Unit21

4 Trends in Credit Unions to Combat Fraud

FROM THE 3RD ANNUAL STATE OF FRAUD & AML

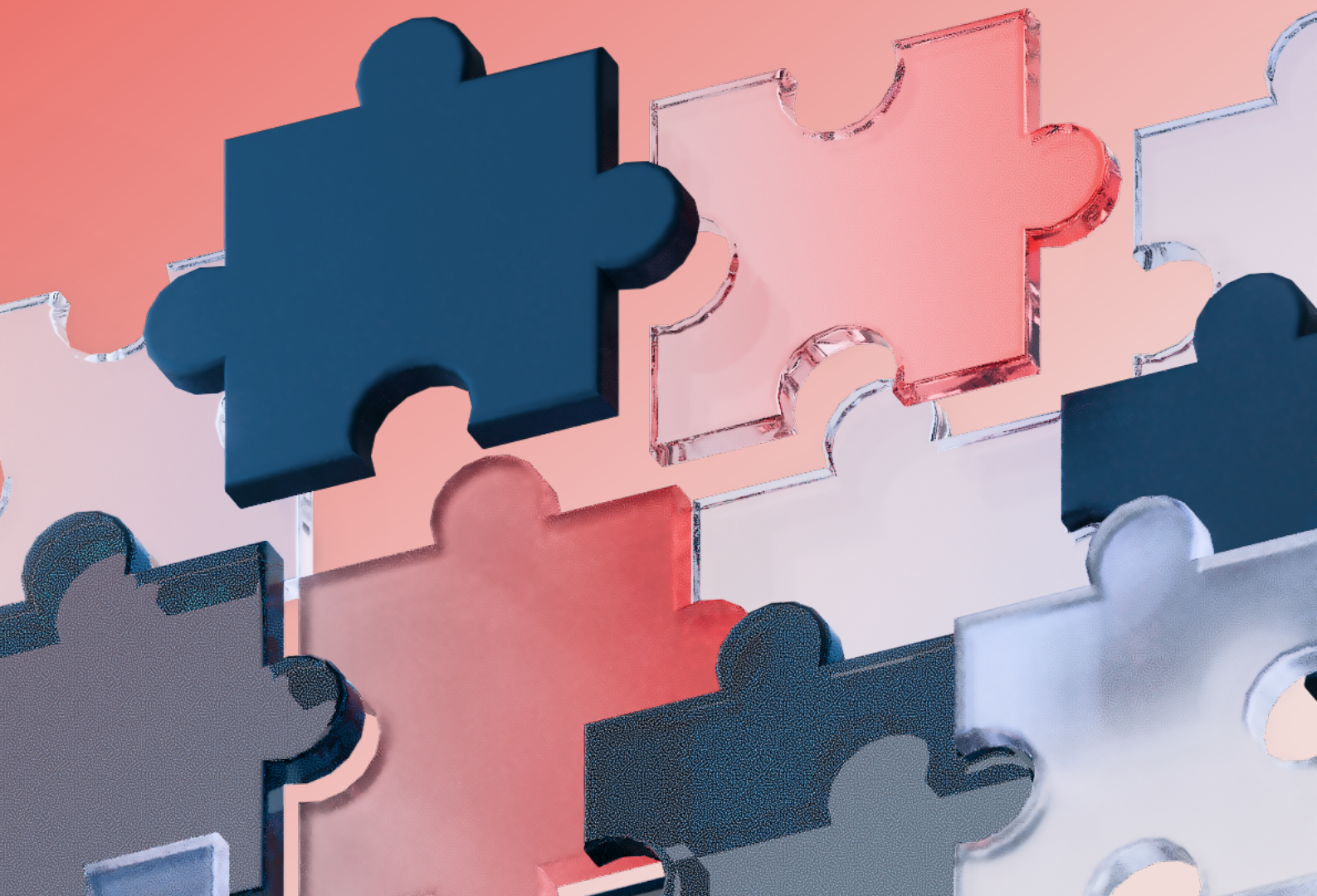
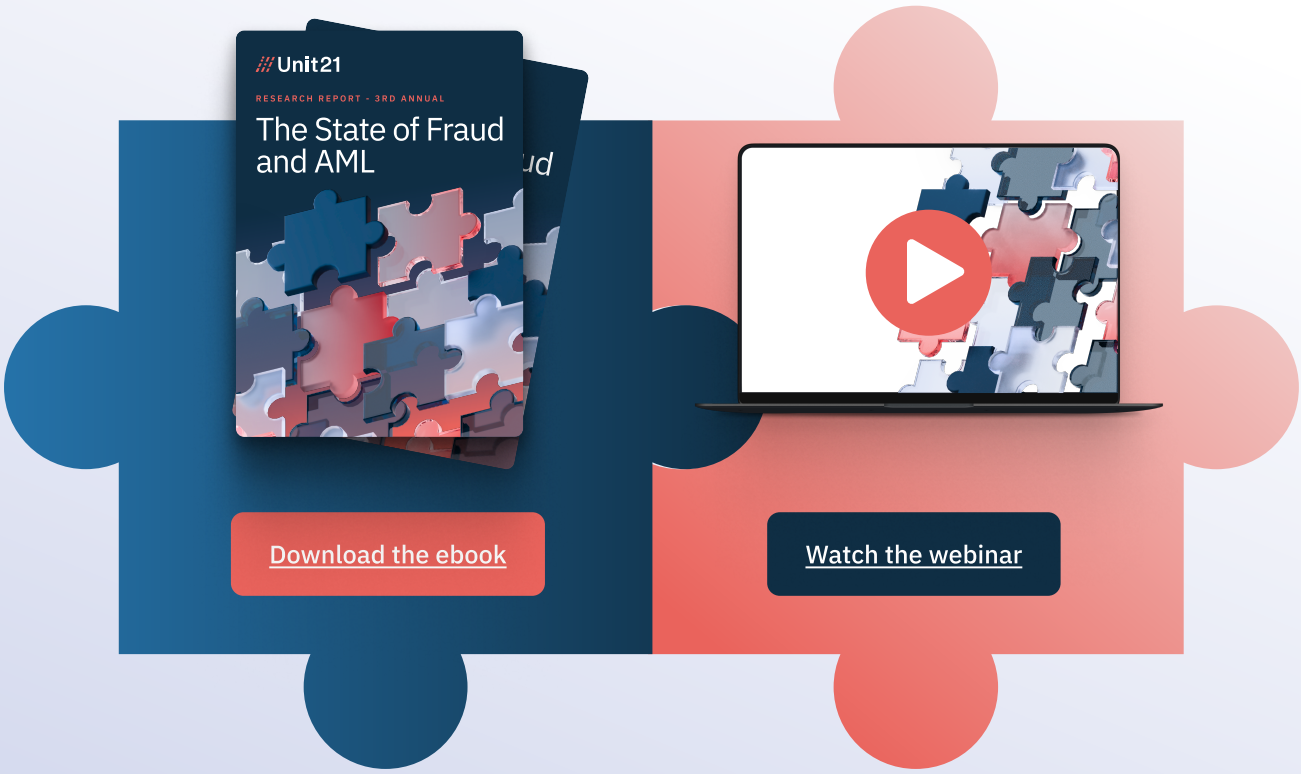


Table of Contents

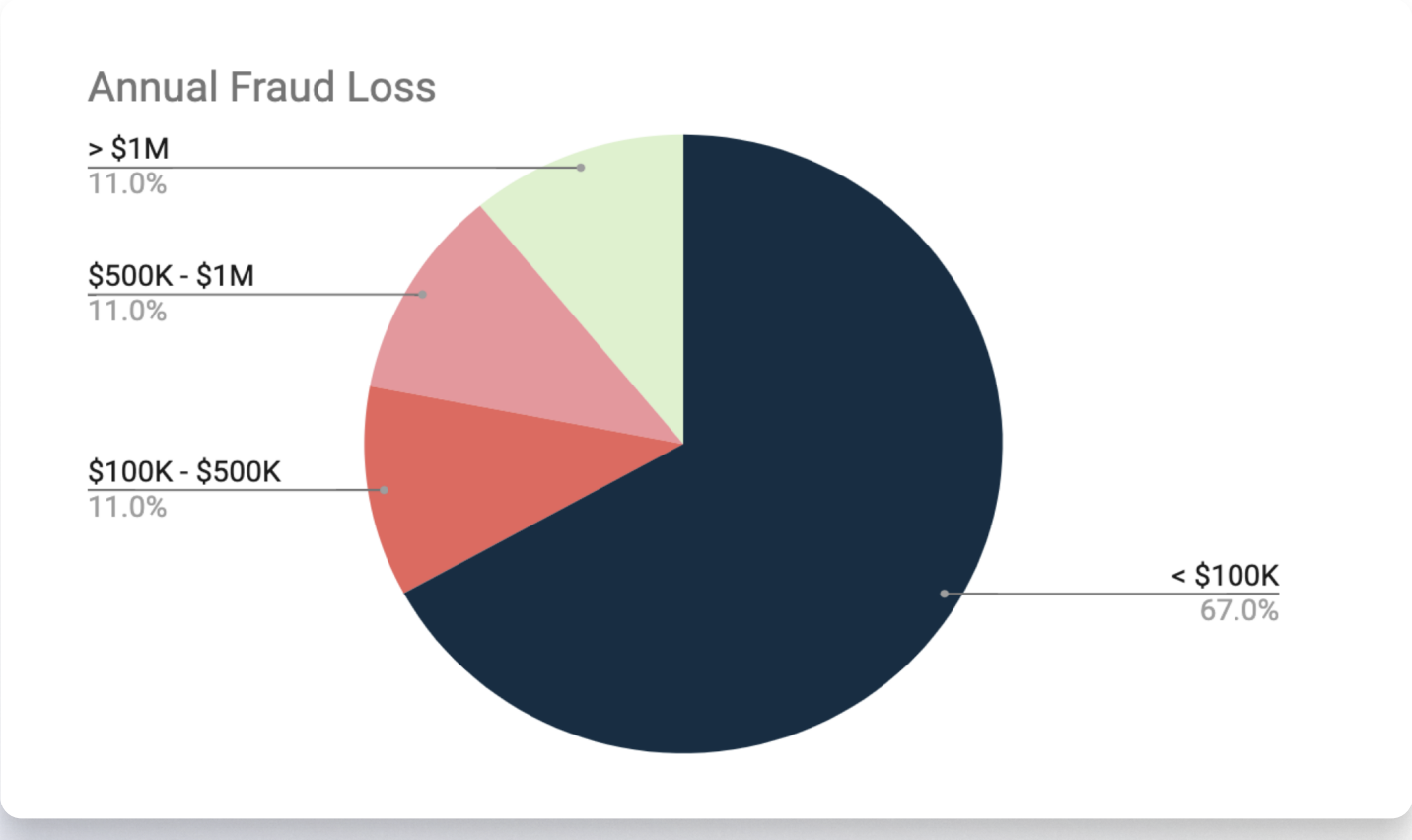
The Big Picture	03
The Looming Threat: Account Takeovers & Scams	04
The Stubborn Persistence of Check Fraud	07
Real-Time Defense: Strengthening Fraud Prevention	09
Investigative Burden Mounts	12
Who Did We Survey?	13

Unit21's 3rd annual Fraud and AML report delves into the evolving landscape of fraud and AML. This year, we surveyed over 350 financial professionals in fraud, AML, and FrAML across banks, credit unions, and fintech. This brief focuses exclusively on findings and trends across 54 Credit Unions.



The Big Picture

The financial landscape is continuously changing. Fraud is rampant and payments are moving faster than ever. Credit Unions are facing account takeovers and a rise in scam activity, costing them time and money. Check fraud also continues to plague credit unions. The ability to perform real-time monitoring (RTM) and deploy rules quickly can assist in preventing fraud losses.

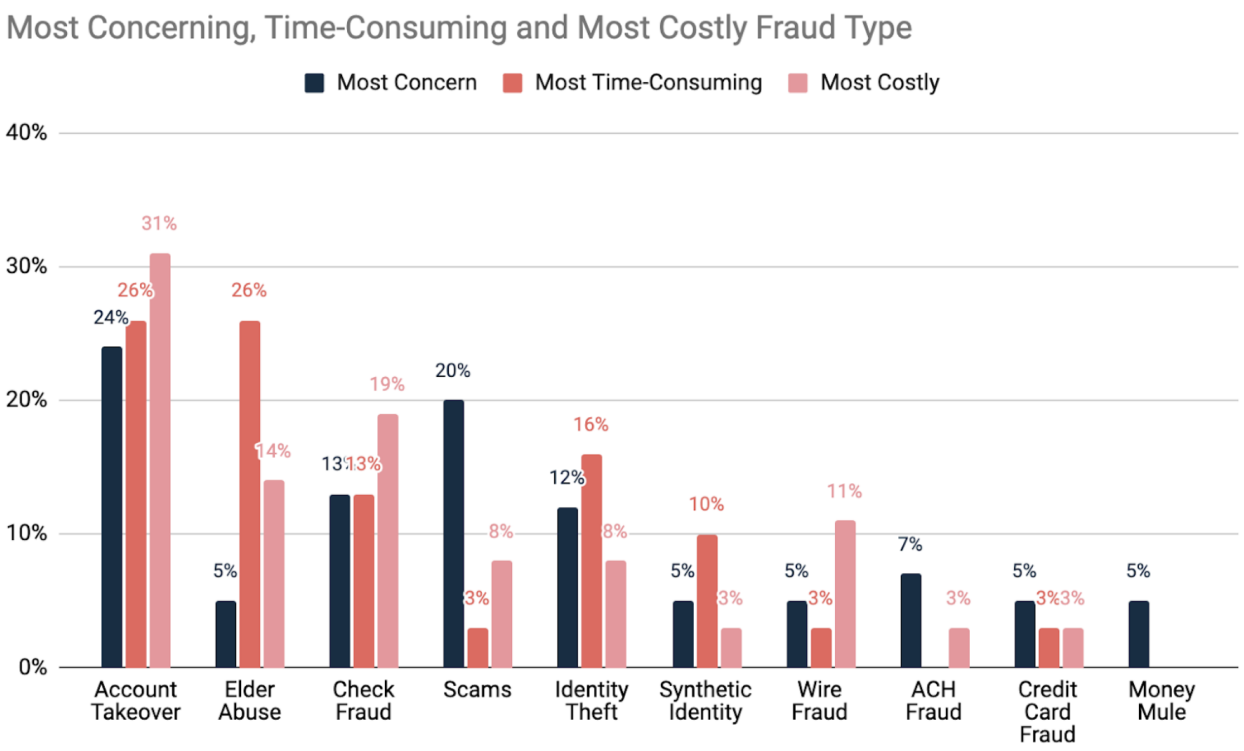


As new fraud schemes continue to arise, credit unions listed account takeovers (24%) and scams (20%) as the most concerning. When looking at most time-consuming, account takeover and elder abuse are tied at the top at 26%. Lastly when looking at most costly to the intitute, again account takeover (21%)is top of the list, followed by check fraud (19%).

TREND 1

The Looming Threat: Account Takeovers & Scams

Credit unions are facing a complex fraud landscape dominated by two prominent threats: account takeovers (ATOs) and scams. These rising threats exploit vulnerabilities in both tech and human behavior, demanding action to curb the trends.



Account Takeovers: A Concerning, Costly *and* Time-Consuming Crisis

The unauthorized access of member accounts, known as ATOs, presents a substantial financial and operational strain on credit unions. Our survey reveals that 31% of credit union respondents identify ATOs as the costliest fraud attack, surpassing other prevalent threats like check fraud and elder abuse. Account takeovers cost both money and time.

#1
most **concerning** fraud attach

#1
most **time-consuming** fraud attack
Tied with Elder Abuse

#1
most **costly** fraud attack

Contributing to the cost could also be the fact that 67% of credit unions reimburse victims. Keeping that member-first mentality is what makes credit unions appealing to customers, but can also be costly to the business.

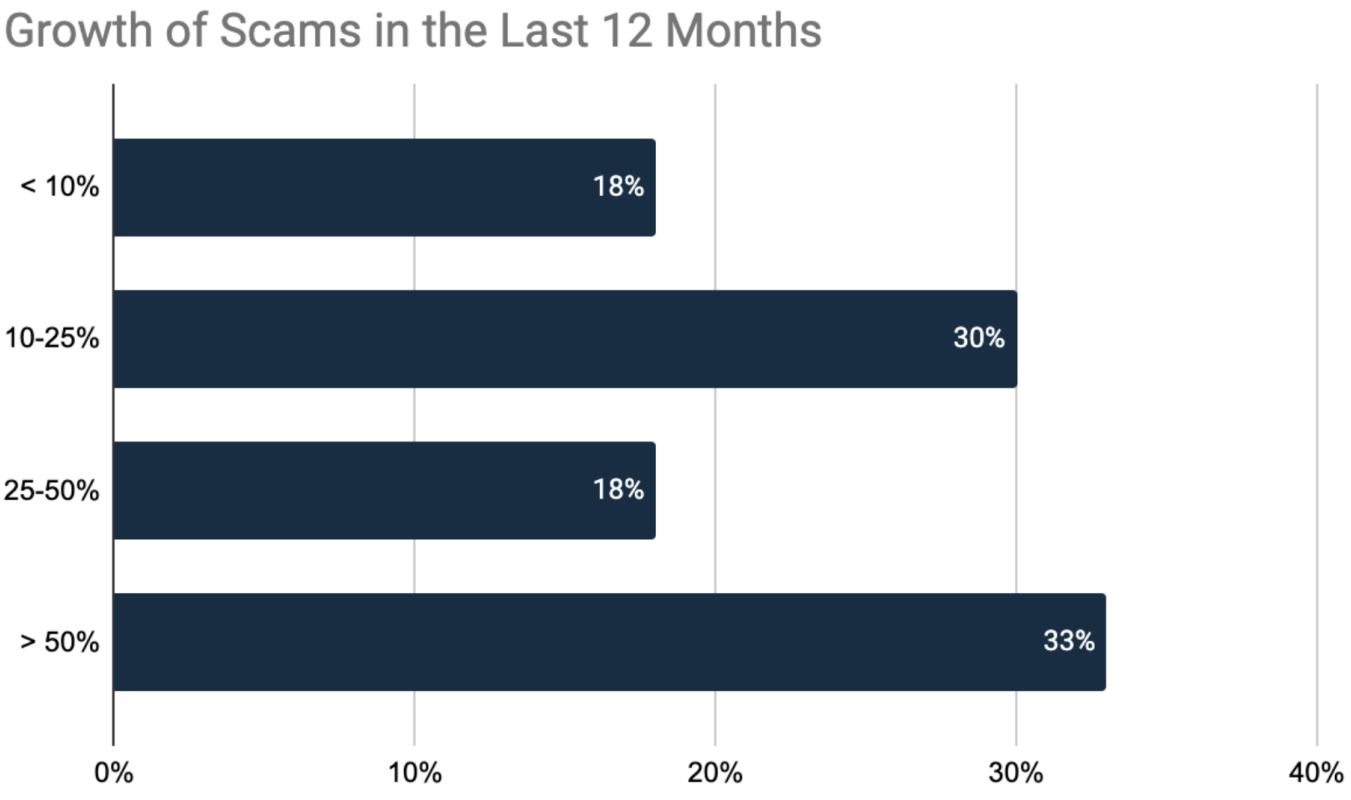
Beyond the immediate monetary losses, ATOs are incredibly time-consuming for credit union staff. Respondents were split 26% each on whether ATOs or Elder Abuse are the most time-consuming fraud cases to investigate and resolve. This highlights the complexity of ATO investigations, which often involve multiple departments and require careful analysis of transaction patterns, device information, and communication logs.

The rise in ATOs can be attributed to several factors:

- **Phishing:** Fraudsters are becoming increasingly clever in their phishing schemes, often impersonating trusted organizations or people to steal login information.
- **Credential Stuffing:** With so many data breaches happening, cybercriminals are using stolen login information from one website to try and break into accounts on other platforms.
- **Authentication:** Traditional security measures, like simple or stale passwords and security questions, leave accounts vulnerable to attack.

Scams: A Growing Epidemic

Scams, especially those designed to trick people, are a growing danger to credit unions and their members. A shocking 33% of credit unions surveyed saw these scams increase by 50-100% in just the past year. This huge jump makes it clear that credit unions need to act. They need to put strong prevention measures in place to protect themselves and their members from these evolving threats.



Among the most common scam types are:

- **Romance Scams (34%):** These scams target people seeking love. Scammers create fake profiles and shower victims with attention to gain their trust. Then they invent a crisis and ask for money.
- **Phishing Scams (31%):** These scams use fake emails, texts, or websites to trick people. They want you to give up passwords or credit card numbers. Sometimes they try to get you to download harmful software that can steal your information or damage your computer.

The success of these scams hinges on the fraudsters' ability to prey on human emotions and exploit trust.

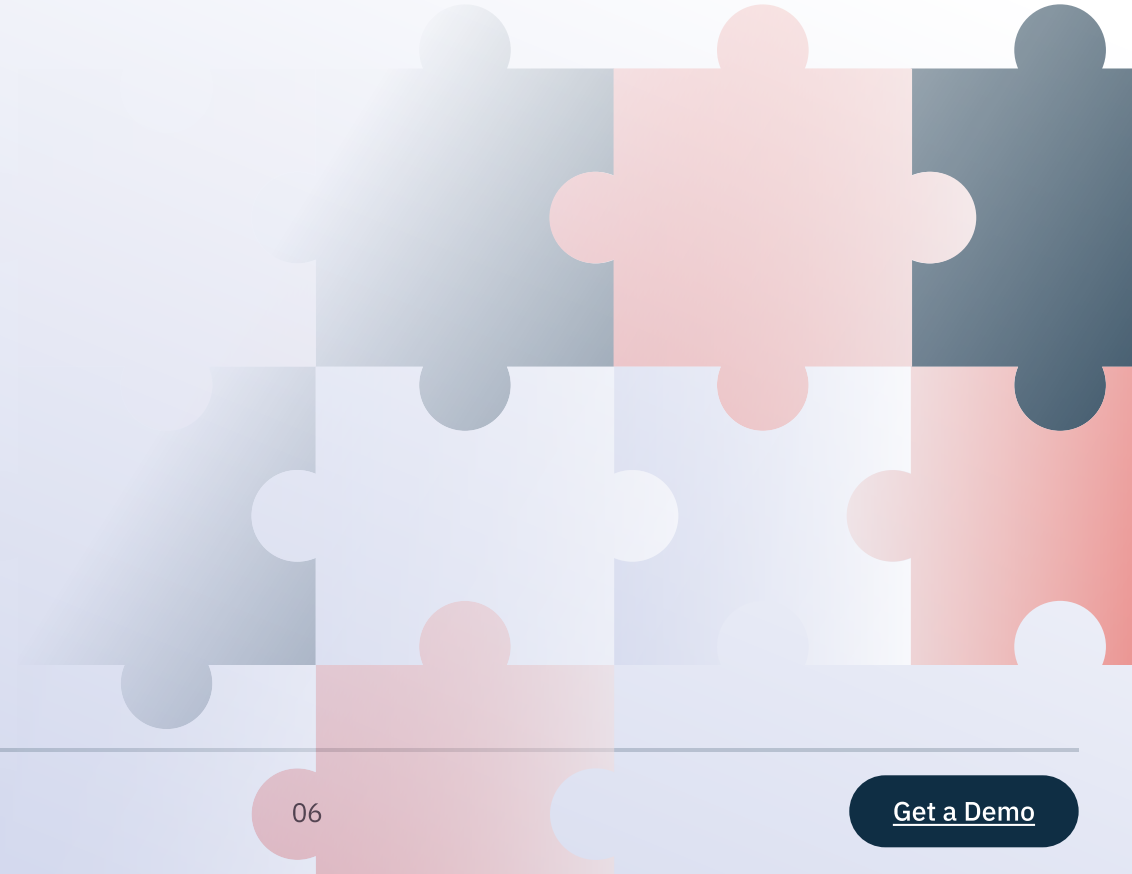
67%

of credit unions reimburse victims of scams

The Path Forward to Combating Scams & ATO

To beat account takeovers and scams credit unions need to act first and use a mix of strategies. This means:

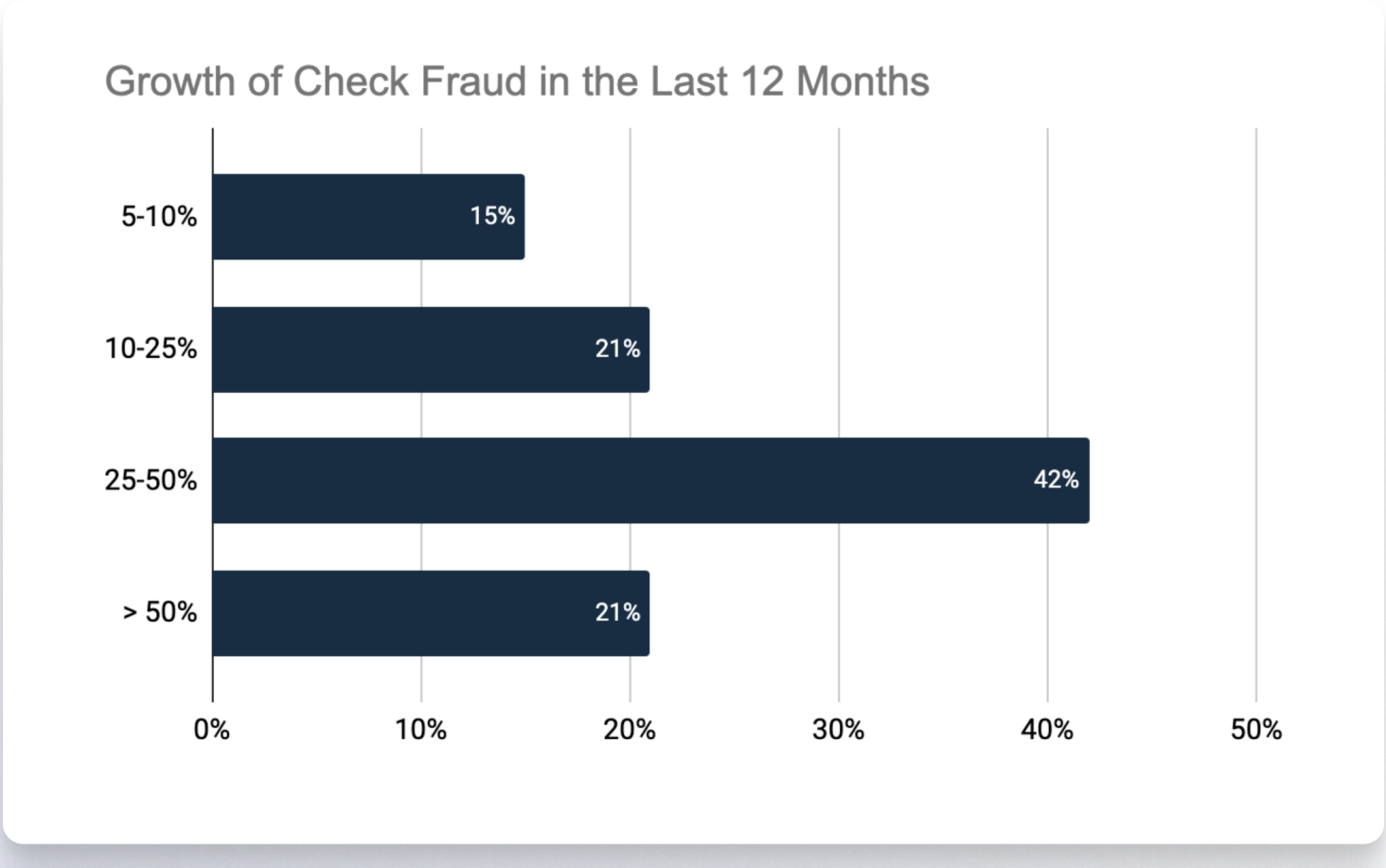
- **Stronger login security:** Using tools like multi-factor authentication (MFA) and biometrics (fingerprint or face recognition) can make accounts more secure.
- **Investing in technology:** Advanced fraud detection systems that use machine learning can help spot and stop suspicious activity immediately.
- **Educating members:** Teaching members about common scams and how to stay safe online can help them protect themselves. Credit unions should also make it easy for members to report suspicious activity.
- **Working together:** Taking advantage of consortium data to share information with other credit unions and industry groups can improve everyone's ability to fight fraud.



TREND 2

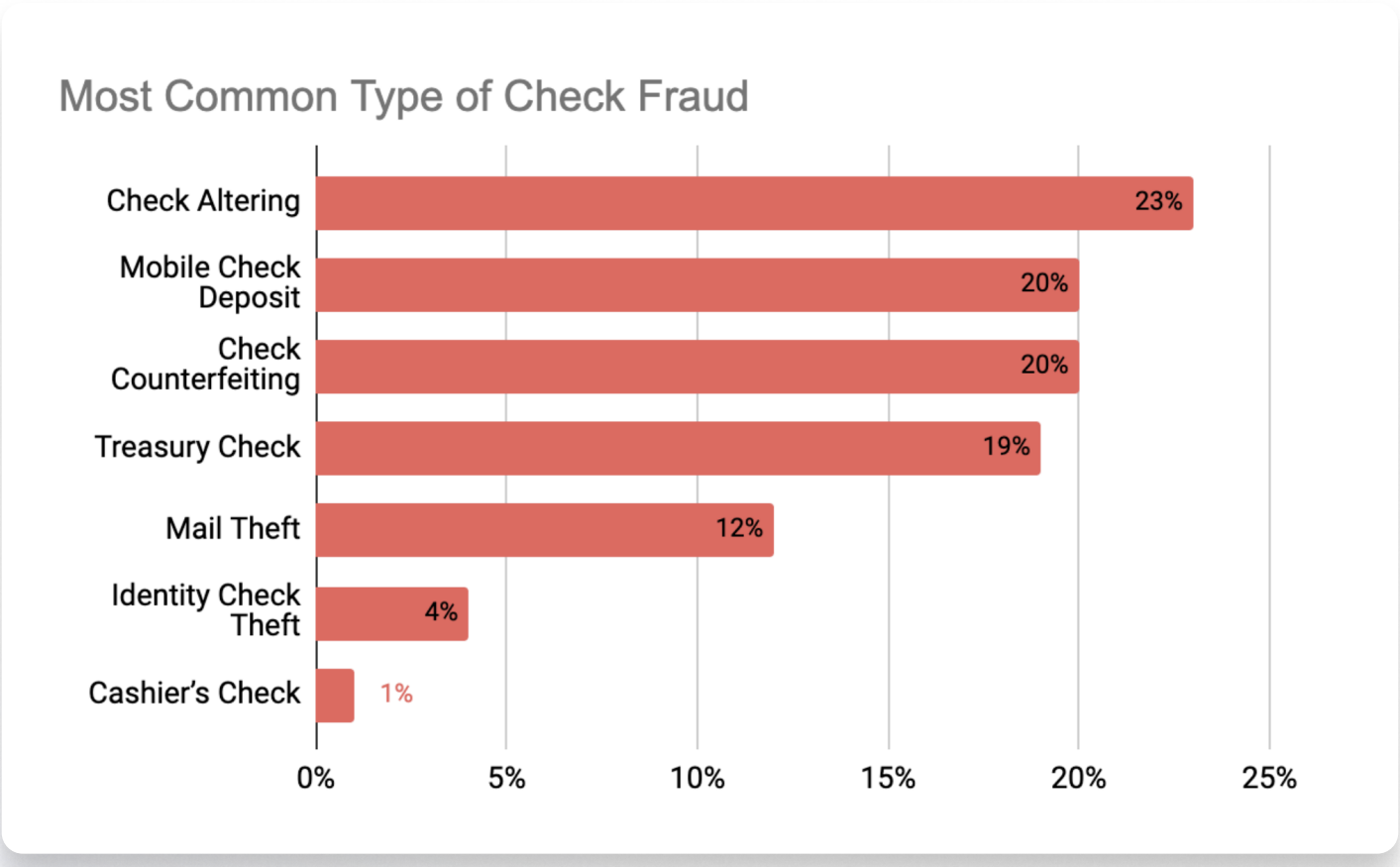
The Stubborn Persistence of Check Fraud

Even with the rise of digital payments and the mantra that “checks are dead”, check fraud is still a major headache for credit unions. Check fraud is reported as the second most costly type of fraud. And it's not trending down as one would expect - more than half (52%) of credit unions in our survey reported a 25-75% increase in check fraud in the past year. This drives a higher financial burden compared to other fraud types for these credit unions with 92% reporting annual losses of up to $500,000 due to check fraud.



Several factors contribute to this persistent threat:

- **Accessibility:** Checks are still widely used, especially by certain demographics and for specific transactions. This provides ample opportunity for fraudsters.
- **Vulnerability:** Checks can be easily altered, counterfeited, or deposited fraudulently, particularly with the rise of mobile deposit capture. Our survey showed that the most common types of check fraud are altering (23%), counterfeiting (20%), and mobile check deposit fraud (20%).
- **Detection Challenges:** Identifying fraudulent checks can be difficult, requiring scrutiny and often specialized tools.



This persistent threat demands vigilance. Credit unions need to:

- **Invest in advanced fraud detection:** Solutions that use machine learning can help analyze check images and transaction data to identify red flags and stop fraud in real time.
- **Strengthen processes:** Implement stricter procedures for verifying check authenticity, especially for mobile deposits.
- **Educate members:** Make members aware of common check fraud schemes and encourage them to monitor their accounts regularly.

By taking these steps, credit unions can minimize the impact of check fraud and protect their members and their bottom line.

The absence of RTM is likely contributing to the high false positive rates reported by many credit unions. Our data shows that credit unions without RTM experience significantly higher false positive rates (over 50% for 43% of respondents) compared to those with RTM (over 50% for only 25% of respondents). This not only wastes valuable time and resources but can also lead to alert fatigue and potentially missed instances of actual fraud.

TREND 3

Real-Time Defense: Strengthening Fraud Prevention

Our survey revealed two critical areas where credit unions have significant opportunities for improvement: real-time monitoring (RTM) and rule deployment processes. Addressing these challenges will be key to effectively combating the evolving fraud landscape.

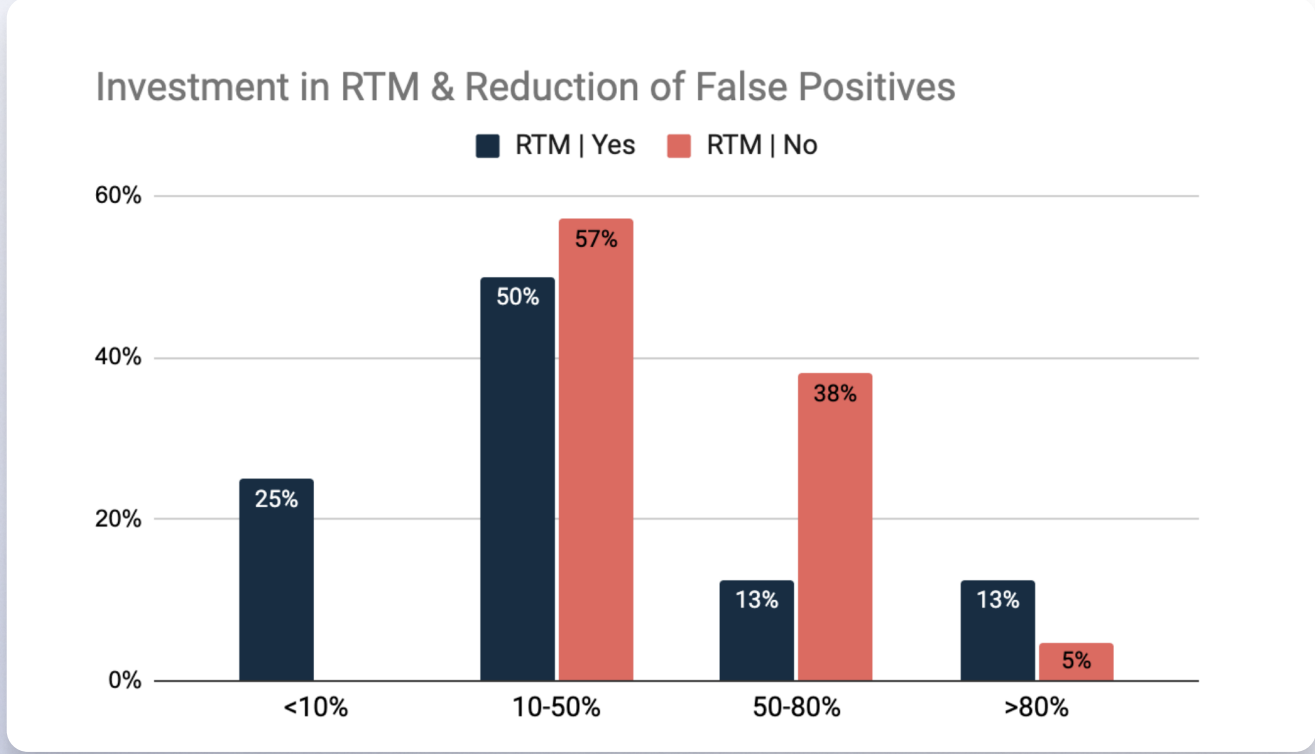
Real-Time Monitoring: A Critical Gap

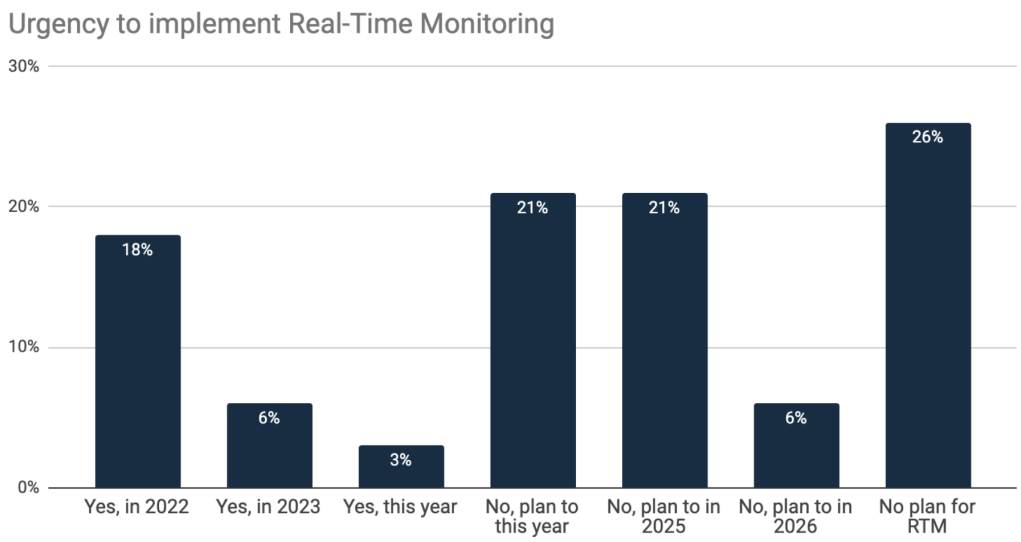
Despite the clear benefits of real-time monitoring in fraud prevention, a surprising 74% of credit unions have not yet implemented RTM software. This leaves them reliant on batch processing and manual reviews, which can significantly delay fraud detection and response.

74%

of credit unions have not yet implemented Real-Time Monitoring!

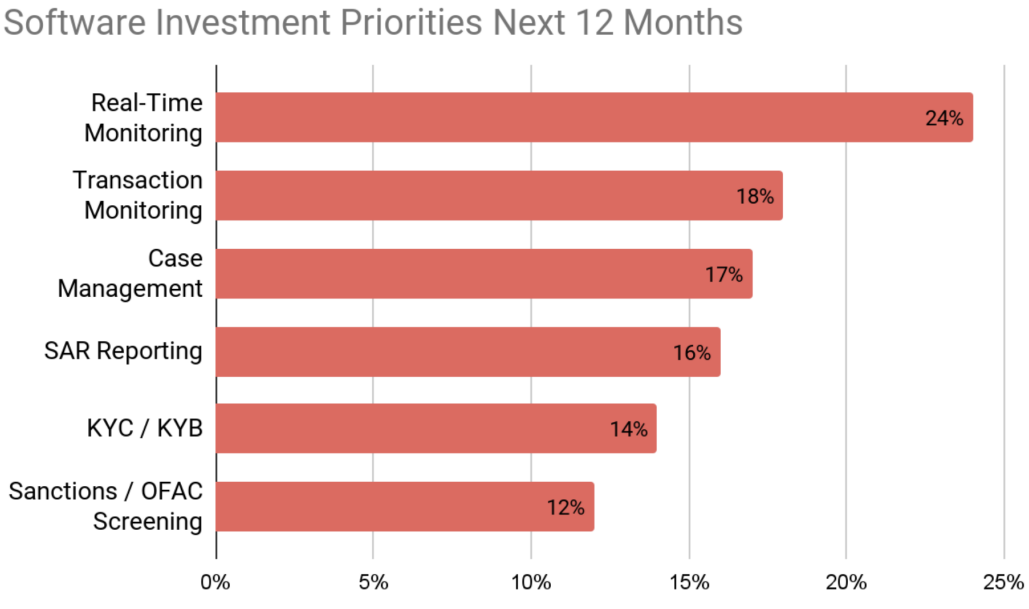
The absence of RTM is likely contributing to the high false positive rates reported by many credit unions. Our data shows that credit unions without RTM experience significantly higher false positive rates (over 50% for 43% of respondents) compared to those with RTM (over 50% for only 25% of respondents). This not only wastes valuable time and resources but can also lead to alert fatigue and potentially missed instances of actual fraud.





The good news is that credit unions recognize this gap. Nearly half (47%) plan to implement RTM in the next three years, and 24% identified RTM as their top priority for future fraud and AML software purchases. Investing in RTM solutions will enable credit unions to:

- **Detect and prevent fraud in real-time:** Identify and stop suspicious activities as they happen, minimizing potential losses.
- **Reduce false positives:** Leverage machine learning and advanced analytics to improve the accuracy of fraud alerts.
- **Improve operational efficiency:** Automate fraud detection and response processes, freeing up valuable staff time.



Speed of New Rule Build and Deployment

Using: 3rd Party Vendors

50%

those relying on 3rd-party vendors to write and deploy rules can do so **within 5 business days**

Using: Engineering

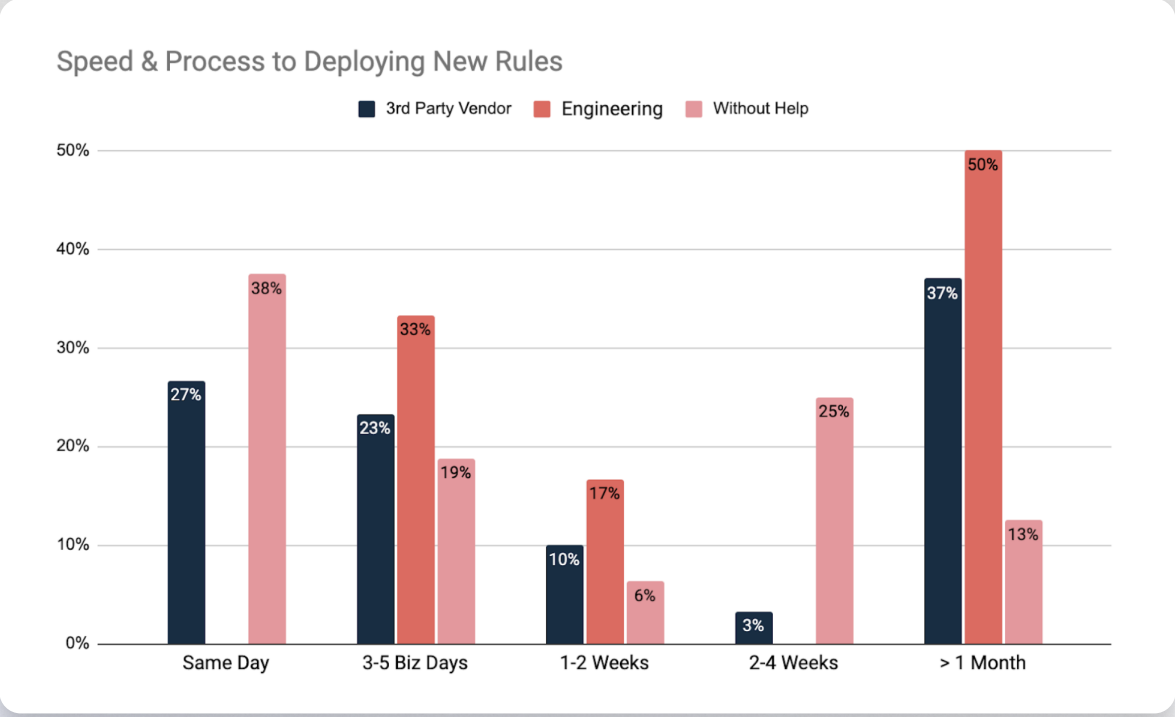
50%

those relying on engineering to write and deploy rules **take over a month**

Being Self-Reliant

57%

Those writing and deploying rules independently can get them built and live **within 5 business day**



These findings suggest that credit unions can significantly reduce deployment times by:

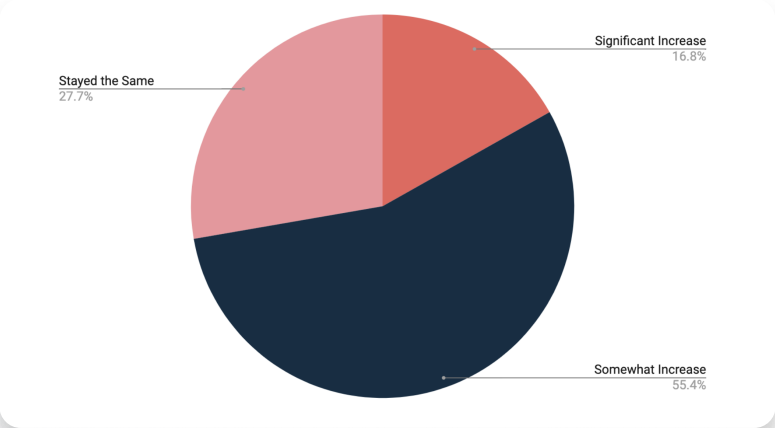
- **Empowering fraud and AML teams:** Provide them with the tools and resources to write and deploy rules without relying on engineering or 3rd party support.
- **Optimizing internal processes:** Streamline workflows and communication channels to accelerate rule implementation.
- **Carefully evaluating third-party vendors:** Choose vendors that offer agile solutions and prioritize rapid deployment.

By embracing real-time monitoring and streamlining how they deploy new rules, credit unions can revolutionize their approach to fraud prevention. It's about moving from reacting to fraud to actively preventing it. This shift will help credit unions stay ahead of fraudsters and protect both their institutions and their members in the ever-changing digital world.

TREND 4

Investigative Burden Mounts

AML investigators are experiencing more on their plate than ever before. An increase in Suspicious Activity Reports (SARs), additional alerts and the work associated with consent orders puts strain on organizations. According to our survey, 13% of credit unions are working through regulatory actions such as consent orders. There is a critical need for more efficient and streamlined investigation processes. In addition to consent orders adding more time, 73% of credit unions report seeing an increase in SAR Filings. Of those, 17% reported the increase was significant.



Over 50% of credit unions report an increase in the time spent per alert. This growing burden on investigators can lead to burnout, delays in investigations, and potentially missed opportunities to identify and mitigate financial crime.

Time Spent Per Alert Per Investigator in the last 12 months	
Increasing Significantly	**12%**
Increasing Somewhat	**41%**
Staying the Same	**47%**

These findings suggest that credit unions' staff are becoming increasingly burdened by additional work and time spent on alerts. To help ease the burden, credit unions should:

- **Take time to build out teams:** Build out proper systems, processes, staffing and tooling early.
- **Avoid thinking of compliance as a cost center:** Steer away from optimizing for cost and cutting corners. Building out a robust compliance center can help reduce financial costs in the future.

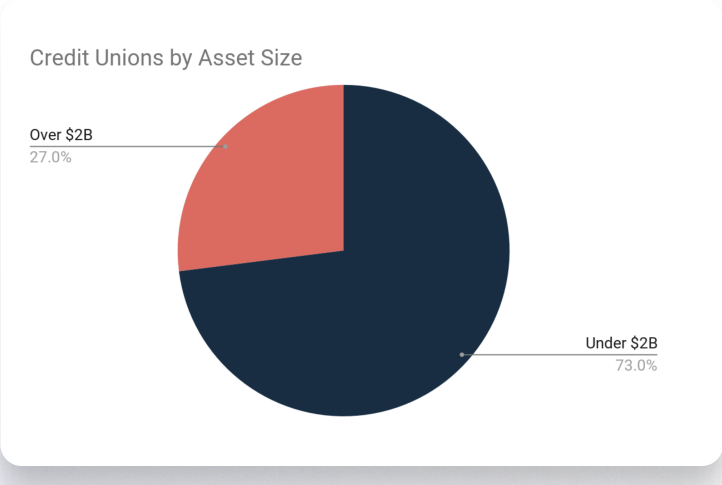
By putting the work in early, credit unions can avoid reputation risk, friction with partners, and cost associated with remediating problems. Negative consequences can occur if compliance centers are not properly staffed and have the tools necessary. It's important to build out a robust, risk-based compliance center to help avoid many potential issues.

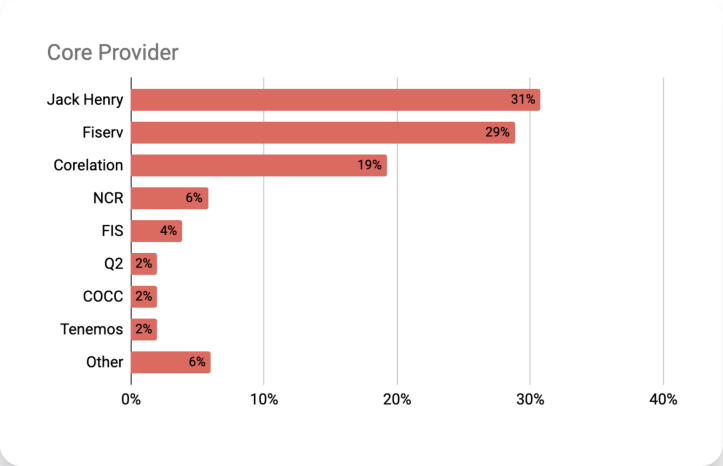
Who Did We Survey?

Methodology

We surveyed 369 fraud and compliance professionals from commercial banks, credit unions, and various fintech companies to understand the challenges facing the financial industry and learn best practices for fighting financial crime. Out of those 369, 54 were credit unions.

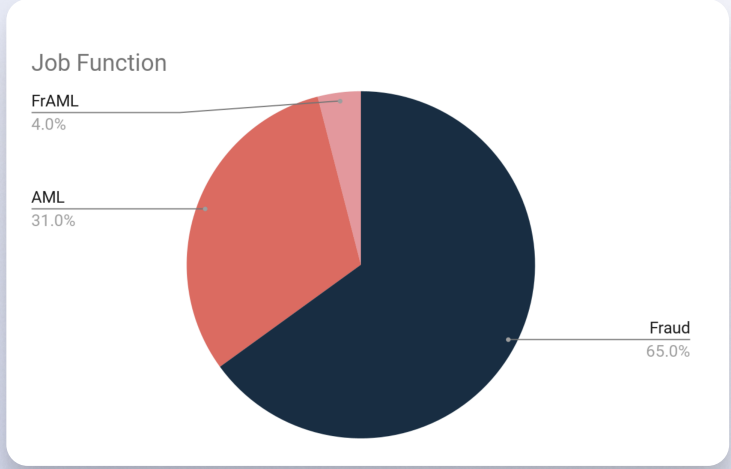
Survey Dates: June - September 2024
Survey Size: 369
Credit Unions: 54

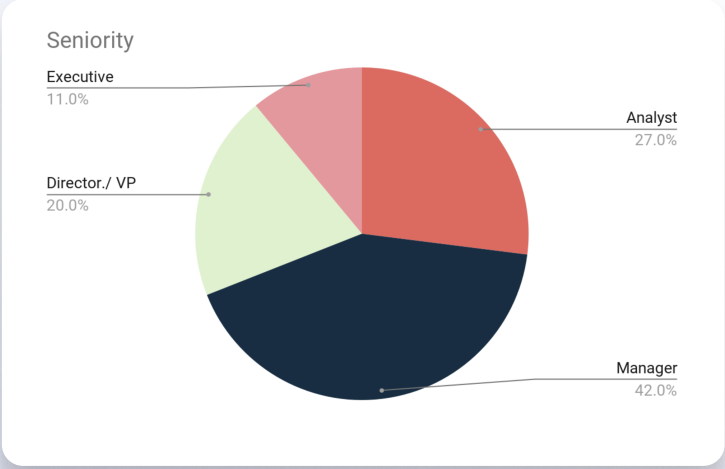




Respondent Firmographics

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, 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