Unit21

4 Trends in Banking to Combat Fraud

FROM THE 3RD ANNUAL STATE OF FRAUD & AML

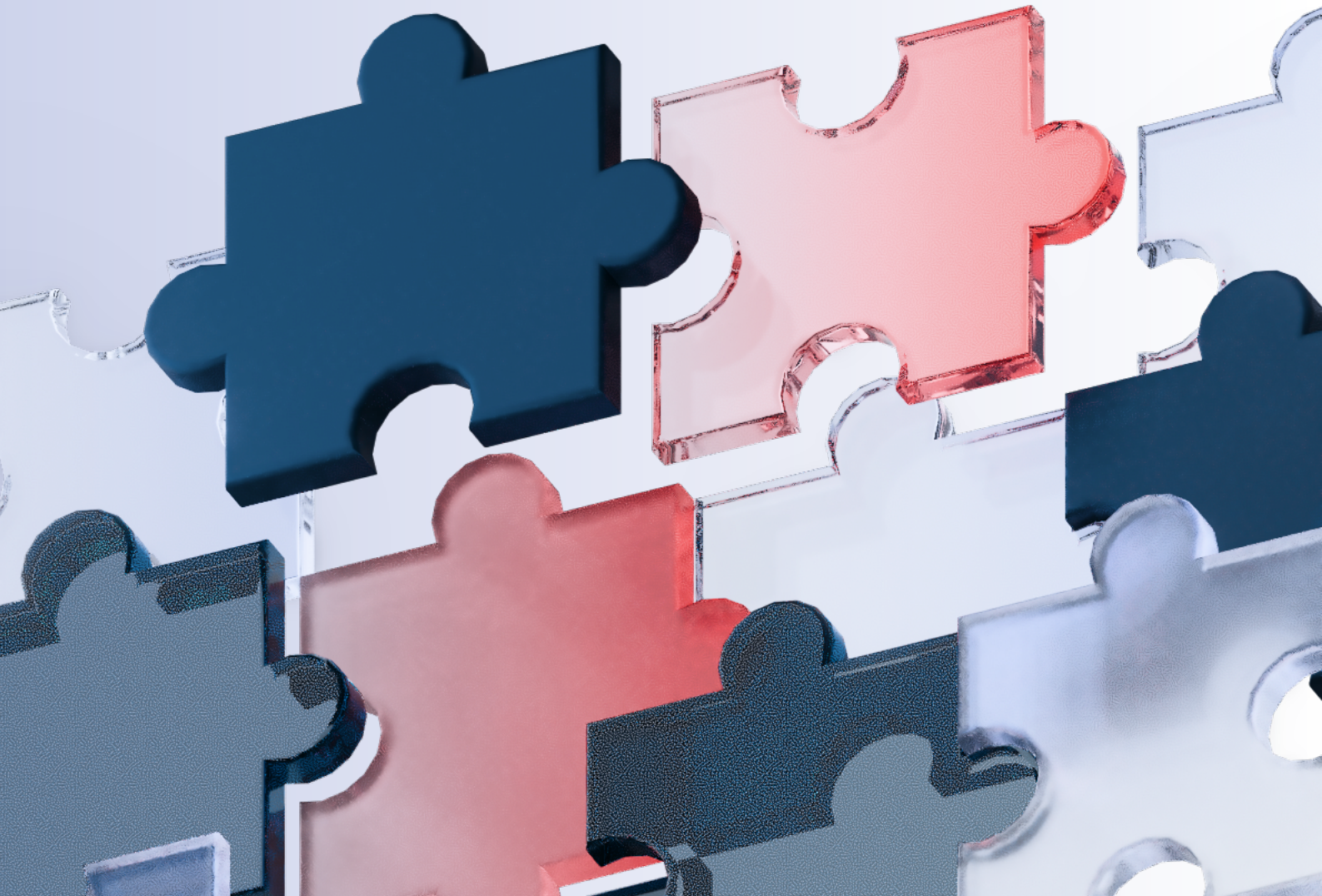
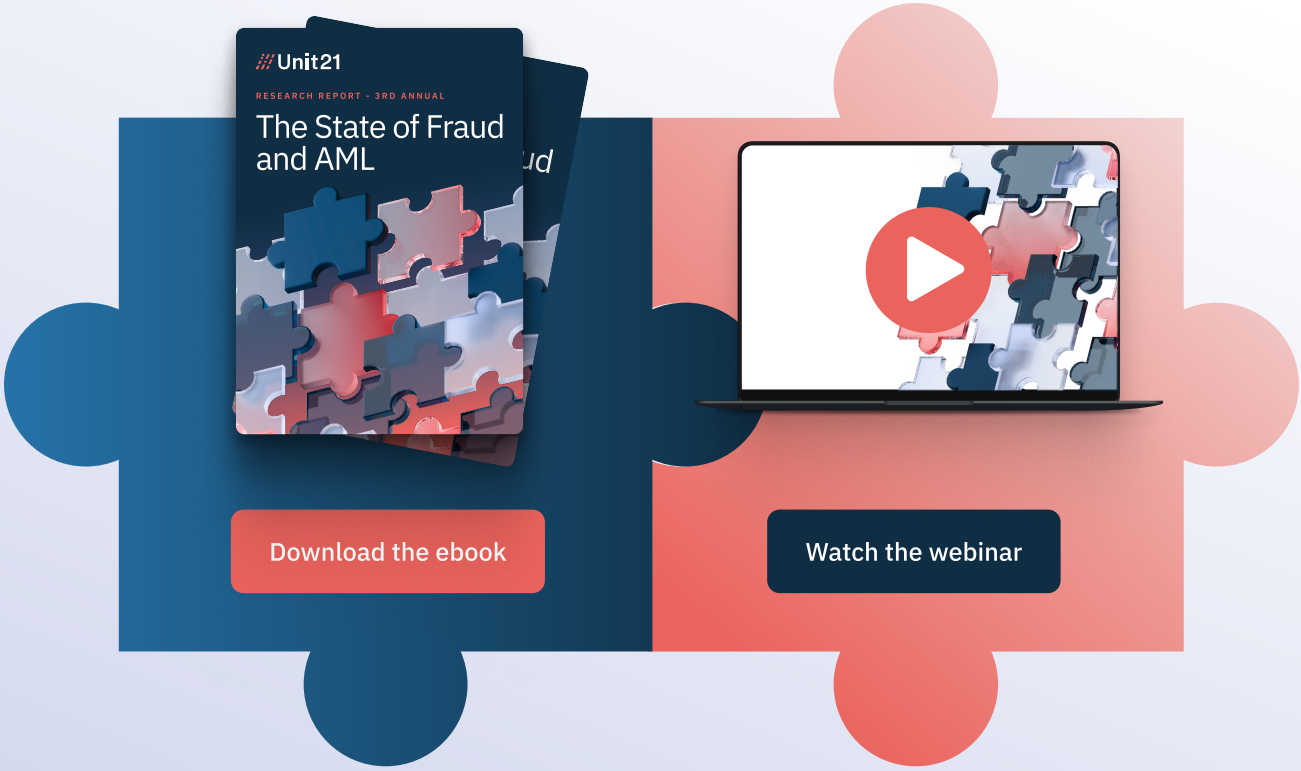


Table of Contents

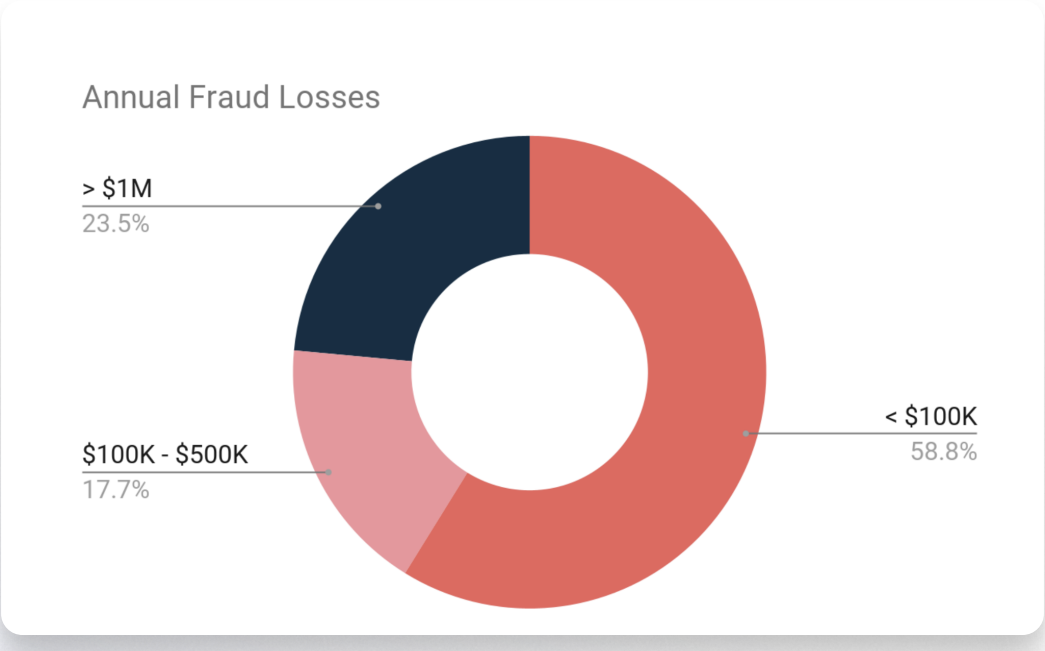
The Big Picture	03
Scams: The Wild West of Fraud	05
Check Fraud: An Evolving Threat	07
Real-Time Monitoring is a Real Need	08
Operational Efficiency	10
Who Did We Survey?	12

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.

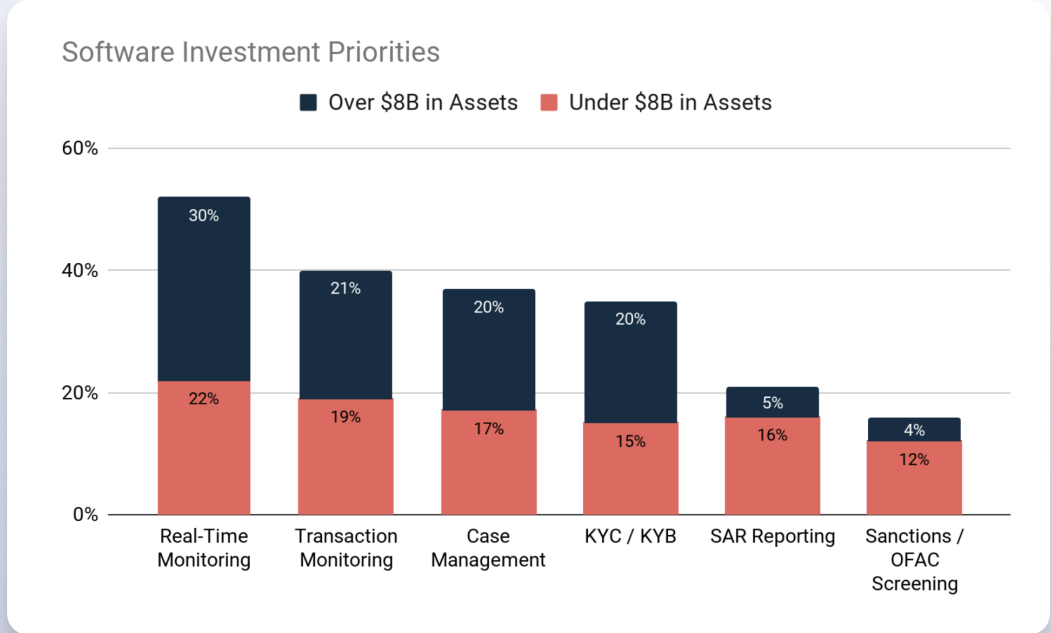


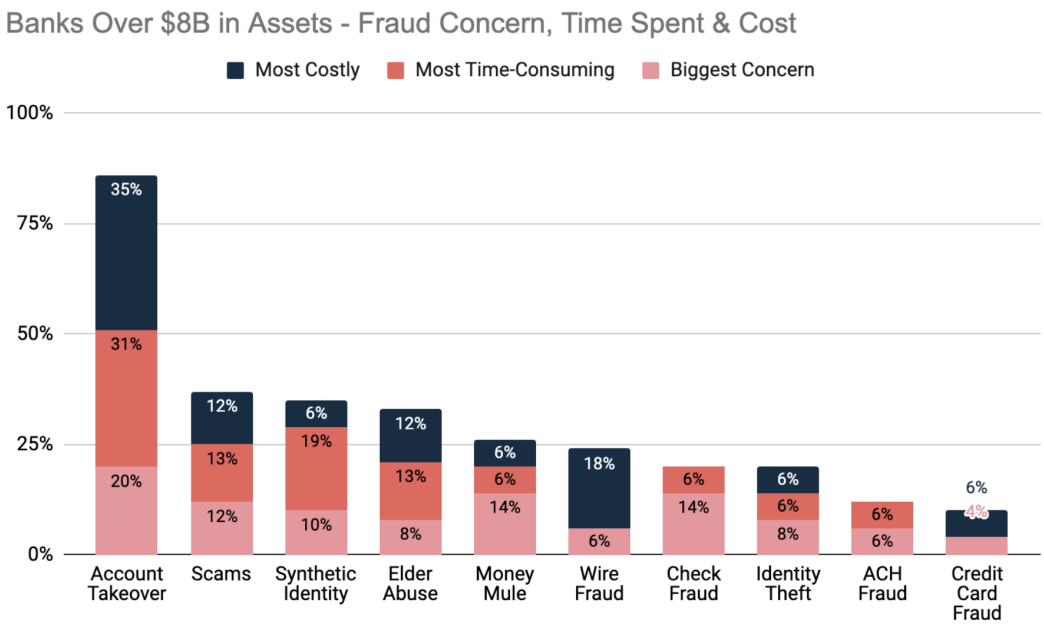
The Big Picture

The financial services industry is facing a fraud crisis that's not just changing—it's escalating rapidly. Banks are especially feeling the pressure. Payments are moving faster than ever, and new fraud vectors are emerging continuously. Although banks are seeing fraud increase, some have had success implementing things such as Real-Time Monitoring (RTM) or combining teams. Regardless, banks are still experiencing large fraud losses, with almost a quarter reporting losses above $1 million.

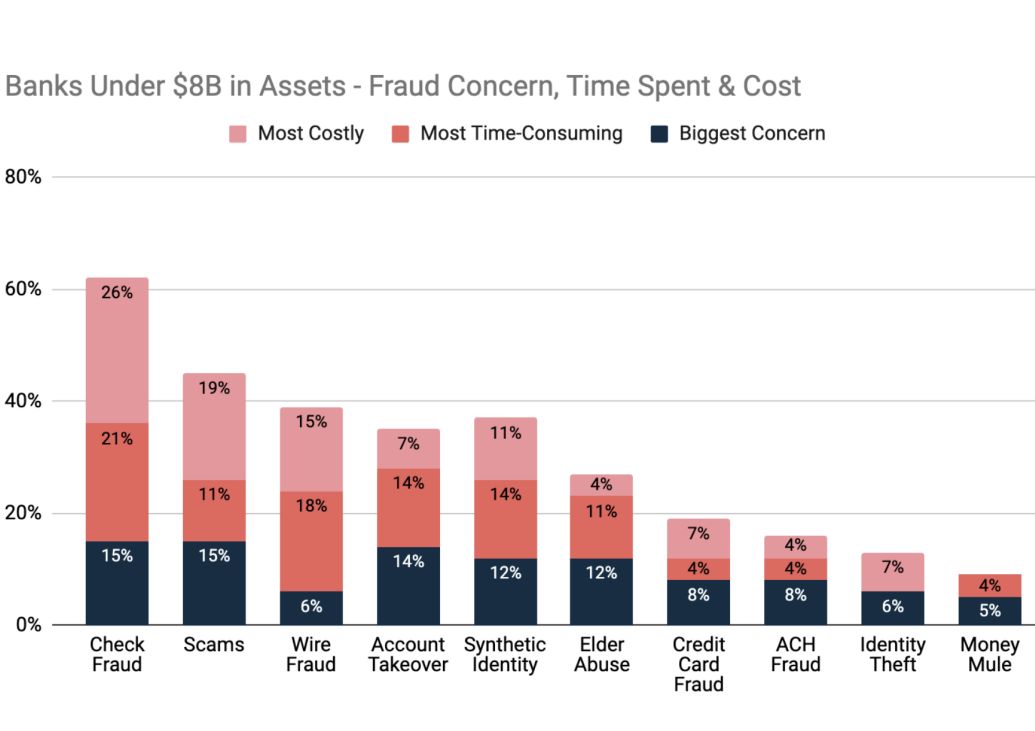


When thinking about priorities and what to invest in over the next 12 months to keep fraud at bay, Real-Time Monitoring was the top investment for all banks. When looking at larger banks, SAR reporting and Sanctions / OFAC Screening were a notability lower priority, than smaller banks.





When looking at what keeps fraud fighters up at night, larger banks rated Account Takeovers (ATO) as the most concerning, time-consuming, and costliest fraud. Smaller institutions, however, rated check fraud as the culprit.



TREND 1

Scams: The Wild West of Fraud

Amidst the diverse fraud landscape, scams have emerged as the untamed frontier, a digital Wild West where lawlessness thrives. A significant majority (64%) of banks report at least a 10% rise in scam activity, and 16% of banks saw growth over 50%.

64%

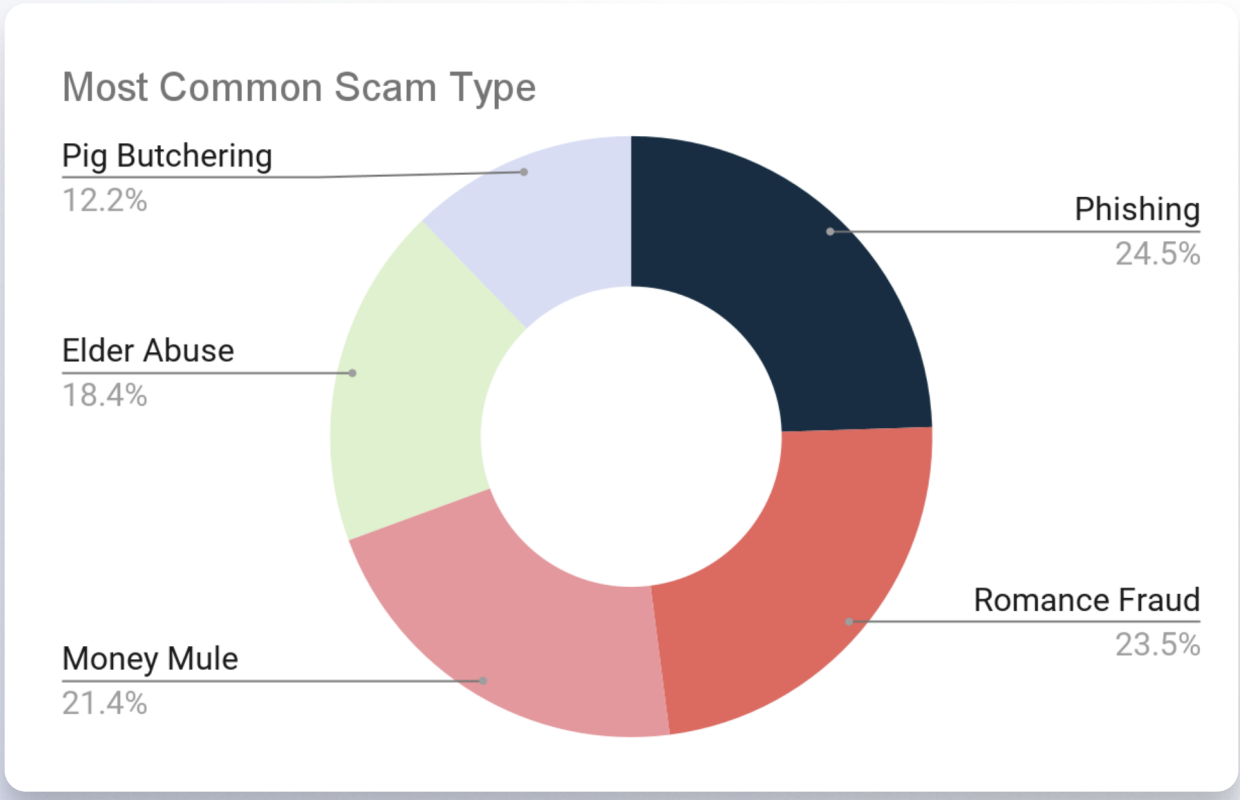
of banks report **at least a 10% rise** in scam activity in the last 12 months

In fact

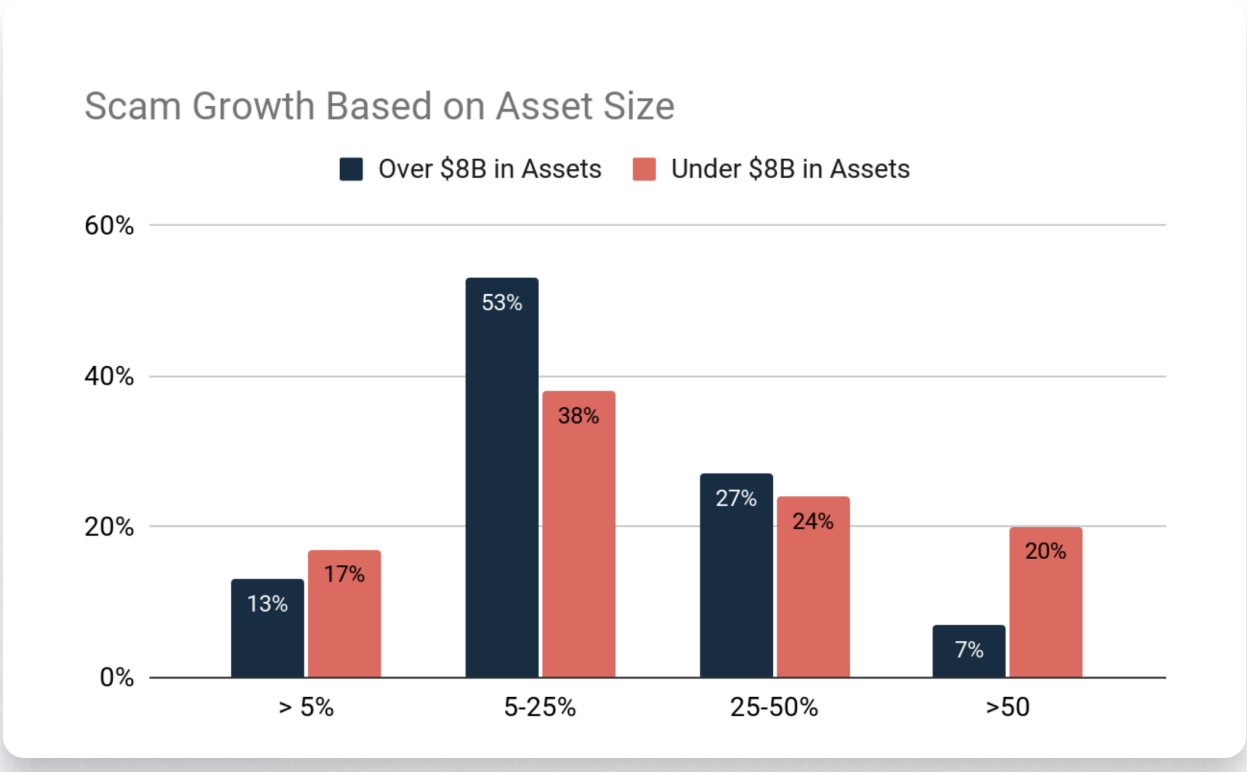
16%

of banks saw **over a 50% rise** in scam activity in the last 12 months

These modern-day outlaws deploy an arsenal of deceptive tactics – phishing emails, romance scams, and sophisticated social engineering schemes – to manipulate and exploit unsuspecting victims. The financial and social damages inflicted by scammers should place scams at the forefront of any fraud mitigation strategy.
Phishing scams were reported as the most prevalent at 24%, followed by romance fraud at 23% and money mules at 21%.



Smaller banks are feeling the pain of scam growth more than larger banks. The research found that 44% of smaller banks saw at least a 25% growth in scams, whereas 66% of larger banks saw less than a 25% growth in scams over the last year.



Banks often reimburse customers who fall victim to scams, with 70% of banks reporting they reimburse victims of scams. This customer-centric approach aims to maintain trust and loyalty, but it also adds to the financial burden of fraud.

However, when breaking down by asset size, there's a stark difference between institutions below $8 billion in assets and those above. Smaller banks are more likely to reimburse victims, with 85% confirming this policy compared to 50% of the larger banks reimbursing. This hints that smaller banks might prioritize customer relationships with their reputation, even if it means bigger losses in the short term.

Smaller banks prioritize customer relationships more than big banks.

> $8B IN ASSETS

50%

reimburse customers who fall victim to scams

< $8B IN ASSETS

85%

reimburse customers who fall victim to scams

TREND 2

Check Fraud: An Evolving Threat

Despite the increasing digitization of payments, check fraud continues to prove that bad actors are benefiting from the aged payment method, with **53% of banks reporting an alarming 10-75% increase in the last 12 months.**

Check Fraud Concerns & Growth

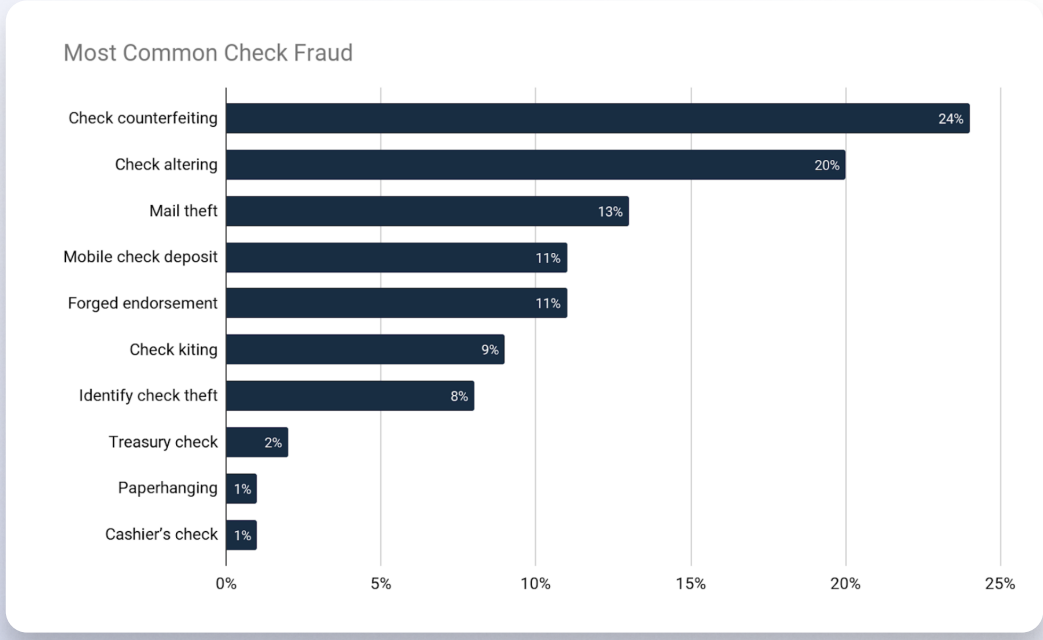
Banks < $8B in assets rank check fraud **top concern, most time-consuming, and most costly**

53%

of banks report an alarming **10-75% increase in check fraud** in the last 12 months

Even though all banks report alarm check fraud growth rates, banks under $8 billion rated check fraud as not only the most costly, but also the most time-consuming and the biggest concern of all fraud types. This low tech, low sophistication payment type lends itself well to fraudsters, making it both incredibly easy to commit and incredibly difficult for banks to catch.

There are a variety of ways that check fraud can take place. Fraudsters employ tactics such as washing checks, creating counterfeit checks, and faking endorsements. Mail theft is also on the rise, enough to prompt FinCEN to issue an alert. However, respondents reported that check counterfeiting (24%) and check altering (20%) were the most prevalent forms of check fraud, underscoring the importance of maintaining vigilance even with traditional payment methods.



Although banks of all sizes agree that check altering and check counterfeiting are top concerns, 15% of banks over $8 billion rated mobile check deposit and forged endorsement as more concerning over check altering (12%).

TREND 3

Real-Time Monitoring is a Real Need

Banks face a dynamic fraud landscape where threats evolve rapidly. Balancing the need for robust fraud prevention with operational efficiency is a constant challenge. Banks are laser-focused on enhancing their real-time fraud detection and prevention capabilities and shifting from a reactive to a proactive approach. This strategic priority is likely driven by the increasing sophistication and speed of fraud attacks, which demand immediate response to minimize losses.

Banks rated real-time monitoring (RTM) as the top priority (24%) to invest in within the next 12 months. However, core providers are often ill-equipped to support real-time monitoring, with 45% of respondents indicating this as a missing capability.

#1

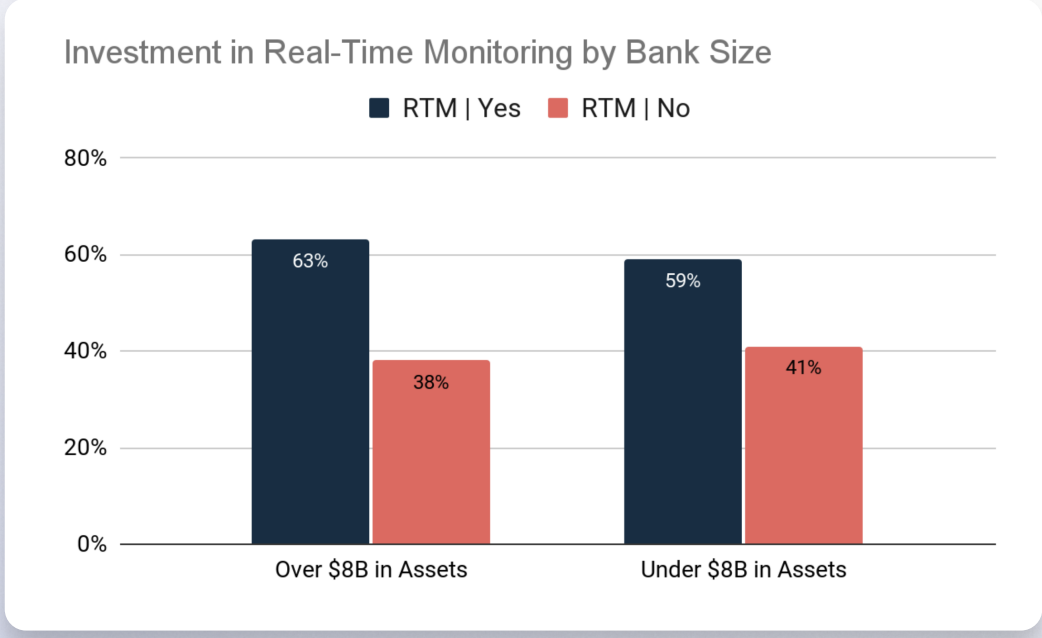
investment priority for banks in the next 12 months

But

45%

report their core provider is missing real-time monitoring capabilities

This technology gap underscores the need for banks to explore third-party solutions or invest in system upgrades to achieve their fraud prevention goals. But even with RTM rated as a priority, adoption is still lagging. On average, 40% of banks do not yet have real-time monitoring implemented.



It's imperative that an institution's capabilities keep up with the speed of its transactions, especially with transactions that have no recall once completed. You need tools that match the speed of the fraud. The capabilities are moving more quickly than most financial institutions' ability to monitor it.

Top benefits seen from real-time monitoring

By integrating fraud and AML functions, institutions can achieve a more holistic view of financial crime risk. This comprehensive perspective enables them to:

1 **Improved fraud detection**
Institutions with RTM report a significant increase in fraud detection, thanks to the ability to analyze data in real-time and identify suspicious activities immediately. This proactive approach enables them to catch potential fraudsters before they can cause damage.

74%

of banks utilizing RTM report notable improvements in fraud detection & prevention

2 **Reduced false positives**
RTM's advanced algorithms and real-time analysis reduce the number of false positives, saving time and resources. This increased accuracy boosts the efficiency of fraud detection. Banks with RTM boast a false positive rate better than those that have not implemented RTM, enabling investigators to focus on genuine threats.

21%

of banks with real-time monitoring implemented have achieved **false positive rates under 5%**

3 **Streamlined alert investigation**
RTM systems can prioritize and filter alerts, allowing investigators to focus on the most critical cases. This reduces the time spent on each alert, leading to faster resolutions and improved productivity.

72%

report with real-time monitoring it takes less than 30 minutes to investigate alerts

TREND 4

Operational Efficiency

Rule Building and Agility

In the rapidly evolving landscape of fraud prevention, the ability to swiftly adapt defenses is paramount. Our survey reveals a stark contrast in agility: banks empowered to handle rule deployment internally demonstrate remarkable responsiveness, with nearly half (46%) of bank respondents stating they're capable of implementing new rules within two weeks.

However, diving into the details, we find reliance on internal engineering teams can manifest as a significant bottleneck, as 52% of these institutions require almost 4x that time frame, up to 8 weeks for deployment. This data underscores the distinct advantage of self-sufficiency in rule management, enabling financial institutions to proactively respond to emerging threats and stay ahead of the mounting fraud and AML pressures.

46%

of banks can implement new rules within two weeks without relying on **outside** resources

52%

rely on engineering

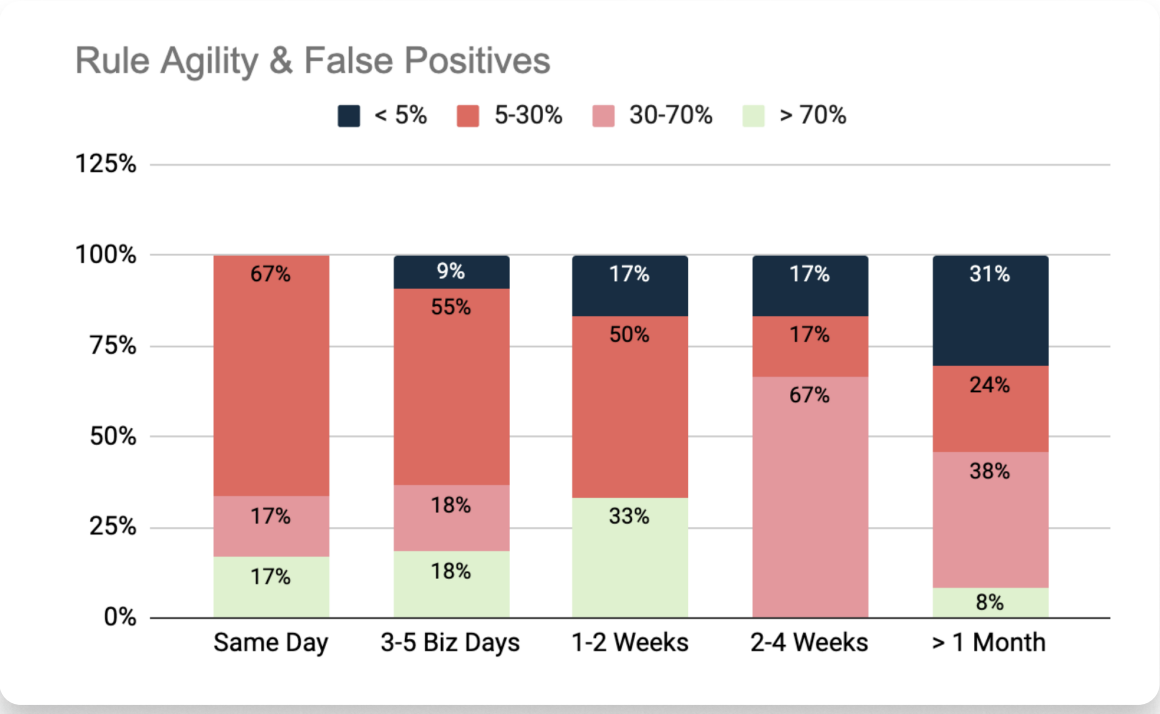
and, therefore, can't get rules deployed for **up to 8 weeks!**

41%

deploy rules themselves

and get a rule out in **5 business days or less!**

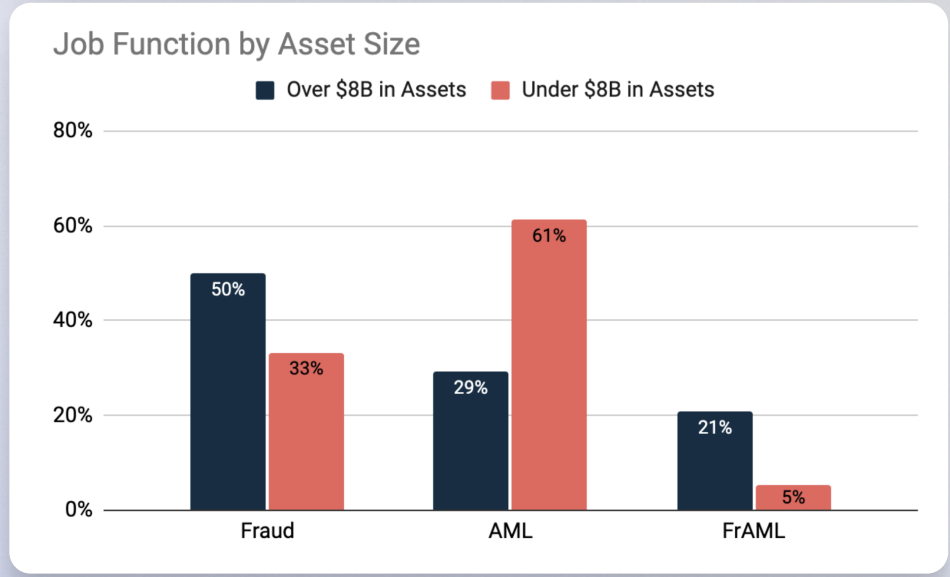
Of those that can deploy rules within 2 weeks or less, 65% average under a 30% false positive rate. Whereas, those who take over a month, only 54% can make that same claim.



The Rise of FrAML: A Path to Enhanced Efficiency

The survey results reveal a fascinating trend: the integration of Fraud and AML teams is gaining momentum, but it's clear that many organizations are still hesitant to commit fully. Surprisingly, 38% of respondents maintain separate teams, tools, and resources, highlighting a reluctance to embrace the full potential of a combined FrAML structure.

Banks with over $8B in assets are more likely to adopt FrAML, with **21% implementing this**. However, only **5% of banks under $8B have switched.**



When diving into those that have adopted FrAML, 57% have merged teams and tools within the last year. Of those teams who converted to FrAML by combining into one team with shared tools and resources, 100% of respondents saw significant improvement in detection and prevention performance. This is a testament to the power of collaboration, streamlined communication, and a holistic risk management approach.

Breaking down silos isn't just an option; it's essential for maximizing efficiency and staying ahead.

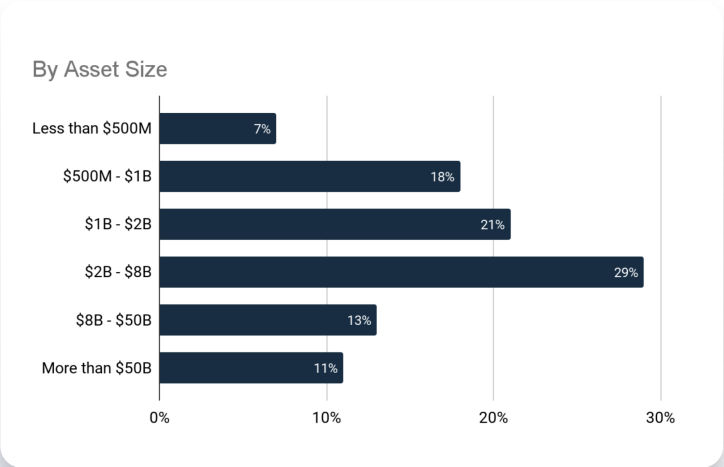
Who Did We Survey?

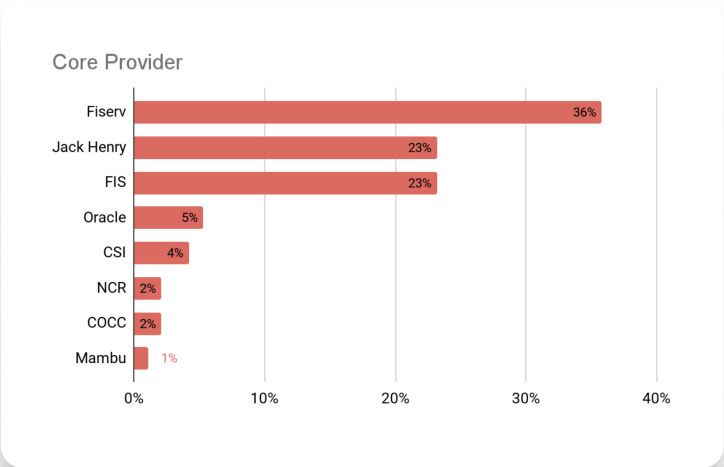
Methodology

We surveyed 369 fraud and compliance professionals from banks, credit unions, and various fintech companies to understand the financial industry's challenges and uncover best practices for fighting financial crime. Out of those 369, 100 were banks.

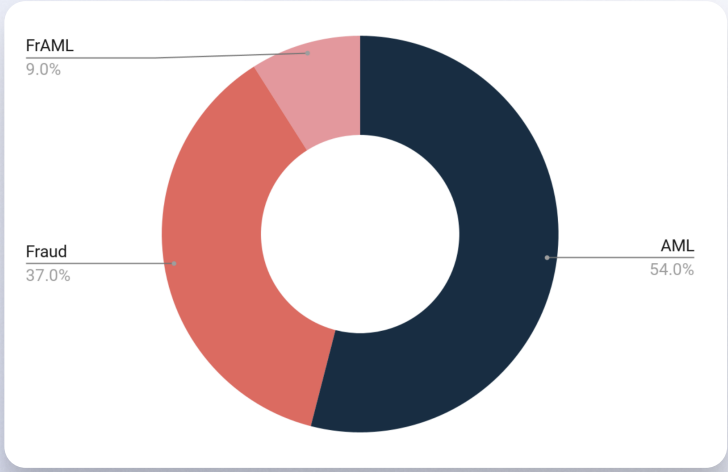
Survey Dates: June - September 2024
Survey Size: 369
Banks: 100

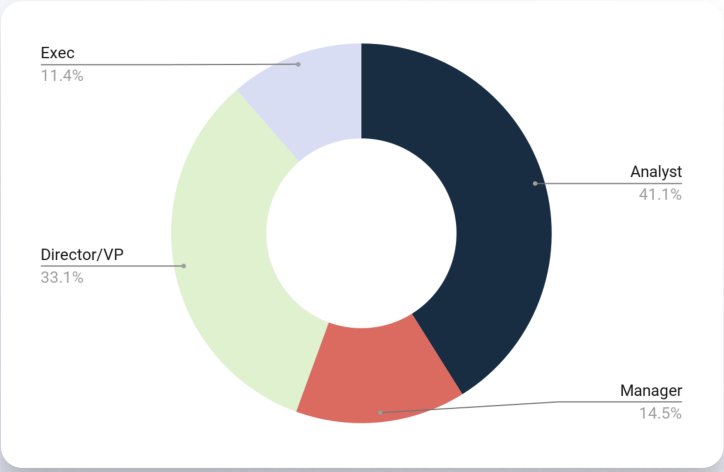
Bank Demographics





Respondent Firmographics





The survey aimed to delve into the biggest pain points and glean insight into strategies that have proven successful in fighting fraud. Respondents were either in Fraud, AML, or part of a FrAML team. Participants ranged in roles from analysts to executives from banks 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