in this year's report, fraud teams are tied up with inflexible systems, minimal engineering resources, siloed data, faster payment rails, and increasing avenues for bad actors to commit fraud, it becomes very clear why moving from detection to prevention is difficult yet critical.

The Power of Shared Data



47% of respondents said they would consider using a fraud prevention data-sharing consortium as part of their prevention strategy.

Close to half of those surveyed are open to fraud prevention data-sharing consortiums. Such platforms are game-changers, transforming detection processes into prevention mechanisms.

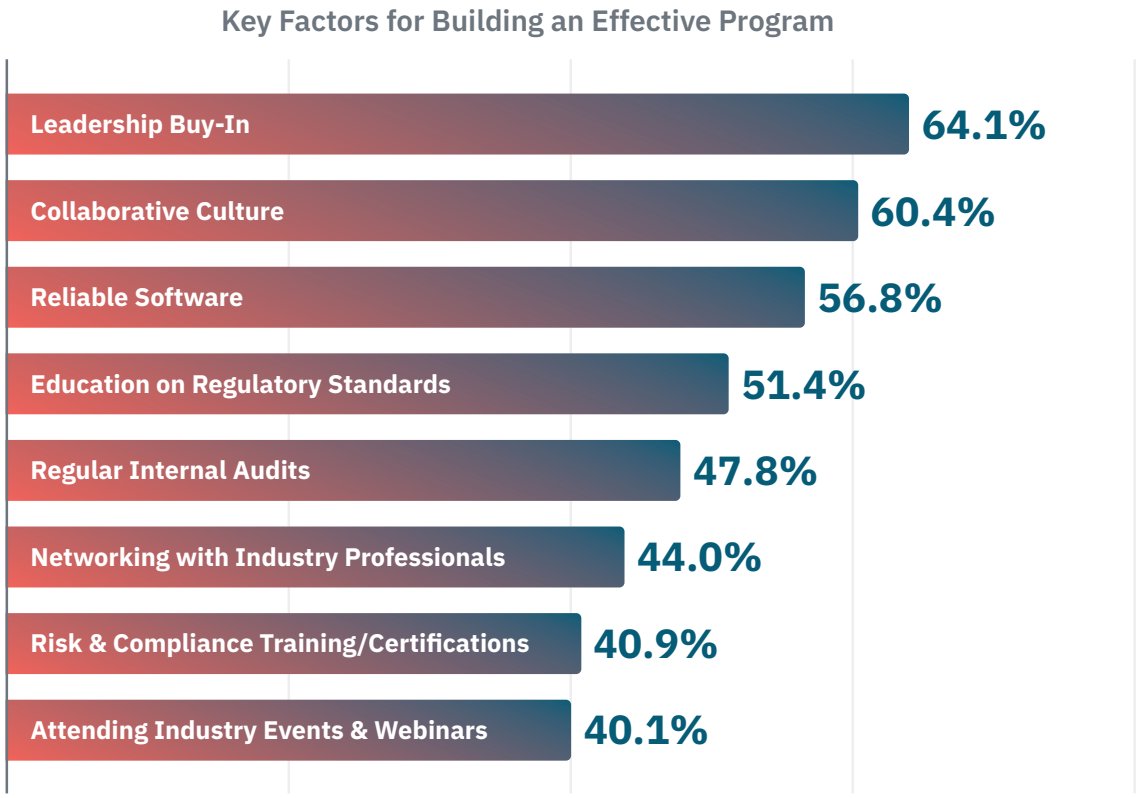
Criminals don't operate in a vacuum—they transcend channels of communication and reach multiple FIs, looking to exploit weaknesses wherever they exist. Fraudsters frequently share information with each other over secret chat forums, the open web, and social media platforms to gain an advantage over the businesses they intend to target.

If criminals will share information and resources, why shouldn't the organizations looking to stop them? With fraud detection done by a partner company, teams can use shared data to jump immediately to

preventing fraud—and help other companies do the same.

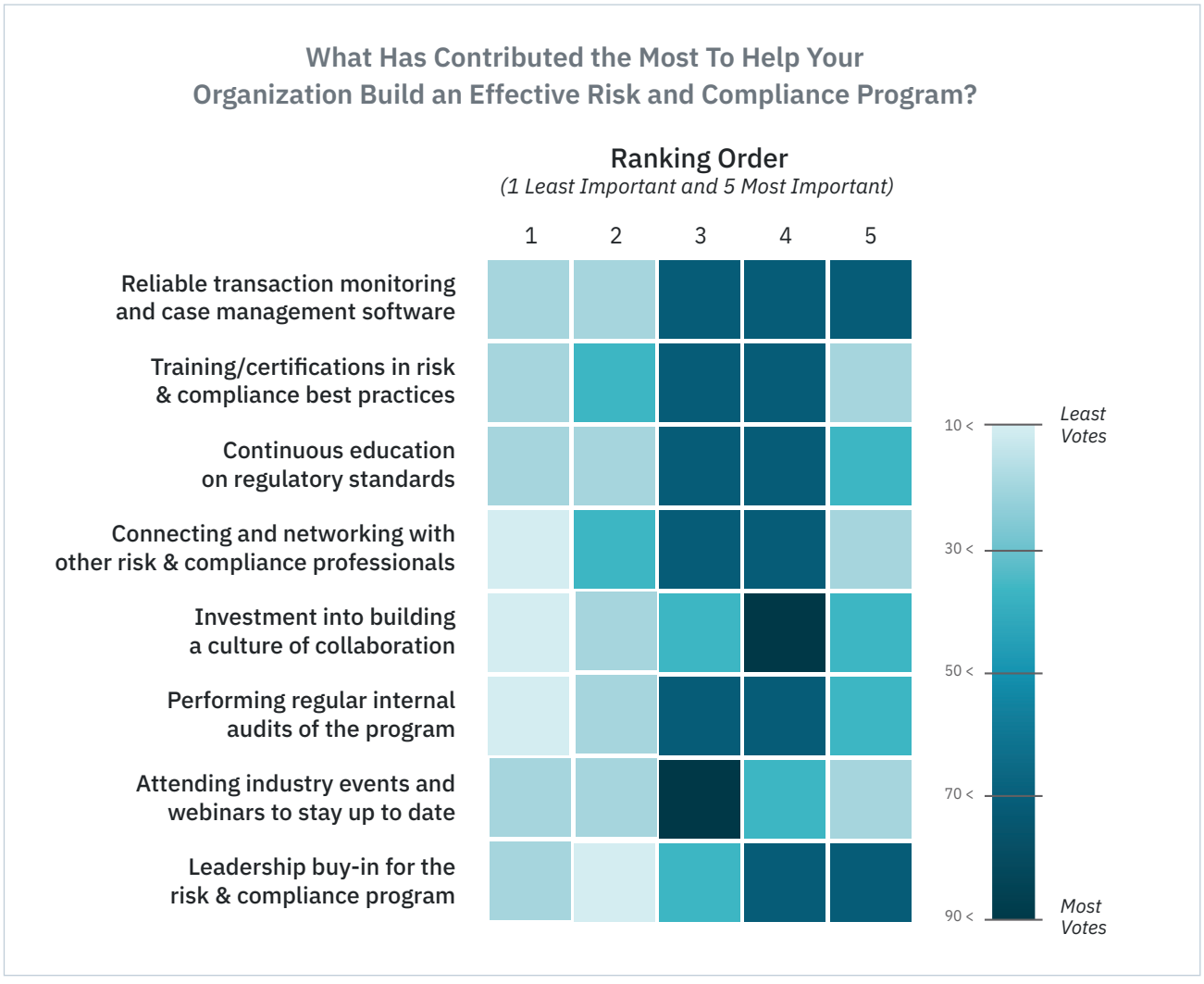
Data sharing capabilities are extremely valuable in cases where transactions are irreversible—such as P2P and real-time payment solutions—as they allow teams to actually use shared information to prevent real-time payments that would otherwise be unstoppable.

Building an Effective Risk & Compliance Program



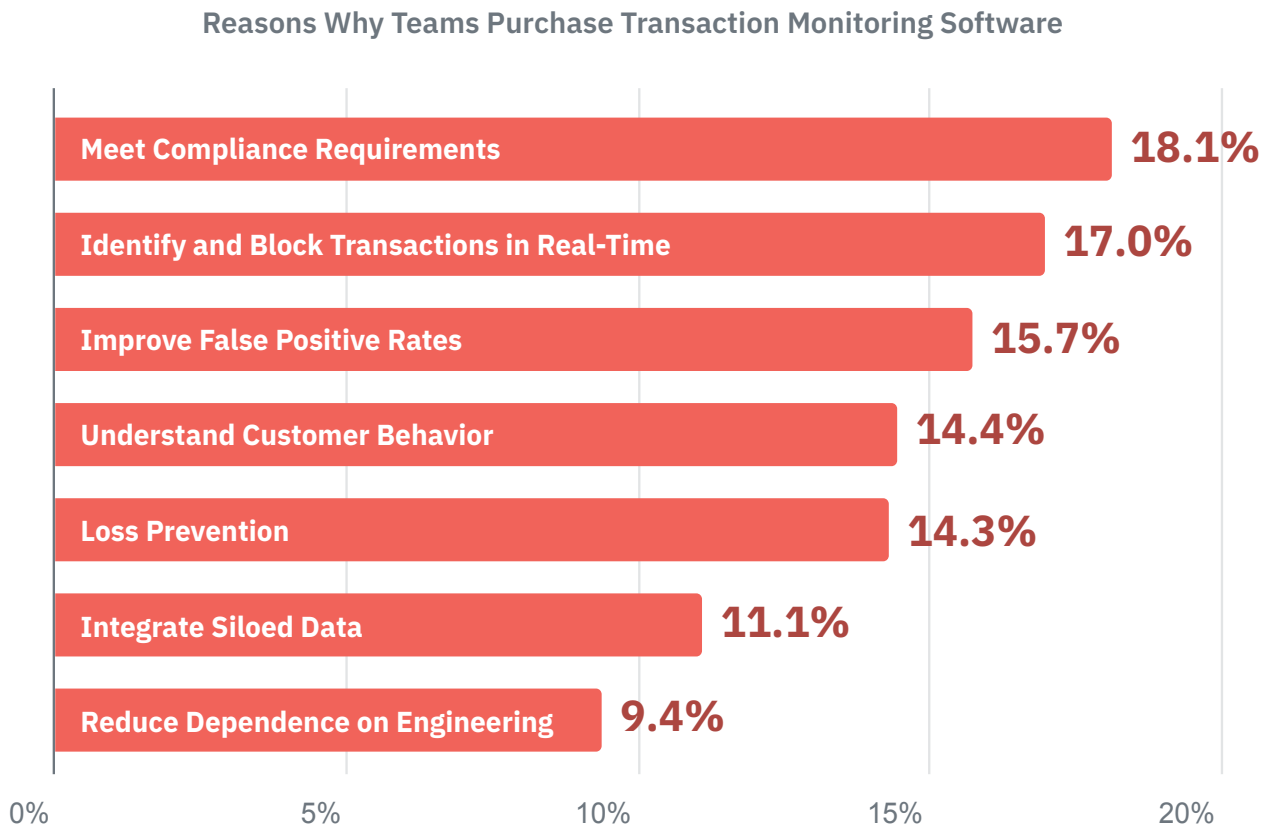
64% of respondents said that leadership buy-in for the risk & compliance program is what has contributed the most to helping their organization build an effective risk and compliance program.

The future of fraud and AML is evolving rapidly. While challenges mount, so do innovative strategies and technologies to curb financial crime. The key lies in collaboration, proactive prevention, and leveraging the right tools.

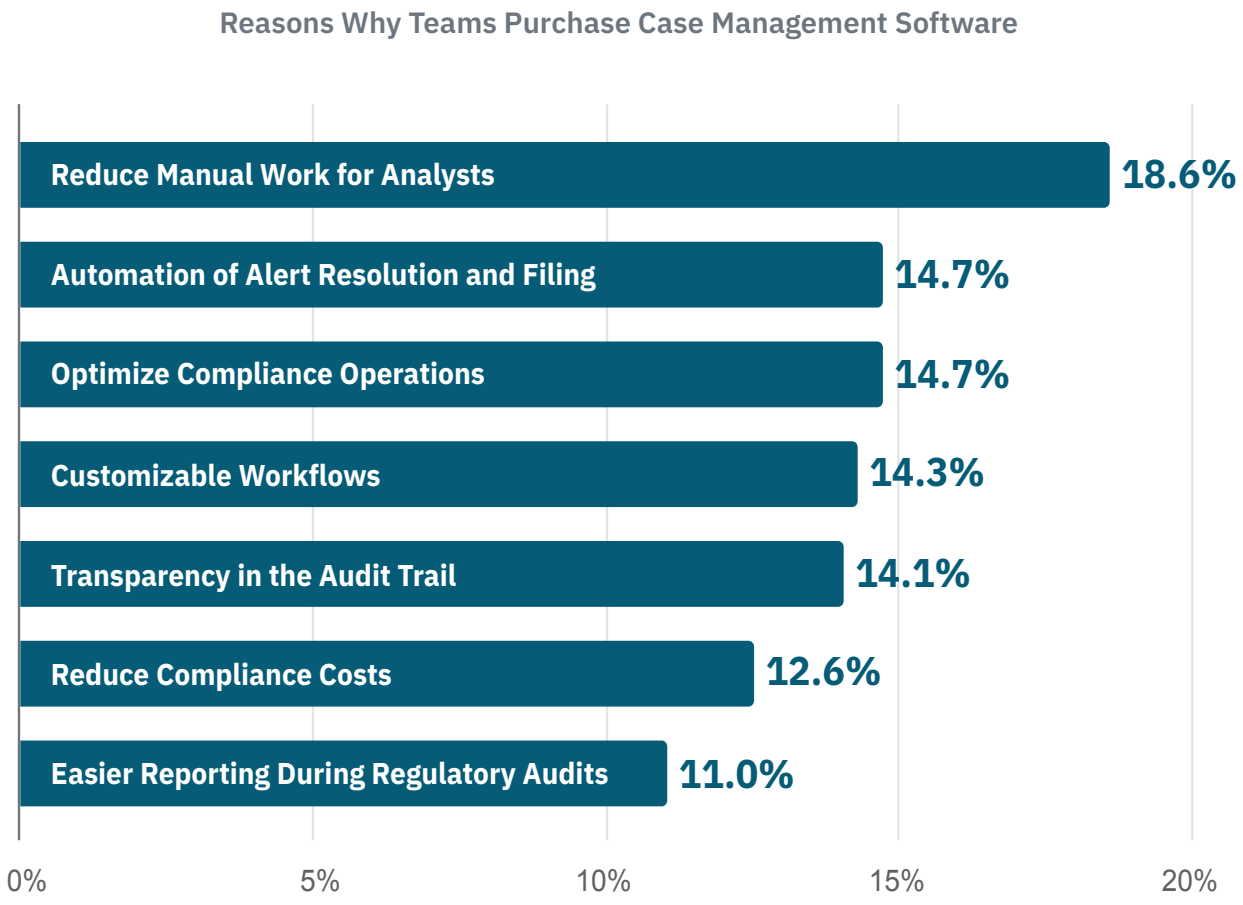


Top Contributors: Leadership buy-in and a cooperative culture are pivotal. Without support from the top and collaborative efforts, risk and compliance objectives remain challenging to achieve.

The Role of Technology: 57% stress the importance of reliable transaction and case management software. Such tools are not mere aids—they are foundational to compliance and risk management.



Transaction monitoring helps teams meet compliance requirements, identify and block transactions in real-time, prevent losses, and provide teams with more data to make informed decisions.

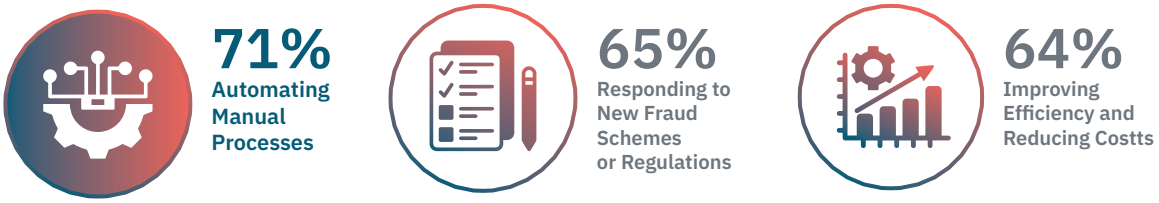


Case management tools reduce manual work for analysts, customize and optimize workflows, automate alert resolution and filing, improve fraud and compliance operations, and reduce costs.

Final Takeaways for Organizations

Manual Processes are a Detriment to Success

Top Priorities for Risk & Compliance Professionals

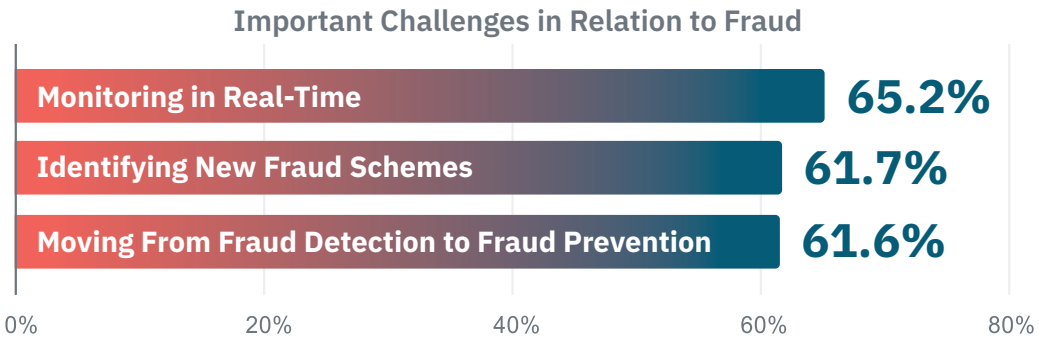


According to this year's data, the primary impediment to efficiency in Risk & Compliance teams is manual processes. Increasing headcount alone fails to elevate productivity cost-effectively. Automation, on the other hand, is the game-changer. It drastically reduces manual work, thereby allowing teams to focus on more sophisticated tasks.

How Unit21 Can Help

- **Filing Automation:** Automate and streamline CTRs, SARs, and other filings.
- **Workflow Automation:** Set up custom workflows and verification processes both inside and outside the system.
- **Decision Automation:** Eliminate repetitive decisions by crafting rules for auto-execution.
- **External Action Automation:** Facilitate tasks within your system based on external triggers and vice versa.
- Embrace automation to equip investigators to work faster and more efficiently and focus on strategies that genuinely prevent financial crime.

Moving From Fraud Detection to Prevention is a Necessity



While detection is pivotal, a proactive approach towards fraud prevention minimizes post-event losses. For this shift to be effective, Risk & Compliance teams need insights to assess threats and craft preemptive rules.

It's an iterative process that involves analyzing data from their fraud detection efforts and then leveraging that knowledge to develop prevention strategies and systems.

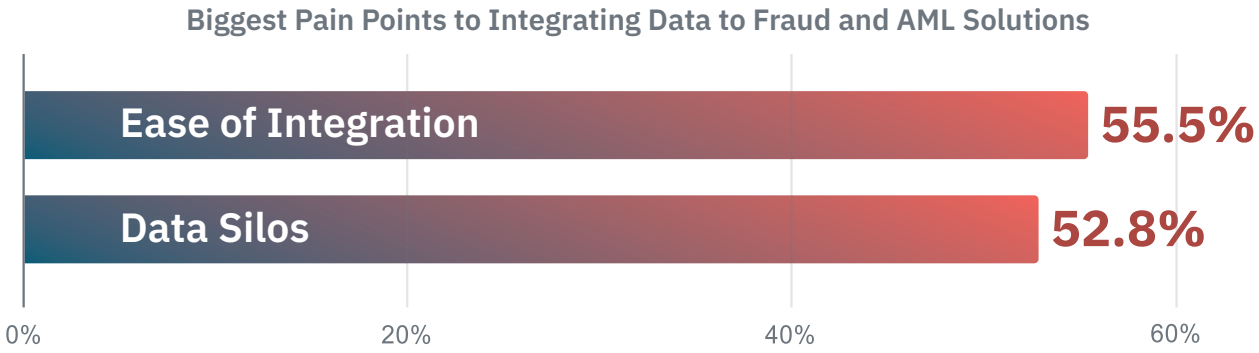
Fraudsters take what they can from one platform and then move to another.

This is why 47% of respondents to this survey said they'd consider using a data consortium. To enhance the chances of preventing fraud, companies must exchange information (not hide it) to learn and benefit from collective experiences.

How Unit21 Can Help

- Unit21 has created a **trusted data-sharing consortium**, which allows teams to share information on fraudsters and gives Risk & Compliance teams the ability to immediately jump to prevention by blocking bad actors that other companies have already had run-ins with.
- We also offer **real-time monitoring solutions** to help fraud teams identify and block suspicious transactions in 250 milliseconds or less.

Data Is Only As Powerful As Your Ability to Wield It



High-grade data forms the bedrock of fraud and money laundering prevention. However, siloed data systems that are difficult to integrate with can stymie timely and accurate decision-making.

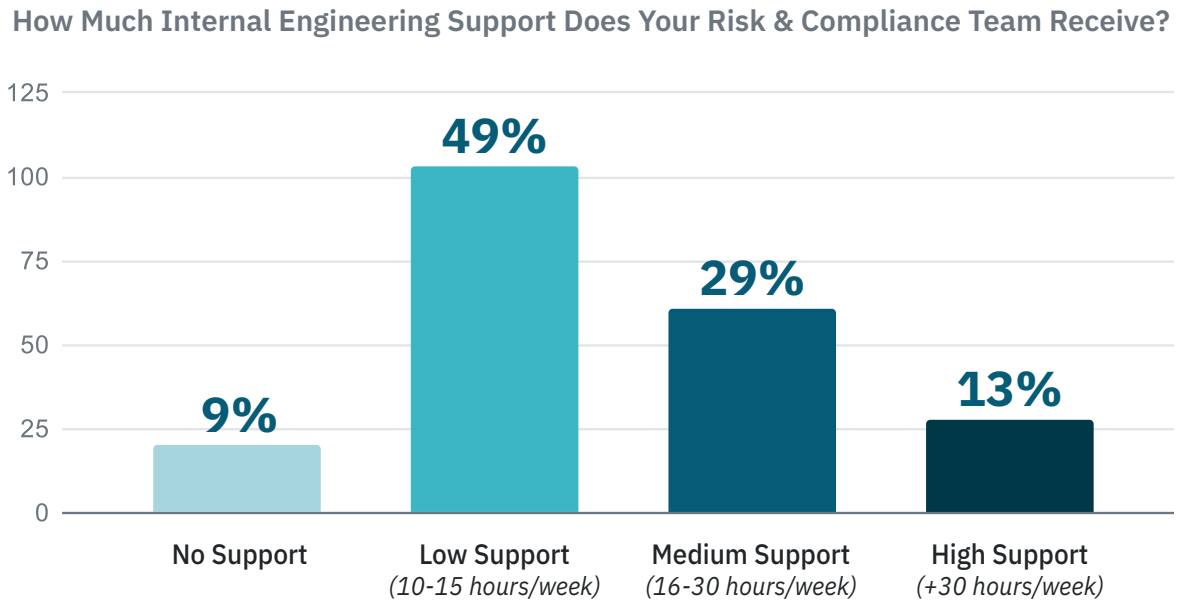
Too often, Risk & Compliance teams must sift through siloed data across various systems to piece together the full picture.

Consolidating data and integrating effectively remain essential.

How Unit21 Can Help

- With Unit21's **robust integration capabilities**, you can easily connect and ingest data from various sources without rigid data formatting, enabling quicker adoption and eliminating the need for extensive customization. By incorporating a wide range of data sources, you can create a more holistic view of your risk landscape.
- Additionally, our **self-service approach** gives organizations more autonomy in configuring our infrastructure, further enhancing the efficiency of the implementation process.

Engineering Support: A Gap that Needs Bridging



With a staggering 58% of Risk & Compliance teams having 15 hours or less of engineering support weekly, the challenge is clear. However, a solution that's easy to update without extensive engineering is the key.

How Unit21 Can Help

- Unit21's **no-code configuration** eliminates the need for lengthy deployment cycles by empowering users to set up, test, and validate rules without relying on engineers.

Reliable Transaction Monitoring and Case Management Software Remain Critical

Aside from obtaining leadership buy-in and working in an environment that prioritizes collaboration, it is clear from the survey responses that having reliable tools in the form of transaction monitoring and case management is critical for success.

Last year, 59% of risk management professionals listed it as a leading factor in building a compliant fraud and AML system, and this year, it is once again in the top 3 when it comes to building a successful Risk & Compliance program, with 57% of respondents listing it as a top contributor to their program.

How Unit21 Can Help

- Unit21's infrastructure helps Risk & Compliance teams stay compliant and prevent fraud. Our users have **reduced false-positive rates by 85%** and have **reduced investigation times by over 78%** after adopting our solution.

About Unit21

At Unit21, we believe that combating financial crime demands a united front. By harnessing the full potential of data, streamlining workflows and bringing teams together, our Risk & Compliance infrastructure takes on fraud and anti-money laundering gaps with precision.

Our adaptable risk engine and versatile case manager empower fraud and AML teams to wield expert data analysis without the need for extensive engineering support. This resonates seamlessly with the ever-evolving landscape of financial crime prevention.

In 2022 alone, we monitored a total of 4.8 billion transactions at a value of $693 billion, handling over 16,000 suspicious activity reports and prevented more than $760 million in fraud attempts. In addition, our newest initiative, the Fraud DAO consortium, which enables FIs to pool and share data, now monitors more than 10% of consumer transactions in the US, establishing Unit21 as a guardian of the financial ecosystem.

Uniquely positioned to solve the problem of financial crime and well-funded, we have raised close to $100 million from Google, Tiger Global, ICONIQ Capital, Jack Dorsey, Diane Greene and other leading VCs. We're on a mission to unite the world's fraud and AML heroes in order to see the financial ecosystem restored to the pathway of opportunity it was meant to be.