Unit21

4 Trends in Fintech to Combat Fraud

FROM THE 3RD ANNUAL STATE OF FRAUD & AML

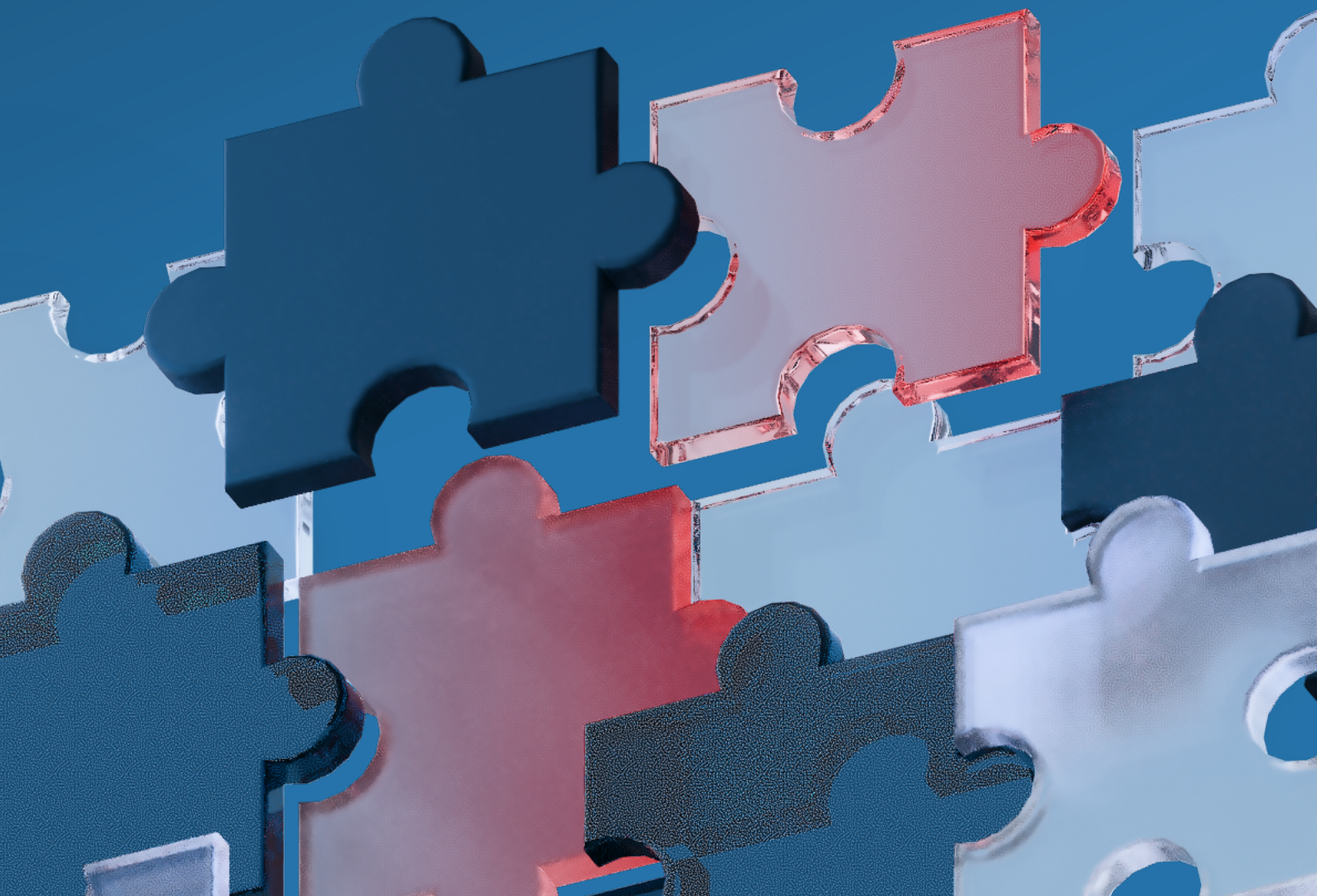
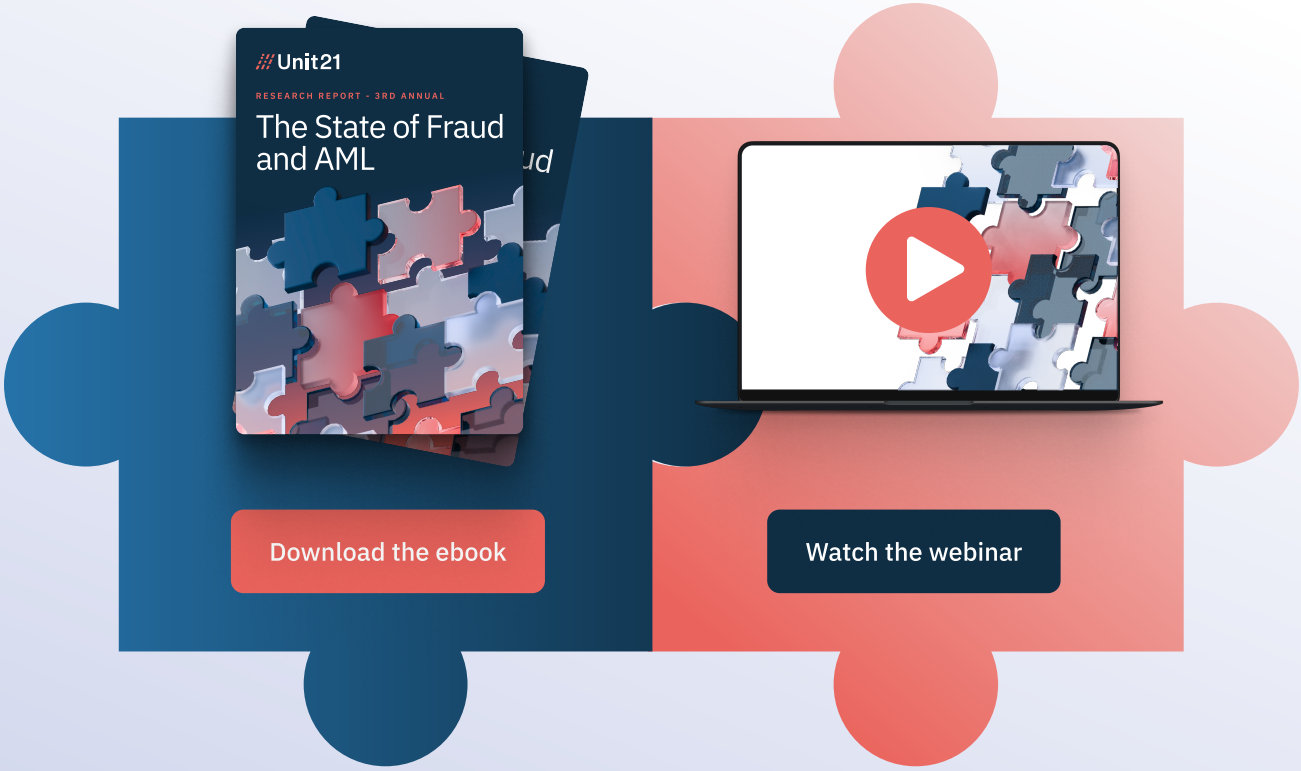


Table of Contents

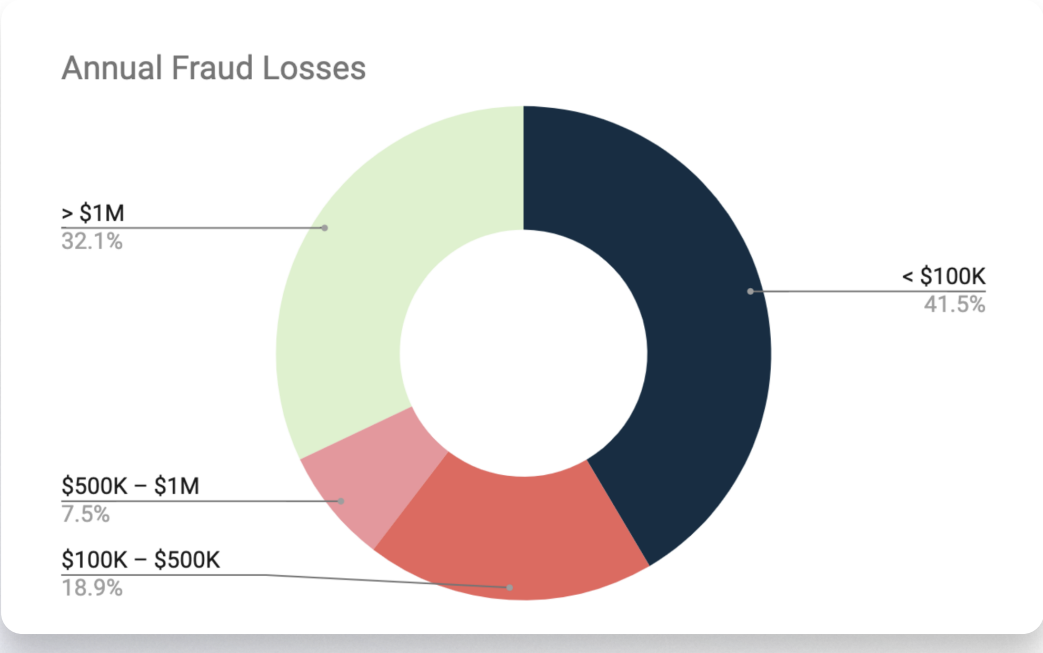
The Big Picture	03
The Scam Surge - A Growing Threat	05
The Hidden Costs of Fraud Prevention	08
Real-Time Monitoring: A Competitive Advantage	11
AML Remains a Resource-Intensive Challenge	13
Who Did We Survey?	15

Unit21's 3rd annual Fraud and AML Survey report delves into the evolving landscape of fraud and AML and the ever-present challenges facing financial institutions and fintech companies. We surveyed 350 financial professionals in fraud, AML, and FrAML across banks, credit unions, and fintech. This brief focuses exclusively on findings and trends in the fintech sector, which amounted to 215 survey responses.

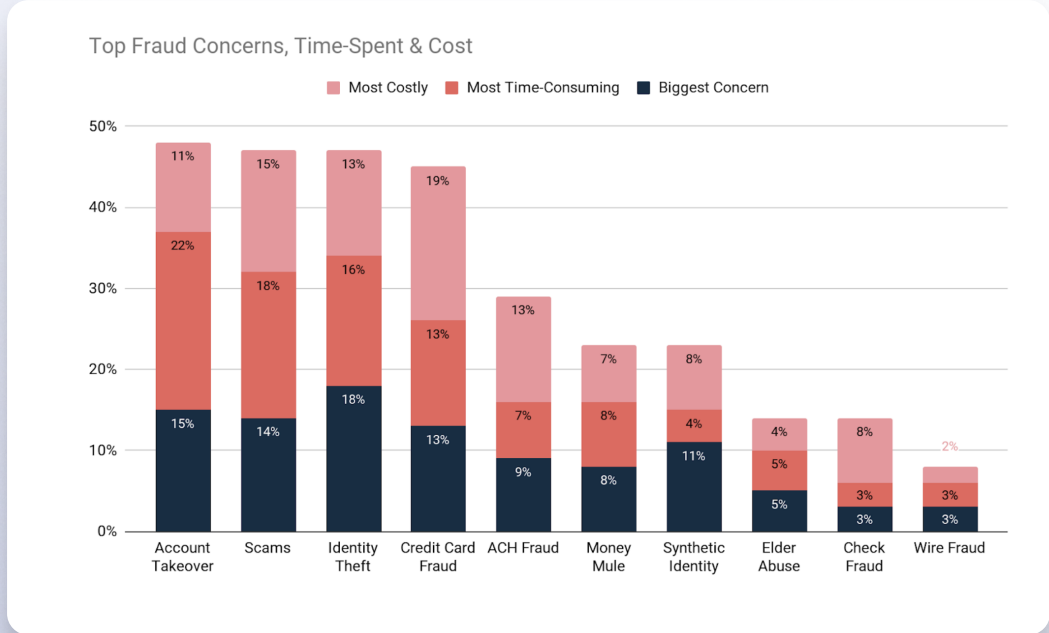


The Big Picture

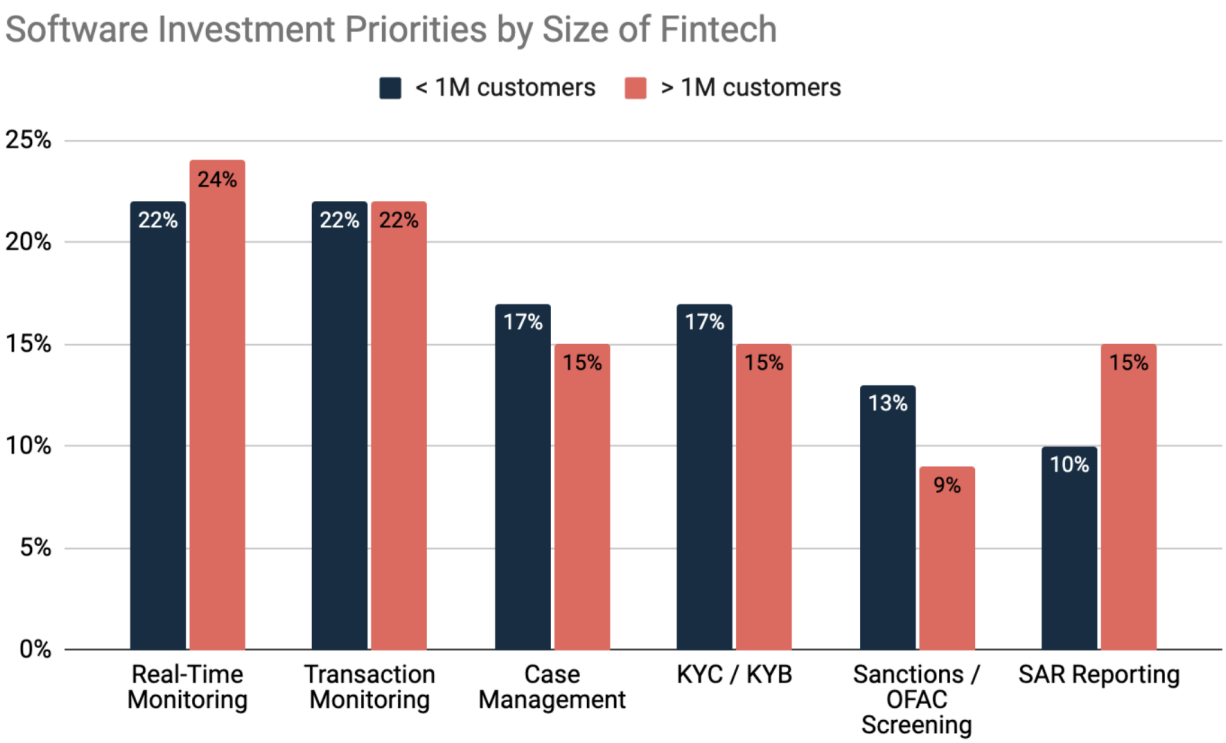
Fraud continues to plague the financial services industry, and fintechs are no exception. Payments are moving faster than ever, and fraudsters are constantly evolving their tactics. Fintechs are seeing a surge in scam activity and are facing constraints due to the burden of AML. Many are seeing large false positive rates and bottlenecks when deploying new rules. Some are using Real-Time Monitoring (RTM) to combat operational inefficiency and assist in catching fraud. Others are combining fraud and AML teams to help. Despite all this, Fintech is still seeing large fraud losses, with more than a quarter of respondents stating losses above $1 million.



Identity Theft was a top concern for Fintech, with Account Takeover and Scams not far behind.



Fintech companies rated Real-Time Monitoring (RTM) as the highest priority (23%) if they were to purchase software within the next 12 months. Right behind that was transaction monitoring at 22%.

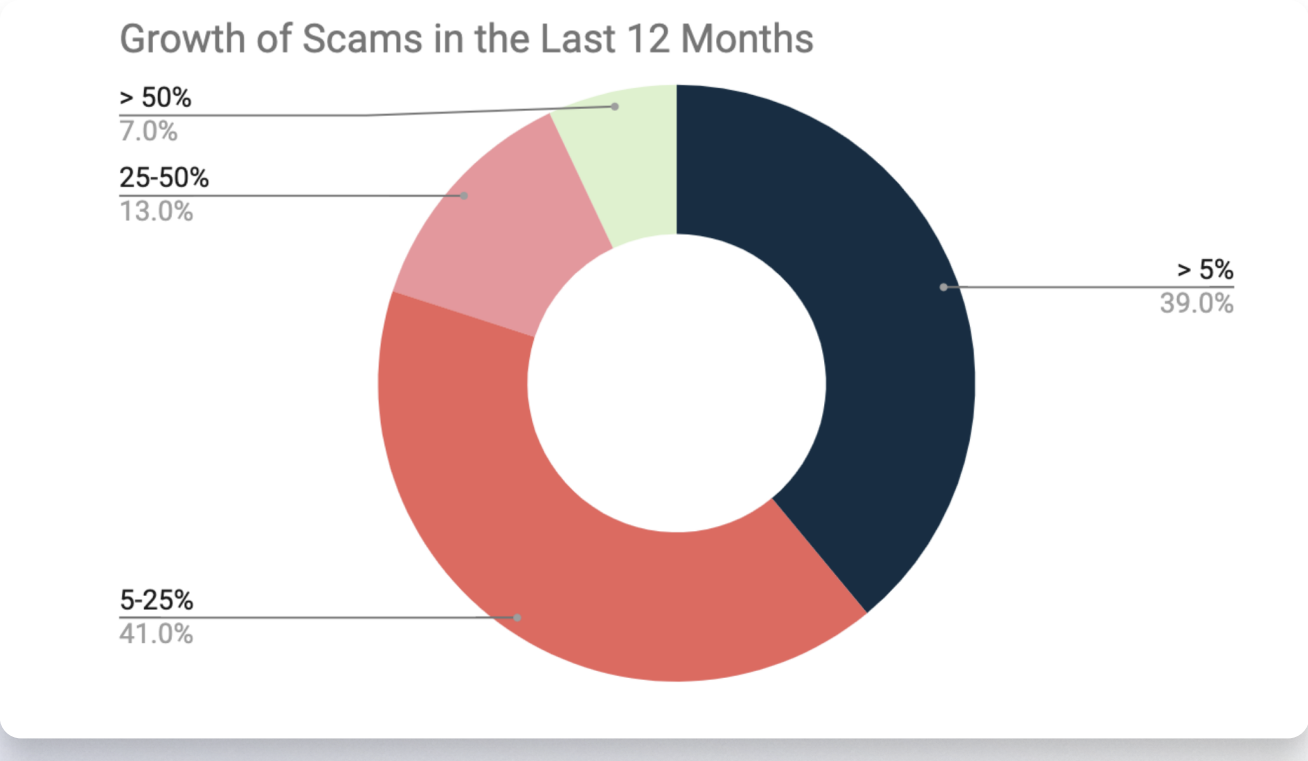


TREND 1

The Scam Surge - A Growing Threat

While credit card fraud remains a persistent concern, particularly for payment-focused fintech companies, scams are rapidly emerging as the biggest threat to the industry. This shift in the fraud landscape signals a pressing need for fintech to re-evaluate fraud prevention strategies and allocate resources accordingly.

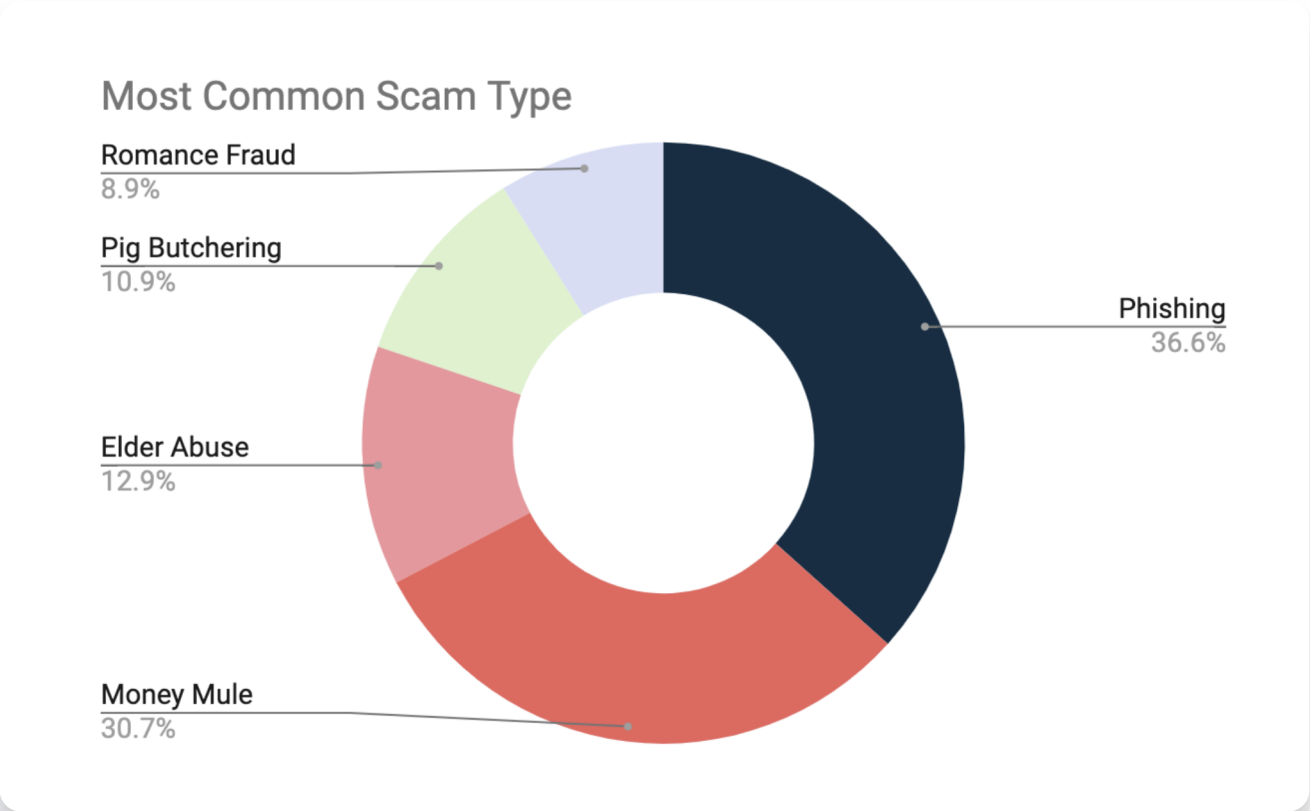
The financial impact of scams is undeniable. Our survey reveals that although credit card fraud is currently the costliest fraud type, scams are a close second, cited by 15% of respondents as the fraud type that costs them the most money. The alarming growth rate of scams further compounds this concern, with 40% of fintech companies reporting a 10-75% increase in scam activity in the past 12 months alone.



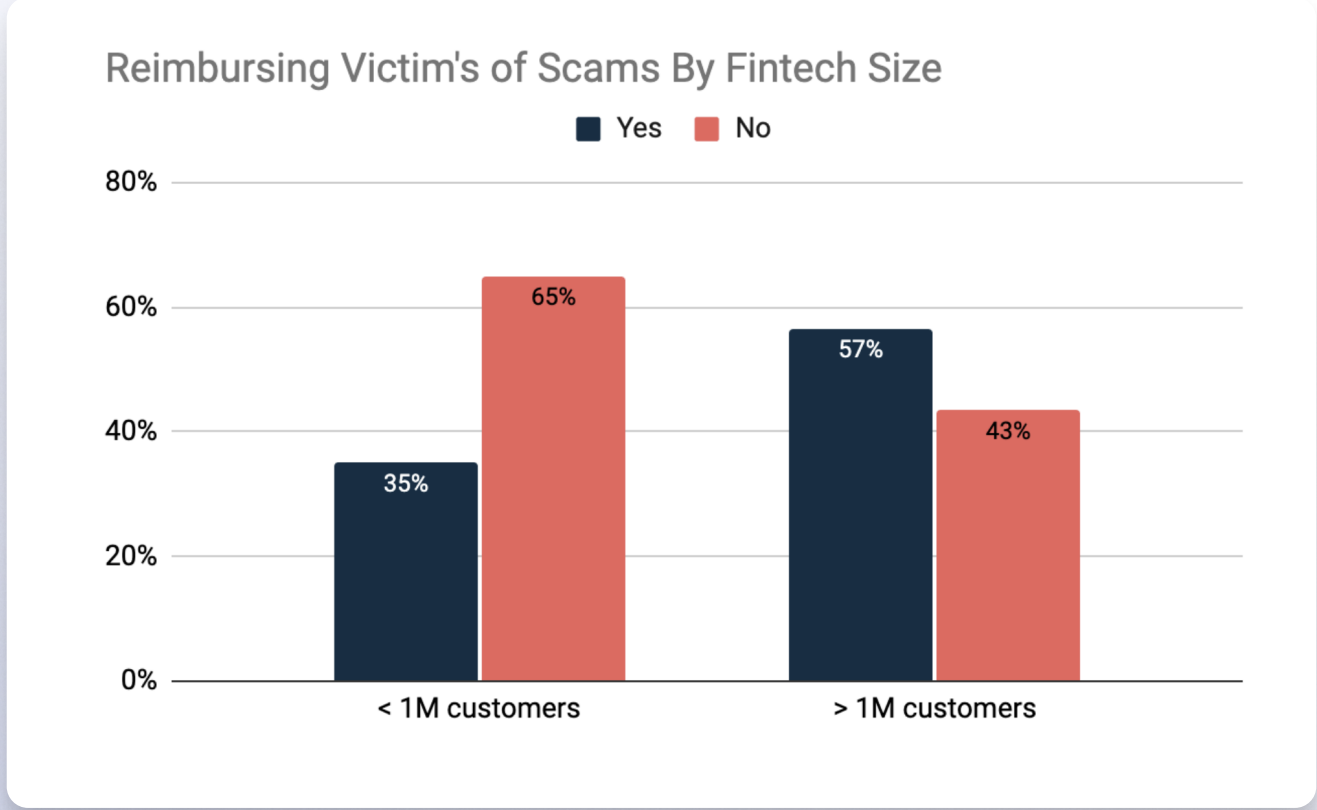
Beyond financial losses, scams also pose a significant drain on internal resources. Our data shows that scams are the second most time-consuming fraud type to investigate and combat behind ATOs, often requiring extensive manual effort and expertise. This operational burden can strain already stretched teams, potentially delaying response times and impacting customer experience.

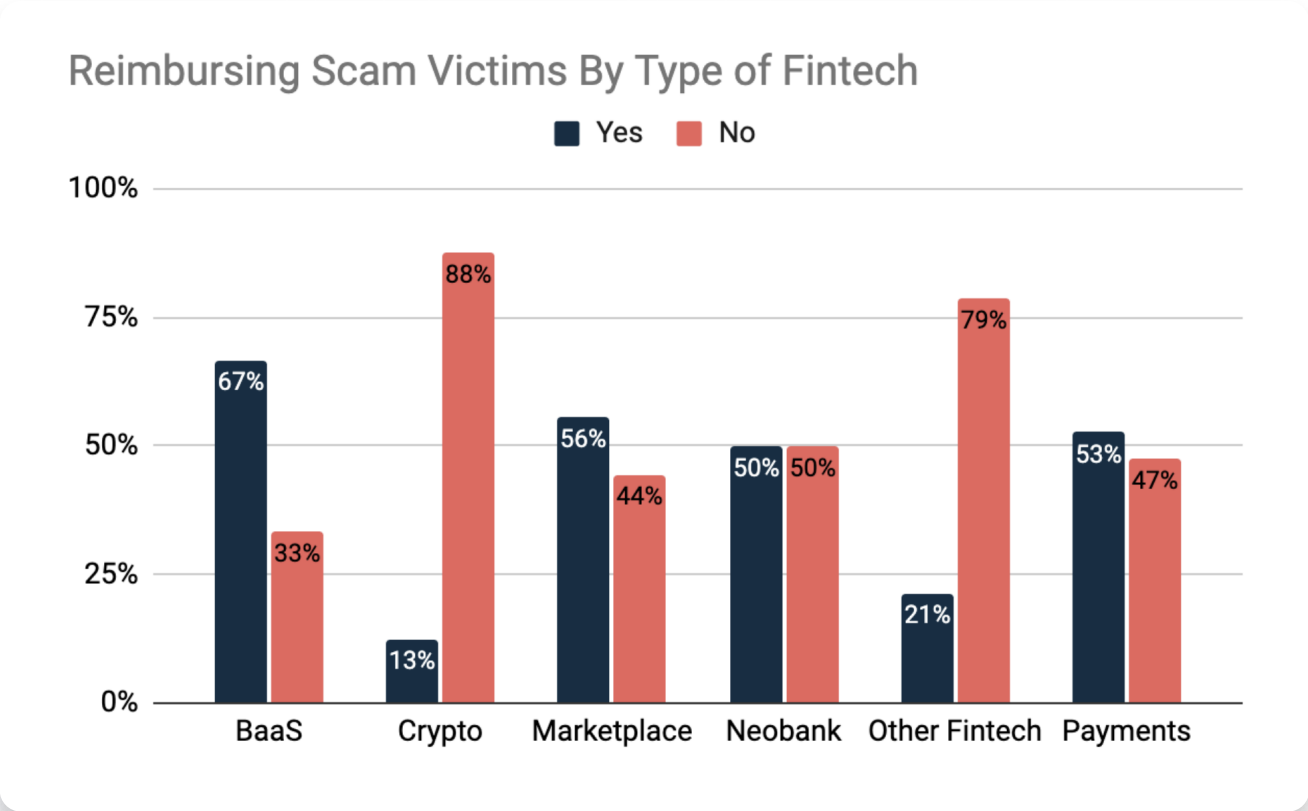
Moreover, the psychological scars of scams cut deeper than any financial loss. Unlike traditional fraud, scams prey on trust and empathy, leaving victims feeling not just violated but also foolish and ashamed. It's a heavy burden, and fintech is responsible for shielding its customers from these predatory schemes and offering support to those who've been ensnared.

Let's not forget the two most common scams haunting fintech are phishing (snagging 37%) and money mules (a close second at 31%). Phishing attacks are becoming increasingly sophisticated. Fraudsters are utilizing artificial intelligence to create hyper-realistic impersonations and clever social engineering to trick even the most vigilant users into handing over sensitive information. Money mules, often unwitting pawns in larger criminal operations, facilitate the movement of illicit funds, further complicating the fight against financial crime.



There's also the question of whether to reimburse customers when they have fallen victim to a scam. It may not necessarily be required, but the pressure to maintain customer satisfaction and the reputation risk associated with not reimbursing can be a factor.





The survey data paints a clear picture: the scam epidemic is real, and its impact on the fintech industry is substantial. Fintech must adopt a multi-pronged approach to tackle this challenge, including:

- **Collaborating with industry peers and law enforcement** to share information and best practices in combating scams, highlighting the need for consortium data.
- **Investing in advanced fraud detection** technologies capable of identifying and mitigating emerging scam typologies, looking beyond the transaction level, and viewing users as assets the way fraudsters do.
- **Implementing robust customer authentication and transaction monitoring processes** to detect suspicious activity and prevent unauthorized access to accounts.
- **Doubling down on educating customers and employees** about the latest scam tactics and providing them with the tools and resources to protect themselves.

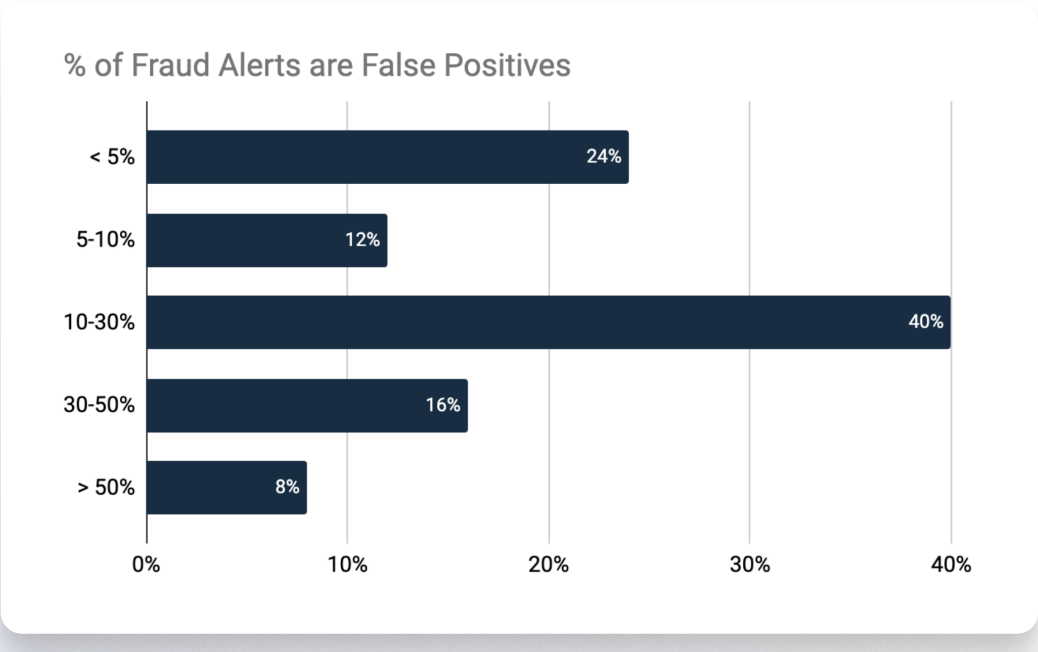
By taking proactive steps to address the scam surge, fintech can protect their bottom line, safeguard their customers, and maintain their reputation as trusted providers of financial services.

TREND 2

The Hidden Costs of Fraud Prevention

Beyond the immediate sting of financial loss, fintechs face a series of hidden challenges that silently undermine their operational efficiency and agility. Our survey results reveal a stark reality: the fight against fraud often comes at a cost.

A staggering 56% of fintech report that 10-50% of their fraud alerts are nothing more than false alarms. This translates to wasted time, strained resources, and frustrated customers. Imagine the cumulative impact of countless hours spent chasing shadows, legitimate transactions flagged as suspicious, and genuine customers left feeling inconvenienced and mistrusted. The cost of false positives extends far beyond the immediate operational burden; it chips away at customer satisfaction and trust, potentially driving users toward competitors with smoother, less intrusive security protocols.

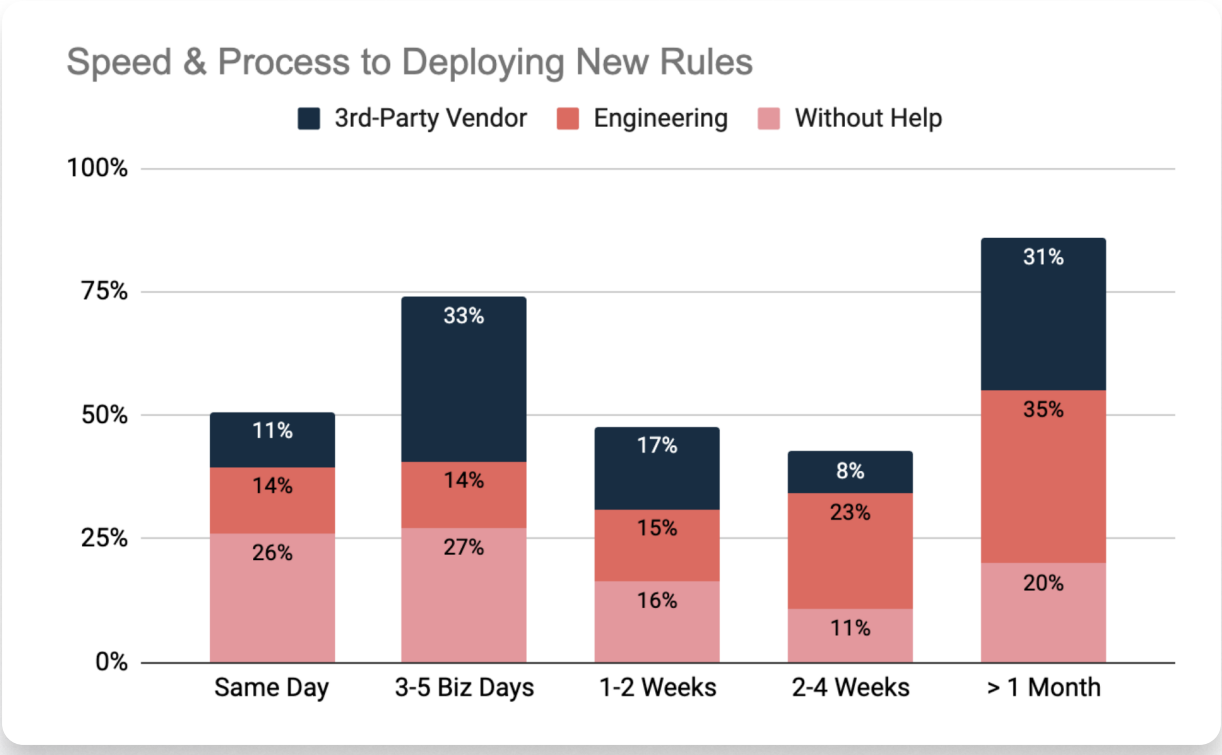


A reliance on engineering teams for rule deployment has emerged as a major pain point. Nearly half of fintech fraud teams (46%) and 34% of AML teams are beholden to engineering resources to implement new fraud rules, leading to frustrating delays and a lack of agility in responding to evolving threats.

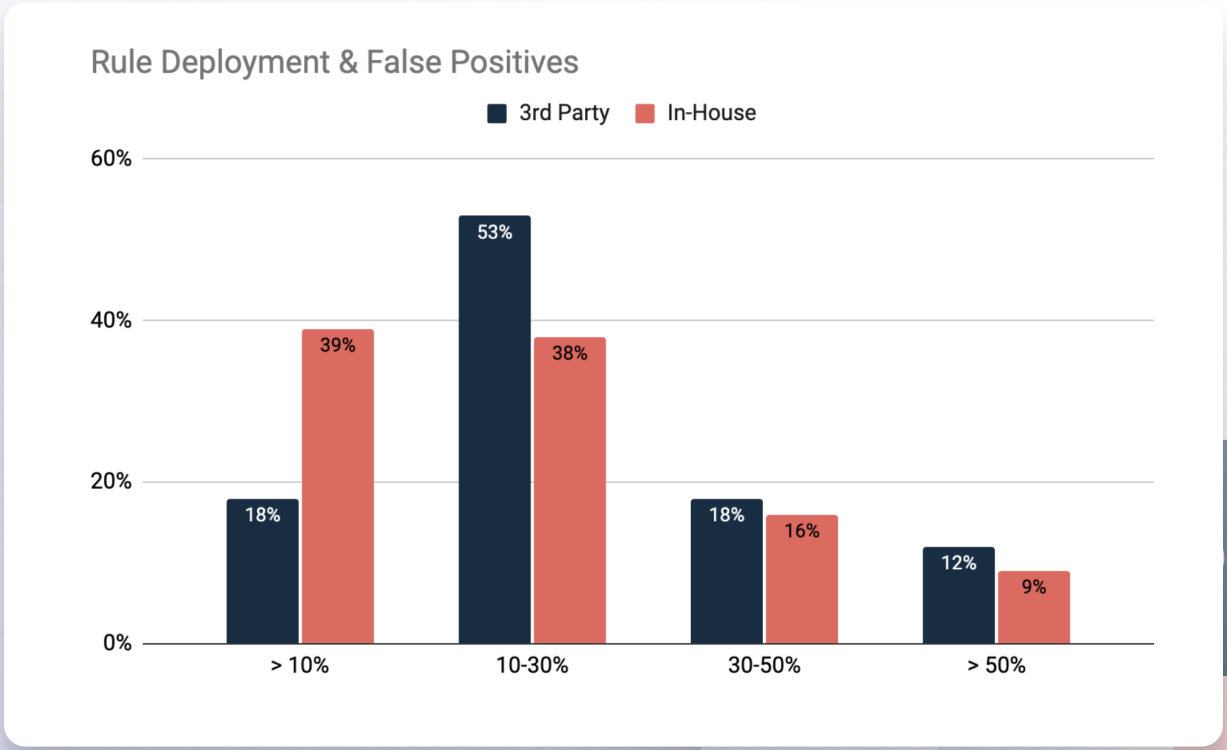
The data tells a bleak story: when teams depend on engineering, only 27% can deploy new rules within 5 business days. This sluggish pace contrasts sharply with the 44% of teams relying on third-party solutions or the even more impressive 53% who deploy rules in-house without engineering involvement, both capable of achieving the same feat. Even more concerning, a significant 35% of teams dependent on engineering report rule deployment timelines exceeding a month - an eternity in the world of fraud prevention.

35%

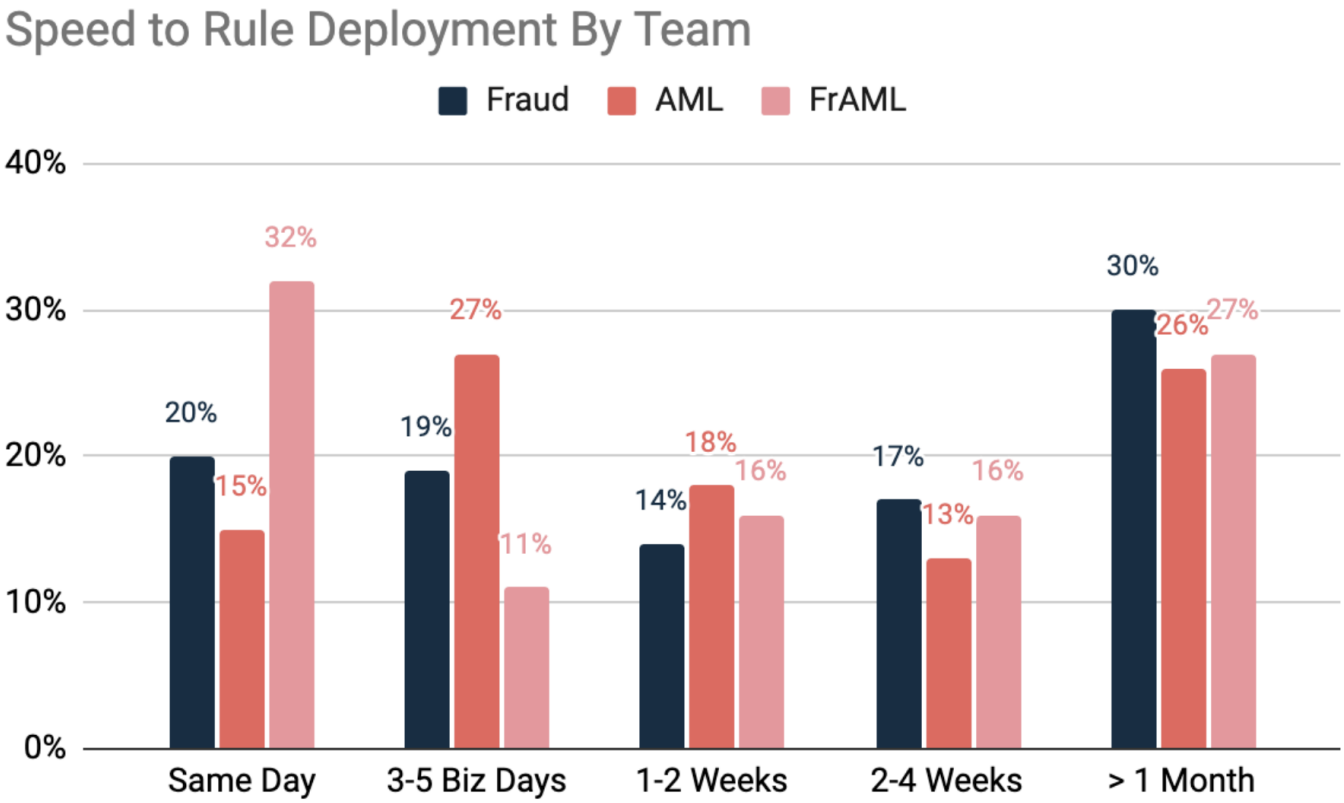
that are dependent on engineering **wait over a month** for rule deployments



Interestingly, 53% of those who rely on a third-party vendor see a 10-30% false positive rate. Whereas 27% that build and deploy in-house see a less than 5% false positive rate.



The good news? There's a glimmer of hope. Consolidated FrAML teams, which merge fraud and anti-money laundering functions, are showcasing a path toward greater agility. With 32% capable of same-day rule deployment, these integrated teams are demonstrating the power of breaking down silos and streamlining processes.



Unfortunately, the switch to FrAML is still a new trend. Only 9% of Fintech have made the switch, with the majority still relying on the traditional siloed approach.

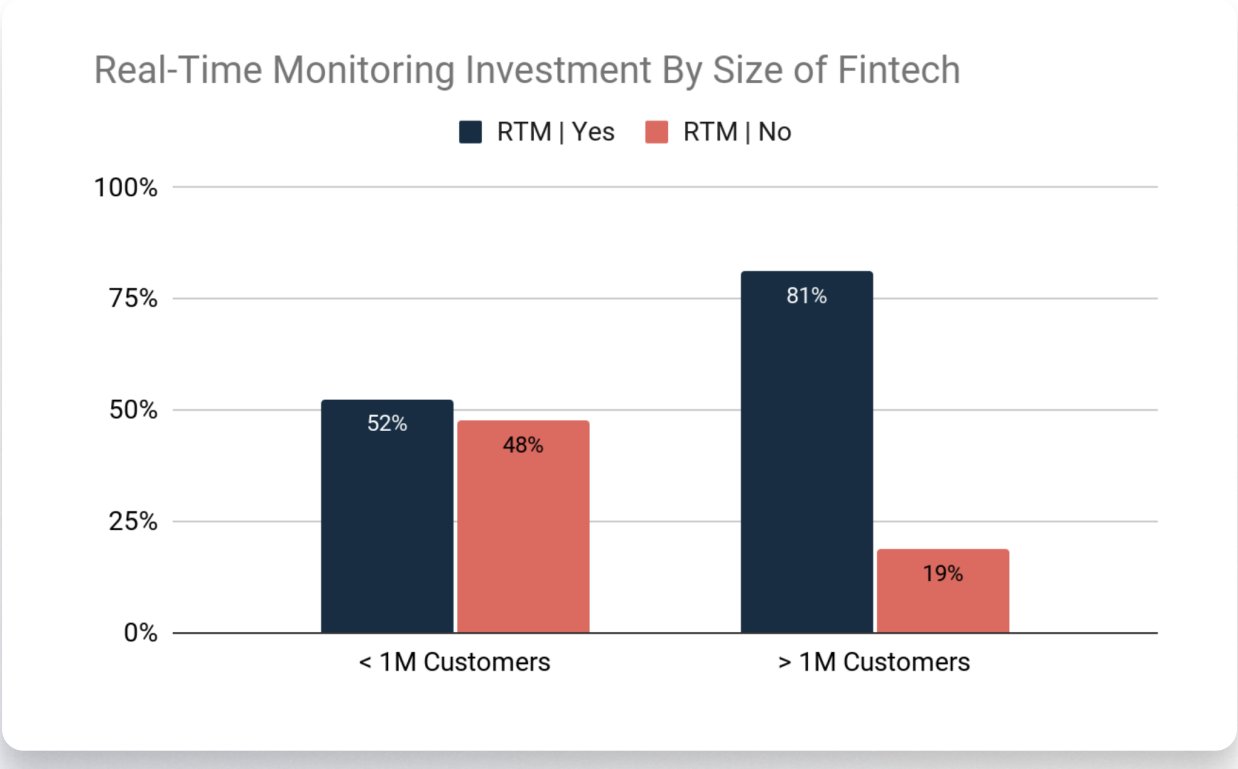
In the battle against fraud, fintech is caught in a delicate balancing act. They must fortify their defenses without stifling innovation or alienating customers. The challenges highlighted by our survey are a clear call for industry-wide action.

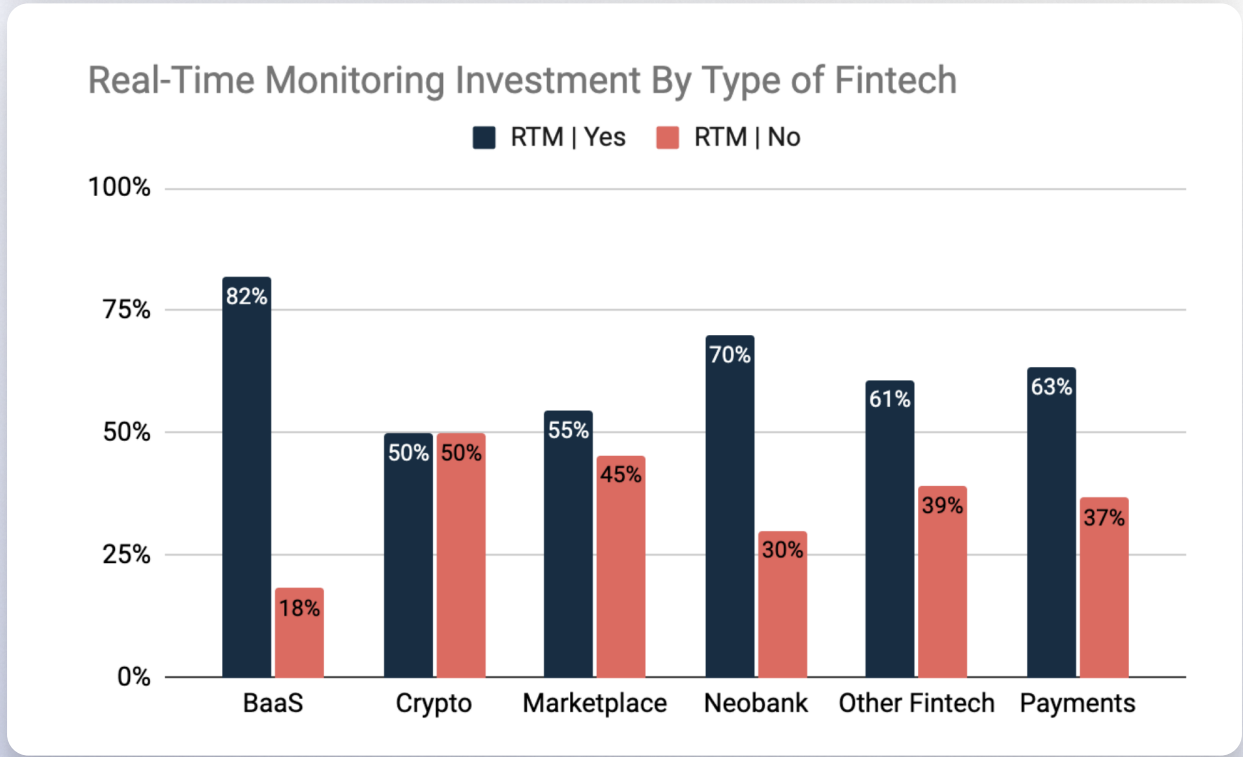
It's time to rethink traditional approaches, shake off traditional notions of how best to build and deploy new rules and foster greater collaboration between fraud, AML, and engineering teams. Only then can fintech strike the balance between security and customer experience.

TREND 3

Real-Time Monitoring: A Competitive Advantage

In the dynamic fintech landscape, where the battle against fraud is fought in milliseconds, real-time monitoring (RTM) has emerged as a formidable ally. Our survey data highlights its growing adoption, with 64% of respondents who addressed the RTM question confirming its implementation. However, its value extends far beyond mere adoption rates.





Fintech leveraging RTM reports a transformative impact on their fraud detection and prevention efforts. A remarkable 96% of those who have implemented RTM for over a year testify to improvements, with 58% noting a significant positive impact. This quantifiable success underscores RTM's role as a competitive ally in the fight against fraud, enabling fintech to reach new levels of protection.

Improvement in Fraud Detection & Preventions Since Implementing Real-Time Monitoring	
No Change	**4%**
Somewhat Improved	**38%**
Significantly Improved	**58%**

Real-time monitoring's positive impact on Fintech

96%

who have implemented RTM for over a year testify to improvements

In fact

58%

note a **significant** positive impact

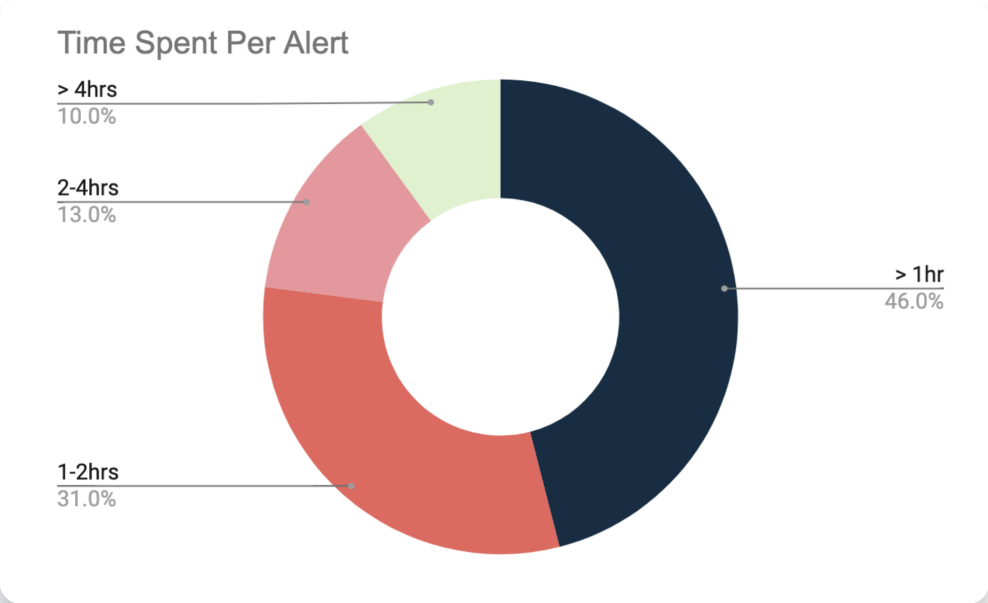
In conclusion, the data paints a clear picture. Real-time monitoring isn't simply a valuable tool; it's the linchpin for maintaining a competitive edge in today's fraud-ridden fintech landscape. As fraudsters grow more sophisticated and their attacks more rapid, RTM offers the agility and precision necessary to counter these threats head-on. It's the difference between losing ground and gaining an advantage. For fintech aiming to protect their financial interests and, perhaps even more importantly, the trust of their customers, real-time monitoring is no longer a luxury but a necessity.

TREND 4

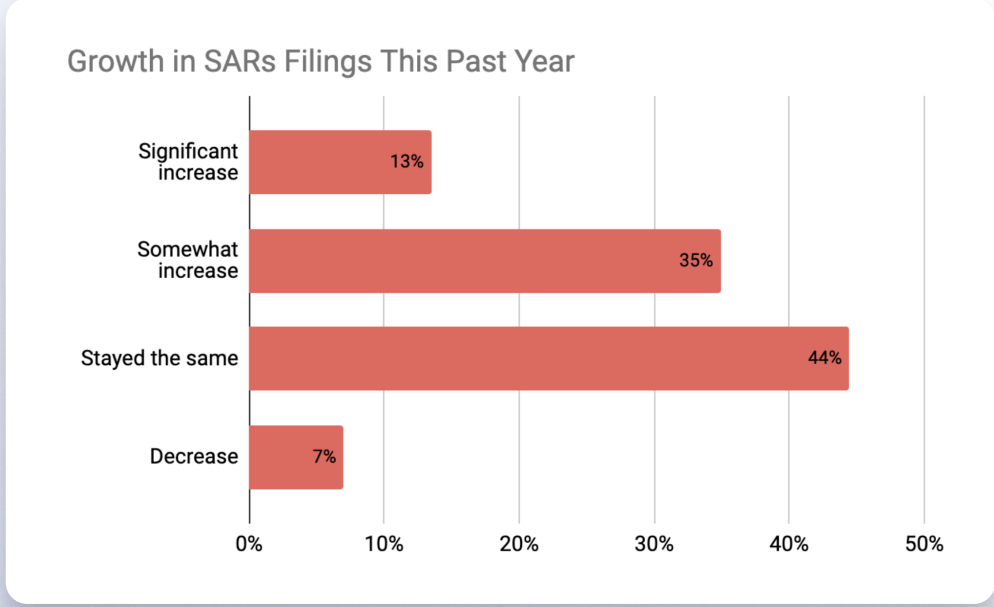
AML Remains a Resource-Intensive Challenge

While the fight against fraud is evolving, AML compliance remains a complex and resource-intensive undertaking for fintech. Our survey findings shed light on the challenges faced by AML teams, particularly in the areas of SAR filings and regulatory actions.

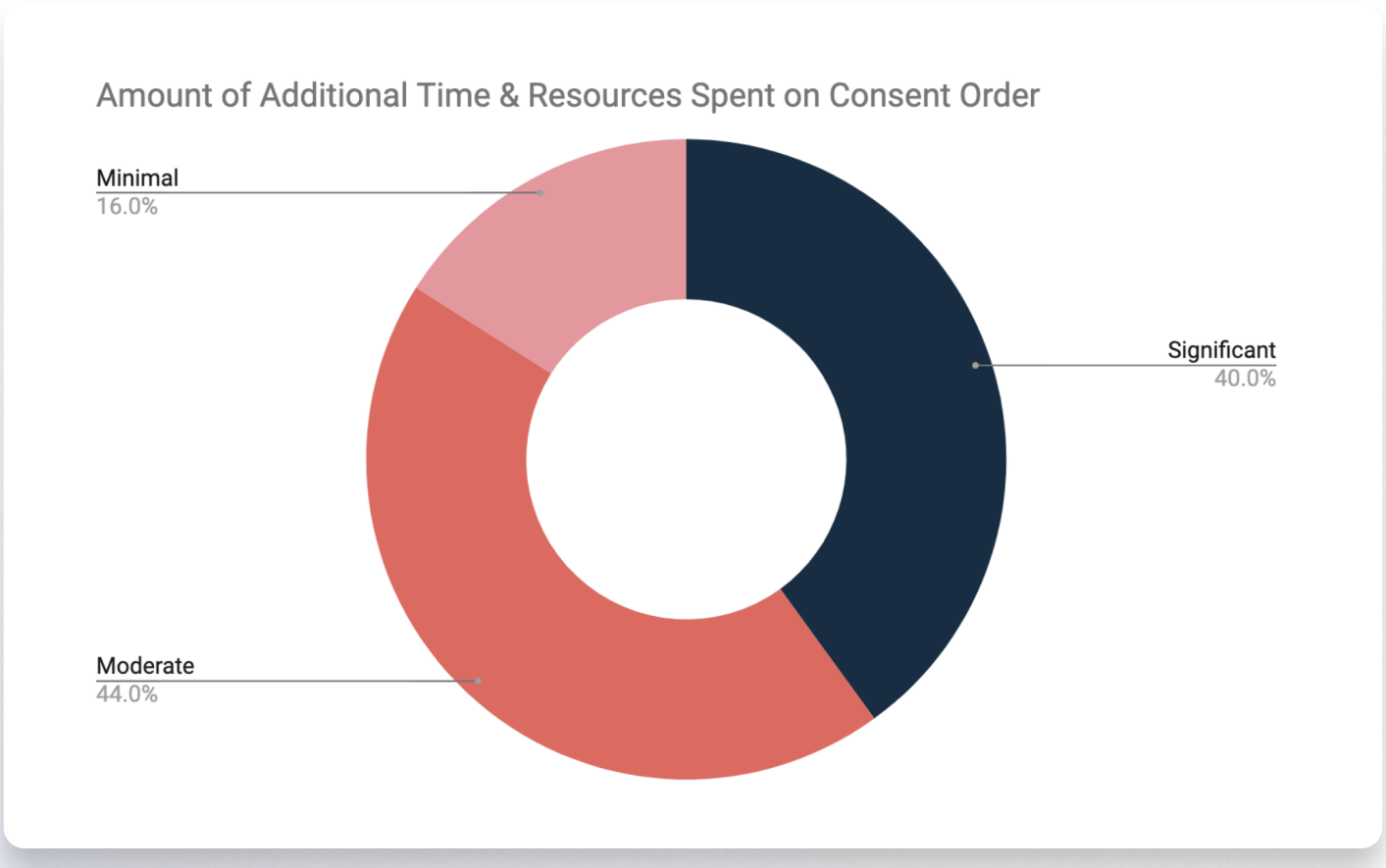
The average AML investigator spends a significant amount of time on each alert. This suggests that AML investigations often require in-depth analysis and meticulous documentation, consuming valuable time and resources.



Furthermore, the volume of SAR filings is on the rise. 48% of fintech companies reported an increase in SAR filings year-over-year, with 13% experiencing a significant increase. This upward trend adds to the workload of AML teams, requiring them to navigate complex reporting requirements and ensure compliance with evolving regulations.



Regulatory actions, such as consent orders—legal agreements imposed by regulators to address compliance deficiencies without formal litigation—further compound the challenges faced by AML teams. A concerning 40% of respondents indicated that these consent orders demand a significant amount of additional time and resources, diverting attention from core AML activities. Within the fintech industry, approximately a quarter (23%) of companies are actively facing regulatory actions. This highlights the ongoing compliance pressures prevalent in the sector.



These results show us that AML compliance isn't a one-time thing but an ongoing process. A plan needs to be developed to see how AML is getting more complex and needs more resources. By putting money into strong AML programs, which include processes, new technology, and skilled people, fintech can turn compliance from a burden into a strategic advantage. It's not just about avoiding fines; it's about lowering risk, building trust, and becoming known as a reliable company in the world of finance.

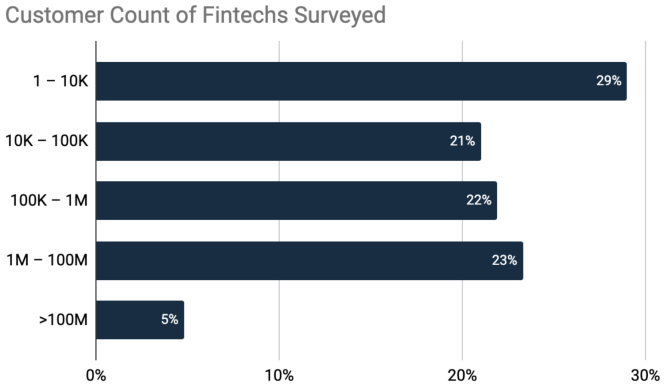
Who Did We Survey?

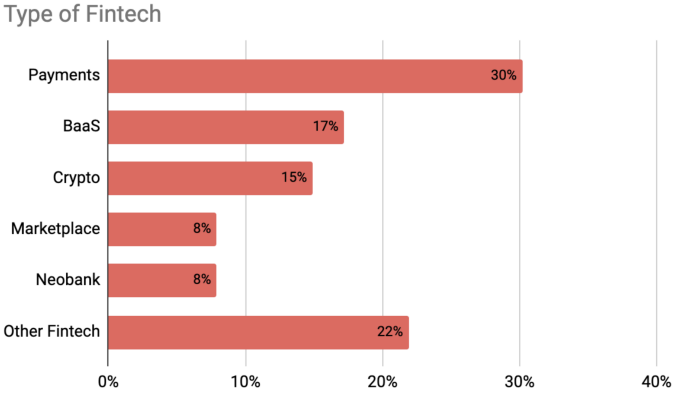
Methodology

We surveyed 369 fraud, AML, and FrAML professionals from banks, credit unions, and various fintech companies to understand the financial industry's challenges and learn best practices for fighting financial crime. Out of those 369, 215 were fintech.

Survey Dates: June - September 2024
Survey Size: 369
Fintech: 215

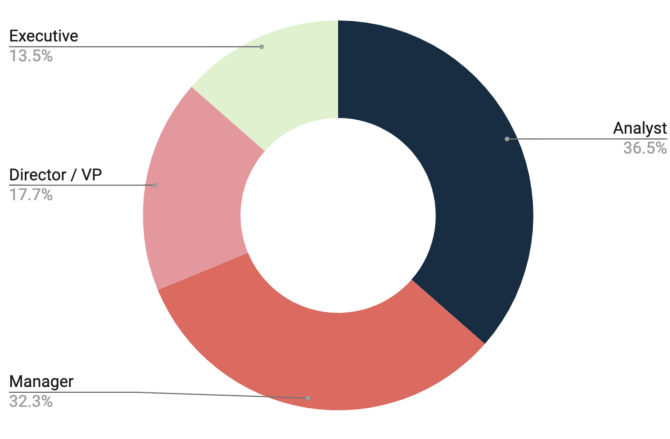
Fintech's Demographic

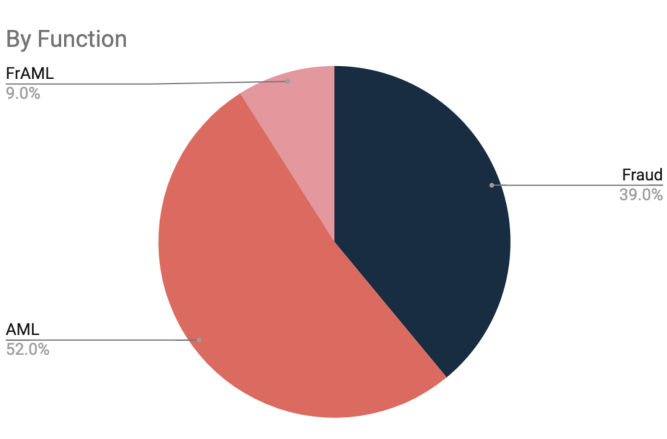




Respondent Firmographics

The survey aimed to delve into the biggest pain points and glean insights into strategies that have proven successful in fighting fraud. Respondents were either in Fraud, Compliance, or part of a FrAML team. Participants ranged in roles from Analysts to Executives from companies of various sizes.





Unit21

About us

Unit21 is on a mission to unite the world's fraud fighters and AML heroes to see the financial ecosystem restored to the pathway of opportunity it was meant to be. We specialize in solutions that don't just identify but proactively mitigate risks tied to money laundering, fraud, and other illicit activities. Uniquely positioned to solve the problem of financial crime and well-funded, we have raised close to $100 million from Google, Tiger Global, and other leading VCs.

Follow us on Linkedin

Visit unit21.ai