GLOBAL AML RESEARCH

The road to integration

The state of AI and machine learning adoption in anti-money laundering compliance

Contents

Introduction

In just a few short years, generative AI tools have become firmly embedded in the public psyche, and the number of business use cases is growing all the time.

The emergence and rapid adoption of this technology has only intensified debates around AI and machine learning (ML) more generally in the detection of financial crimes, including money laundering. With the perpetrators of serious organized crime now using AI to deceive at scale, banks need to fight fire with fire – deploying their own AI and ML solutions to counter increasingly sophisticated criminal activities while also bringing down the cost of compliance.

Although overall adoption has been patchy, there are signs that institutions are not only piloting solutions but fundamentally changing how they work. They recognize how AI/ML can help them solve their biggest challenges, and many are planning to integrate their data, technologies and teams to get to the truth faster.

True integration may be a long way off for many institutions, but those who lay the groundwork now by adopting AI/ML solutions will be at an advantage over those who fail to do so.

But how far along are firms on their adoption journey, and where can these technologies deliver the most value? To find out, SAS, in collaboration with ACAMS and KPMG LLP, surveyed more than 850 compliance professionals and ACAMS members in 2024.

Following our first report in 2021, this report provides a snapshot of how many institutions worldwide are using AI/ML, including GenAI, their reasons for adopting (or not adopting) it, and how far along they are on their integration journey.

Key takeaways

1 Combining data in a single decisioning environment and leveraging different types of AI/ML is the first step toward integration.

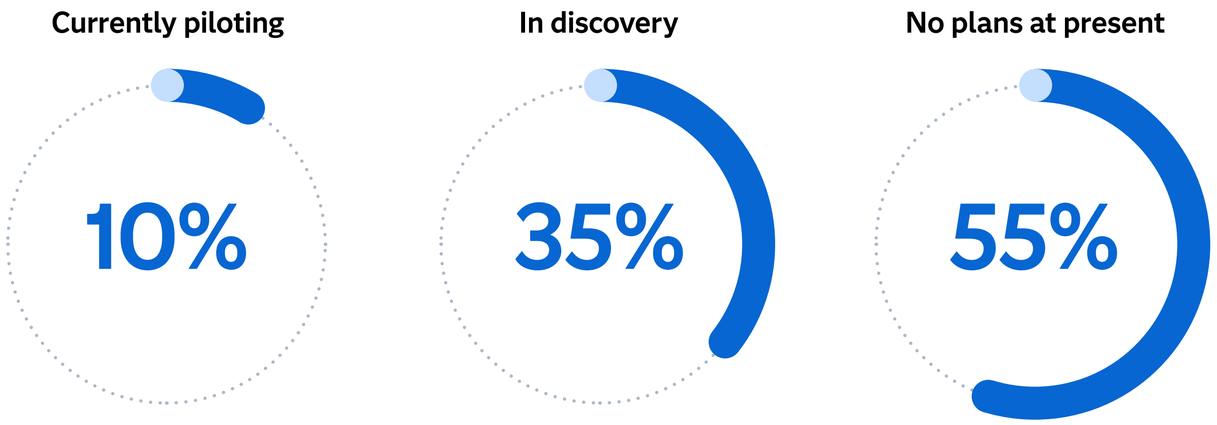
2 Change won't happen overnight, but integration will become more commonplace over the next five to 10 years.

3 Trustworthy AI is critical for adoption and integration.

Chapter 1

AI and machine learning adoption

What are your plans for leveraging GenAI as part of your financial crimes prevention strategy?



When we ran the survey in 2021, GenAI was not yet widely available, so these 2024 figures provide a new benchmark for adoption over the coming years.

Curious about the data? Explore the results at our interactive dashboard **sas.com/amlsurvey**

[1] Source: www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

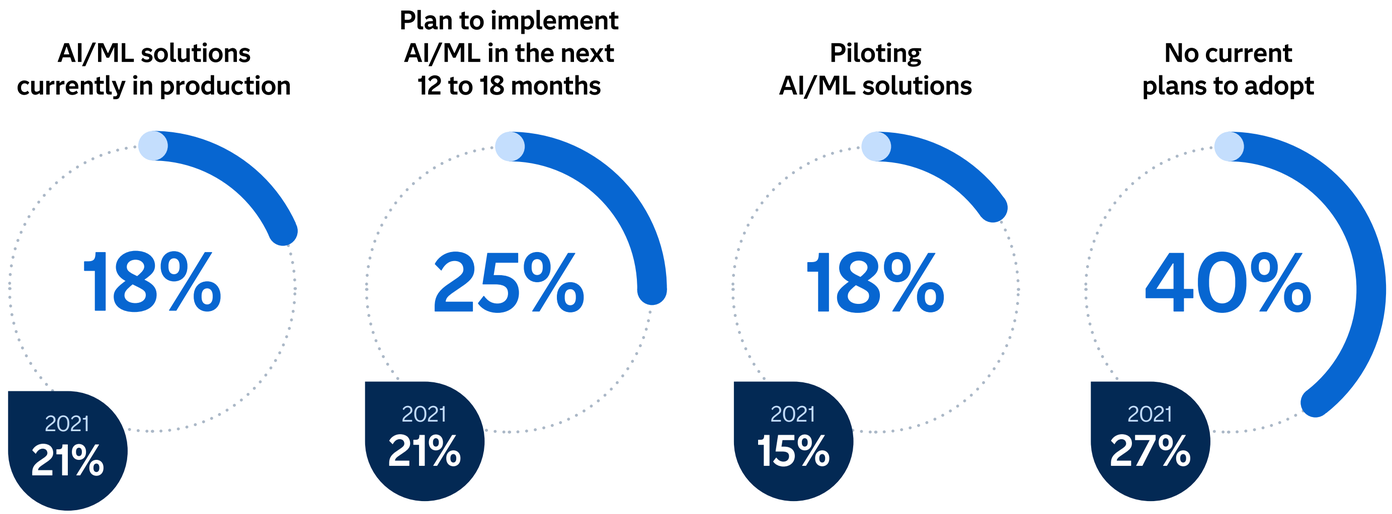
Insight

Two years after the explosion of GenAI tools, organizations are now starting to see the business value they bring.[1] This was clear from our survey. Just under half (45%) of financial institutions surveyed are either in the discovery phase or are piloting the technology.

Still, 55% remain cautious with no current plans to introduce it – possibly because of legitimate concerns about data privacy and security, transparency and biases.

Our survey also revealed marked differences between bigger (US$100 billion total revenue and above) and smaller (less than $5 billion) firms with varying IT resources. Just 5% of smaller institutions are currently piloting GenAI, while more than 63% have no plans to do so. In contrast, 17% of larger firms are piloting the technology, and only 38% say they have no plans to do so.

Which statement best describes your AML Compliance program in terms of AI/ML adoption?



(NB: 16% responded 'don't know' to this question in 2021)

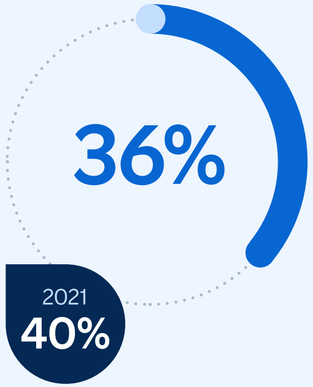
Insight

When it comes to AI in general and machine learning, the balance is tipped the other way – with more decision-makers either piloting solutions, having them in production or planning to implement them in the near future. That may be due to the availability of proven solutions specifically developed to manage large and disparate datasets and support detection, forecasting and decisioning. GenAI, on the other hand, is still new, so adoption is trailing behind.

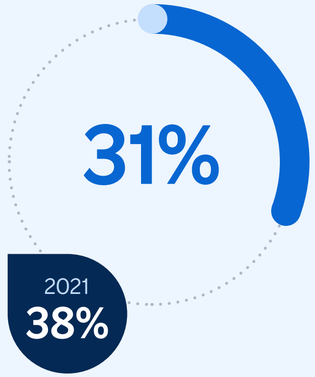
The proportion of organizations with AI/ML solutions in production has dropped compared to 2021, from 21% to 18%. The good news is that 43% say they are either piloting or planning to implement them in the next 12-18 months – up from 36% in 2021.

What is your organization's primary justification for adoption of AI/ML?

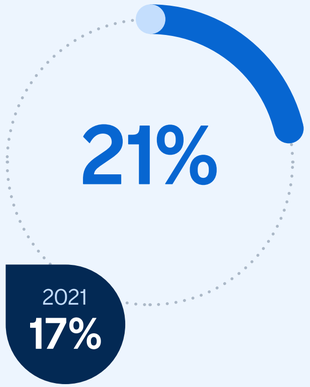
Improve the quality of investigations



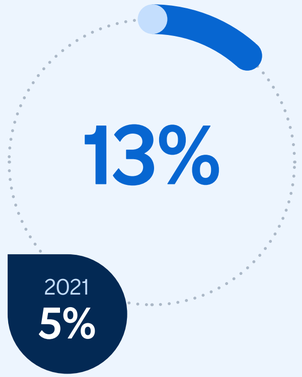
Reduction of false positives



Detect complex risks that are currently undetected

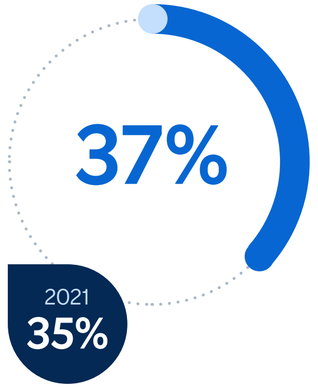


None of the above

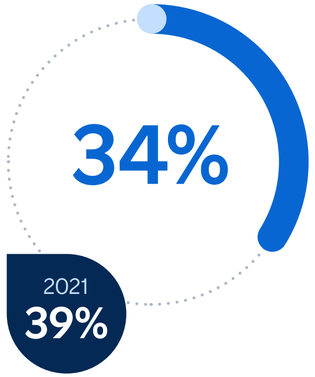


Please state the reason why you are not currently planning to adopt AI/ML?

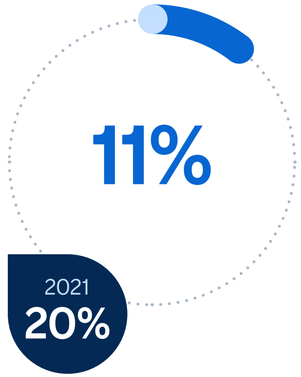
Not a regulatory imperative



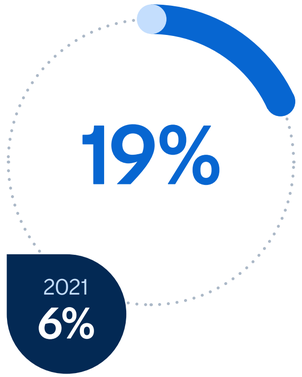
Budget



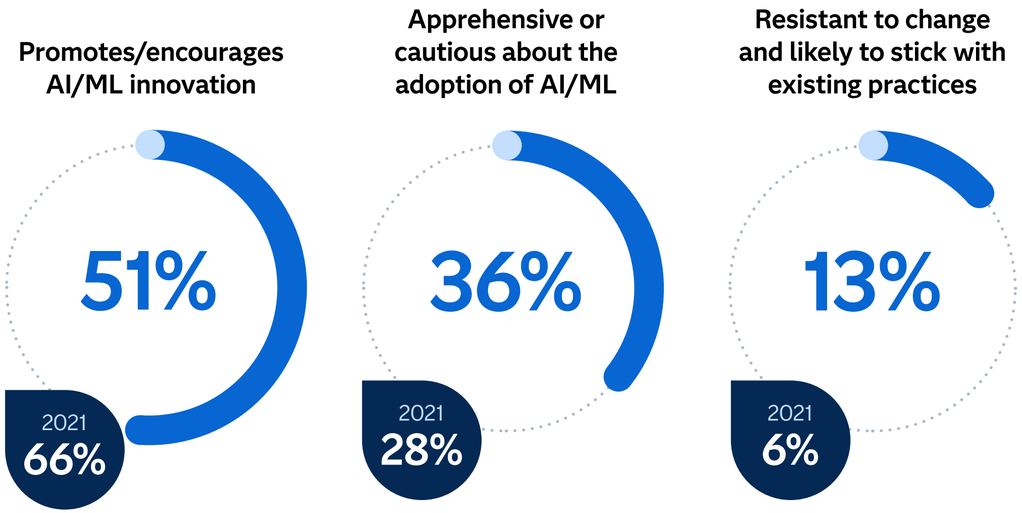
Skills



Other



Which statement best characterizes your AML regulator's current position on AI/ML?



> ***We are all on this AI journey together. Despite the myth that it's new, we've actually been using forms of AI in financial crimes for some time. If you perform negative news scanning searching for keywords, you're likely using Natural Language Processing (NLP), a form of AI. Transparency is seminal to trusted AI.***
>
> **Dan Boylan** Principal (Partner) / Head of Financial Crimes Practice (US), KPMG LLP

Insight

Decision-makers have a clear idea of the areas where AI could help – including better quality investigations and fewer false positives and negatives. In other words, they want to get to the truth faster and fulfill their regulatory obligations.

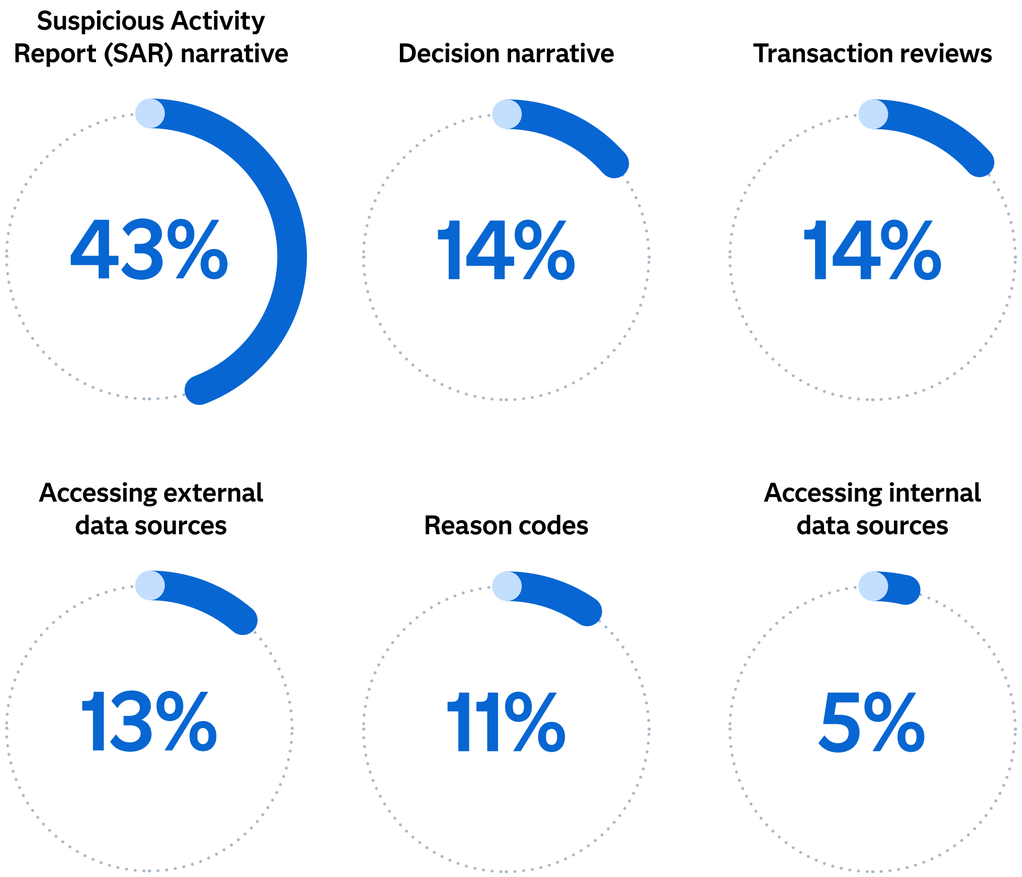
The lack of regulatory imperative seems to be the biggest roadblock for organizations not planning to adopt AI. This is despite regulators like the Federal Reserve having their own AI Program, which "promotes the responsible use of AI and enables AI-related innovation."

The idea that regulators aren't pushing AI has become more widespread since 2021. A higher proportion now believe that the regulators don't see it as an imperative (37% vs. 35%). The percentage who see their regulators promoting AI has also dropped (51% vs. 66%).

Chapter 2

AI in action

What are the most time-consuming BSA (Bank Secrecy Act) and AML compliance tasks?

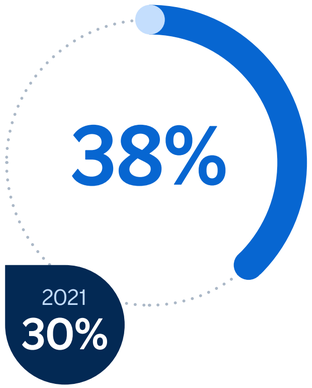


Insight

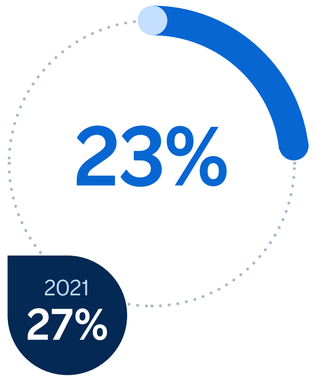
More than 40% of decision-makers cite Suspicious Activity Report (SAR) narratives as their most time-consuming compliance task. It's far more time-intensive than other compliance tasks, such as decision narrative (14%) and accessing data, both external (13%) and internal (5%). Natural language generation (NLG) – a type of AI linked to NLP – could drastically reduce the time it takes to produce SAR narratives by turning data into readable reports.

What are the priority areas for AI/ML deployment?

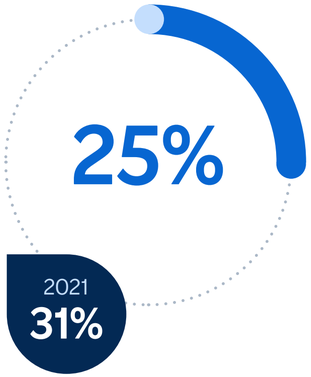
False positive reduction of existing surveillance system(s)



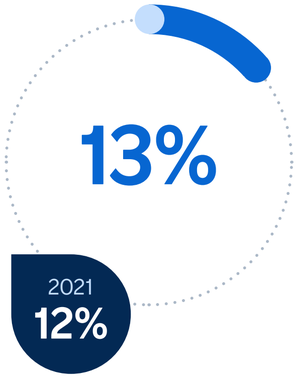
Detect new risks with advanced modeling techniques



Automate data enrichment for investigations and/or due diligence



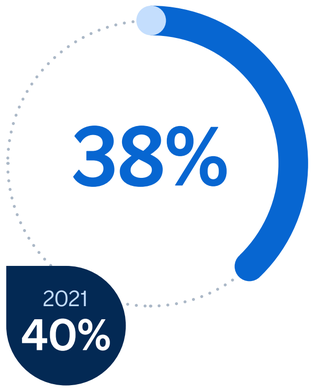
Customer segmentation for behavioral analysis



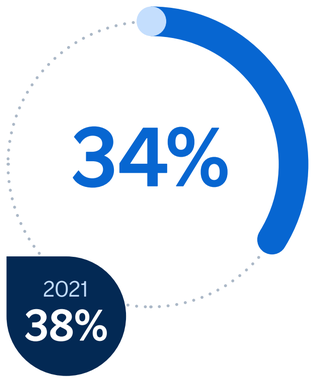
Curious about the data? Explore the results at our interactive dashboard **sas.com/amlsurvey**

Which of the following areas currently offers the most value for your organization in terms of deploying AI/ML? Select one.

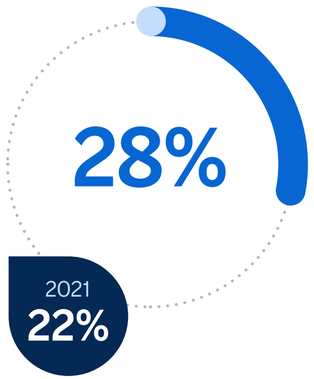
TM platform (reduce false positives and negatives at the source)



Investigations (get to a better answer more quickly)



Triage (classify high- and low-risk alerts before they are touched)

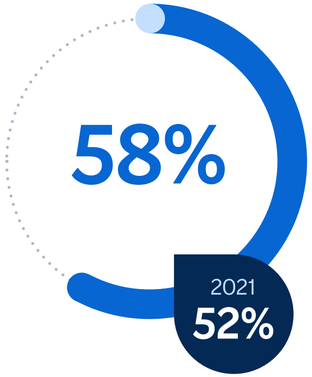


Insight

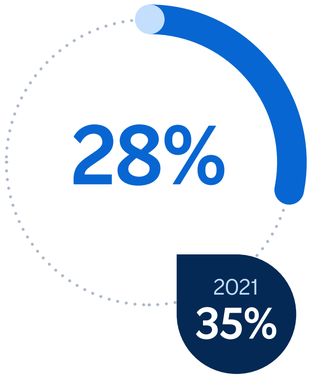
Financial institutions that reduce their false positive rates can expect higher revenues. So, it's no surprise that decision-makers see false positive reduction as a priority area for AI/ML and believe that the technologies will have the most impact at the source. They also recognize that AI/ML can identify new risks and get to the truth faster.

Please rank the following technologies from 1 to 3 in terms of which would have the greatest impact on your institution.

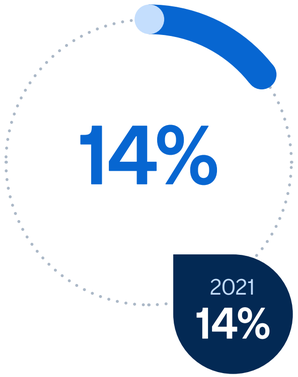
Machine learning



Robotic process automation (RPA)



Natural language processing (AI)



Insight

Machine learning is expected to have the biggest impact because it can proactively identify ‘hidden’ patterns in large amounts of data. This was evident in 2021, but the proportion is even higher today.

By continually optimizing models, compliance teams can improve the accuracy of their results and stay alert to new threats. RPA, the next most impactful technology, is also well-suited to financial crime detection since it can derive insights from raw data, detect real-time events and automate and manage decisions using AI.

But what about NLP, a type of AI that turns unstructured data (such as human language, both text and speech) from disparate customer communications into valuable assets? The fact that relatively few respondents ranked NLP first suggests compliance teams may be missing early warning signs because they haven’t built up their NLP capabilities. Natural language generation, a subfield of AI and a type of GenAI, could also cut the time it takes to produce narratives for SARs.

Case study: Deutsche Kreditbank AG

The second-largest direct bank in Germany, Deutsche Kreditbank (DKB), relies on online banking for its private customer business.

"The expectations of the customers are changing rapidly – they expect service in real time and maximum security. At the same time, they're open to various types of online transactions.

We take great measures to protect our customers from fraudulent transactions, and, of course, we will ensure this for the future.

In times of digitalization, banks must focus on innovating in the fight against fraud and money laundering. Therefore, we're using an analytical SAS platform to be able to act and react even faster.

Everything comes together to guarantee that the number of false positives remains as low as possible. Ultimately, we wish to not suspect a single respectable customer.

SAS isn't an out-of-the-box solution, and that's exactly what we wanted. With the help of SAS, we can personalize every single screen and every process, thus satisfying the needs of every department involved.

First, DKB has succeeded in offering a particularly high standard of safety combined with fast and innovative customer service. Second, the platform is so effective that the compliance department has ultimately changed from a cost center to a profit center.

Not only do we secure our customers' money, but we also win their trust. Our new, ultra-modern solution uses an extremely efficient system that not only enables Workplace 4.0 in the area of compliance but also provides for improved efficiency in many of the bank's units."

Head of Compliance,
Deutsche Kreditbank AG

DKB
Deutsche Kreditbank AG

Read more: Deutsche Kreditbank AG combats fraud and money laundering with SAS®

Smarter analysis – and smarter investigations

Timo Purkott, Partner, Global Fraud and Fincrime Transformation Lead, KPMG LLP

The financial crime landscape is constantly shifting – partly due to geopolitical tensions and new sanctions, but also because perpetrators are becoming more sophisticated in their use of technology. Regulators are now focusing more on money laundering, so there's an increased compliance risk, too. All this translates to an upward trend in the cost of compliance as caseloads have become bigger and more complex.

At times like these, institutions can find themselves in firefighting mode because they haven't had time to strengthen their processes as compliance priorities changed.

AI and machine learning won't solve all these challenges by themselves. However, they are proving to be effective when applied to elements of the detection process – specifically, where there is repeatable work and large amounts of data. This includes case handling based on the alerts generated from transaction monitoring and optimization of the sanctions screening. As well as being more efficient, automation can also lower the risk of human error. For example, we've observed quite significant variations in the quality of alert handling depending on the time of day or day of the week. This isn't the case when you use AI or ML.

We're also seeing more broadly how AI and ML can help directly support financial crime investigations. Moreover, we help organizations pilot an enterprise-wide assessment using large amounts of data to create quantitative analysis and use this to come up with an overall risk assessment. Reporting suspicious activities, AML checks and KYC – these are all use cases where information processed by AI and ML and enriched by human analysis could be highly effective.

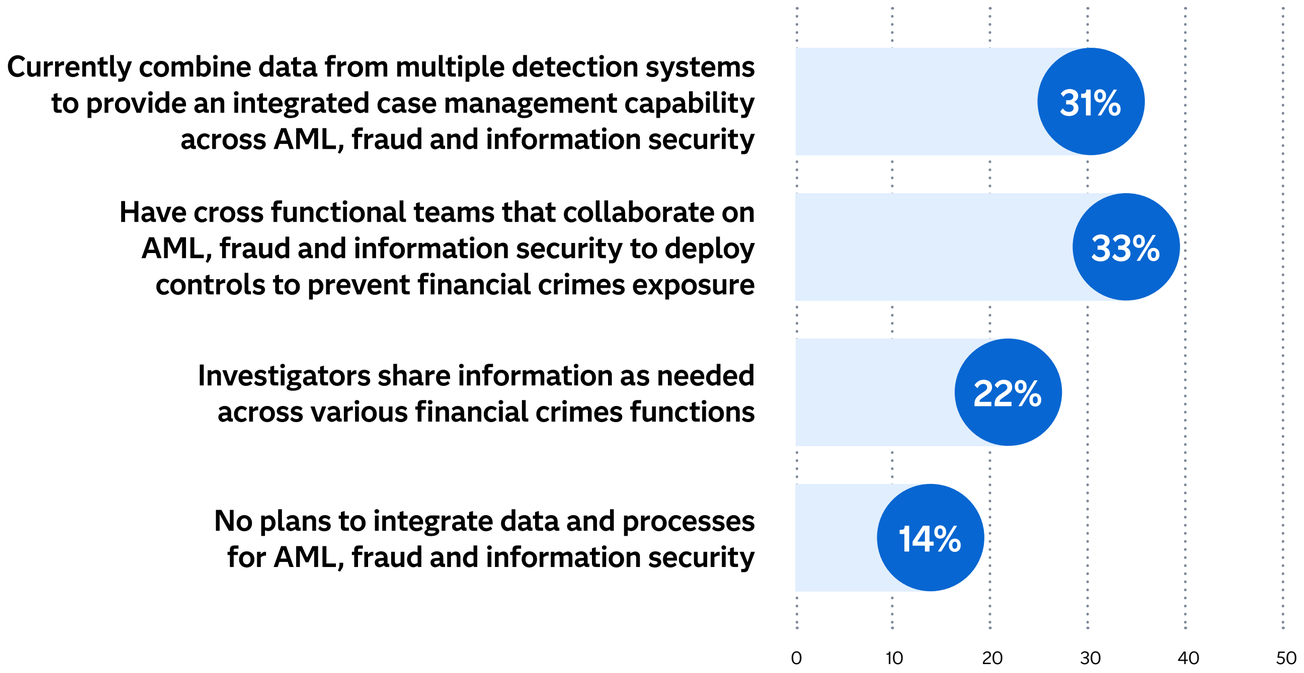
Reducing false positives is a key priority for risk managers, and the rise of advanced technologies allows us to rethink the concept of monitoring risks holistically. When you apply a specific rule-based system and a certain dataset, you need to classify and evaluate each signal as an alert, which may result in a huge number of false positives. With AI and ML, you will be able to analyze anomalies and signals more broadly and consider these as a trigger to more in-depth analysis, but not every signal needs to be an alert: it can be indicative of a wider trend. This should result in smarter analysis and smarter investigations.

Ultimately, it's a data game. Institutions need to enhance their data management framework so they have more data sources but also better data quality and analytics that can be accessed quickly. This is essential to cope with both current and upcoming regulations. Pre-analysis of this data is also an absolute; teams need to be able to intelligently identify anomalies and signals and not be limited by rules. Perpetrators of financial crime often don't limit themselves to one type of crime or technology – and neither should we.

Chapter 3

From adoption to integration

How would you describe your state of integration between AML, fraud and information security processes?



Insight

Respondents overwhelmingly see the benefits of sharing information, even if they're at different stages of the journey.

More than 20% of respondents are sharing information on an as-needed basis, while one in three now have cross-functional teams working together to tackle financial crime. More than 30% now have an integrated case management capability, linking AML, fraud and information security – rising to 34% among the biggest organizations surveyed ($500 billion and above). Smaller firms are further behind in terms of integration, though not worryingly so. In fact, nearly 29% of firms with less than $1 billion total revenue have the capability.

Budget and skills are two of the biggest barriers to deployment – and they are just as applicable to integration, if not more so. Forward-thinking decision-makers recognize this; more than half (54%) believe advisory firms and/or technology vendors are the best source for industry best practices on the adoption of AI/ML. In contrast, just 22% said industry trade organizations are the most trusted source.

Case study: Bangkok Bank

We were looking for an enterprise solution that allows us to apply a more advanced score-based approach to risk-rate our customers; a tool to enable us to apply different threshold values appropriate to each segment in terms of customer type, risk level and product used; and most importantly, a solution that allows us to centralize AML decisioning in a standardized AML case investigation workflow.

Suteera Sripaibulya,
Senior Executive Vice President of IT at Bangkok Bank

Read more: Fighting financial crime through a global anti-money laundering platform

Bangkok Bank

"Understanding AI's capabilities is foundational to the entire conversation"

Dan Boylan, Principal (Partner) / Head of Financial Crimes Practice (US), KPMG LLP

We often talk about different types of financial crime – like fraud, money laundering and cybercrime – in general terms, but they are all materially different activities. The idea that teams within financial institutions can always work together in harmony and realize this great synergy doesn't always work because their processes, technology, data and the speed at which they work are so different.

As a result, we have to be more surgical in how we approach them. For example, a unified case management system that cuts across the different disciplines coupled with common data pools can be extremely valuable. What's critical is being able to evaluate the data you have, how it's used and how it can meaningfully help mitigate the financial crime risk. Data in columns and rows versus data curated in a way that lends itself to advanced analytical capabilities makes a big difference.

If you pay close attention to the regulatory actions in our industry, you'll see many failures are due to operational risk (eg, too many handoffs, disparate systems, or holes in the data lineage). That's why the industry is taking a keen interest in AI's capabilities. But most importantly, you really want to have a deep understanding of the different types of AI and what problems you are trying to solve, rather than getting caught up in buzzwords. It is incredibly important that understanding AI's capabilities is foundational to the entire conversation – and can help to overcome the hesitancy people have about advanced technologies.

Explainability is extremely high on the list of concerns because if you can't crisply explain what you're trying to accomplish by using these techniques to internal and external stakeholders, you'll likely face resistance. At a minimum, you'll need to explain the model's intended use, limitations, how you addressed bias and desired outcomes.

On the explainability front, the CEO and board usually set the tone on whether AI and machine learning is something they want to pursue, and there are variations across different institutions.

Finally, there are a lot of discussions on LinkedIn and industry forums about jobs being displaced by AI. Even with AI's advanced capabilities, you'd be hard-pressed to replicate the deep knowledge and nuanced understanding of an expert financial crimes investigator. So, it's not about replacing experts but using AI as an accelerator – a complementary tool. You need a human in the loop. In fact, subject matter experts are the most important part of this whole equation because they can understand what they're doing and explain it to internal and external stakeholders and regulators in plain English.

Chapter 4

Key takeaways

1

Combining data in a single decisioning environment, and leveraging different types of AI/ML, is the first step toward integration

David Stewart
Director,
Financial Crimes
& Compliance,
SAS (retired)

The huge rise in fraud, including romance and crypto investment scams – and the money laundering that often follows – is driving greater integration of teams, technologies and even institutions across borders. Since perpetrators traverse different types of financial crime, institutions are increasingly looking to remove their own silos and bring investigations together on a common case management system.

Given the threat of financial crime, I remain surprised that machine learning hasn't been adopted more aggressively. But that requires additional data science skills that only the larger banks have the resources and funding for. What's changing, though, is the availability of low-code/no-code platforms, with graphical user interfaces that allow investigators to work individually or collaboratively to orchestrate data from multiple sources (including non-monetary data). The layering of other technologies, such as NLP, can enhance contextual awareness – so any suspicious activity logged by one department can be used by another to build a case. We are also seeing regulatory expectations to perform compliance checks in real time to address nefarious activity by shell companies and sanctioned entities.

The final frontier is being able to proactively manage AML, fraud and infosec events within a consistent decisioning environment – so that teams can detect and prevent financial crimes before they're inside the institution. This covers everything from authentication, identity and verification to credit and fraud decisioning.

We know that criminals operate across borders – but data privacy laws, including GDPR, have always made it difficult to share data. Indeed, transnational criminal organizations often exploit this, depositing their cash in different institutions to avoid arousing suspicion. That could all start to change over the coming year, particularly with the EU moving to a central AML regulator.

I'm also excited by the application of GenAI in creating synthetic data to mimic the activity and behaviors of criminals while protecting sensitive customer information. It would give banks access to extremely valuable consortium data by asking their counterparts what kind of suspicious activity they've been detecting and then simulating their own scenarios. We are piloting the generation of synthetic data internally and have seen considerable benefits.

2

Change won’t happen overnight – but integration will become more commonplace over the next five to 10 years

Christopher Ghenne
Global Lead, Banking Compliance Solutions, SAS

Around 99% of the people I meet in the industry recognize that they need to break down silos in financial crime detection teams, even if a truly integrated AML function is still a work in progress. But we are seeing some great examples of what it could look like. We are working with large institutions to develop new decisioning architecture that allows them to identify and monitor activity across different areas with a much higher level of accuracy across the entire life cycle of customers.

The biggest barrier to this is legacy systems with disparate data sources. They might have entirely different systems for customer onboarding, banking and loans – so that’s already three sources of data to reconcile before teams get a 360 view of their customer. While this is a long-standing problem among established banks, it’s also being felt by the newer digital-first banks, which have quickly amassed large amounts of data.

Change won‘t happen overnight. It could take years to build the data lakes. But over the next five to 10 years, we can expect to see much more integration. A common platform with a single source of data, and the application of AI could transform entity resolution processes – as long as the data is good quality. It doesn’t matter how advanced your decisioning architecture is; you need to be able to process the data effectively first.

3

Beth Herron
Americas
AML Lead,
SAS

Trustworthy AI is critical for adoption and integration

Artificial intelligence and machine learning are rapidly becoming the standard for detecting financial crime. Industry-leading monitoring programs take a hybrid approach using behaviorally segmented rule logic, anomaly detection and model-based detection – all informed by AI/ML.

Modern approaches exist on a spectrum, and we are seeing the appetite to adopt drop off as complexity increases. Decision-makers must weigh the value of more sophisticated approaches against heightened model risk management expectations. More governance and control are needed to effectively manage models – so while you may gain efficiencies on the investigative side, it's a trade-off.

For greater adoption of AI, trustworthiness is paramount. Trustworthiness requires a comprehensive approach that spans robust data governance, model interpretability and ongoing model governance. Heightened regulatory expectations can increase the cost and complexity of managing these assets compared to traditional rule-based strategies. Without proper guardrails, unintended consequences can negatively impact customers at an amplified scale.

The good news is these challenges are not insurmountable, and technology is helping financial institutions meet the regulatory expectations that come with moving AI from pilot to production. It is interesting that some of the same innovations enabling us to accelerate and scale human decisions are also helping us govern more effectively. For example, copilots are accelerating model development, language models are providing automated model documentation, synthetic data generation is helping reduce information security risk, and autogenerated model cards are bringing transparency to all levels of the organization so that everyone can participate in building a trustworthy AI culture

It's an exciting time to be working in the anti-financial crime space, and with trustworthy AI, we can unlock the promise held in these advancements.

Conclusion

The adoption of AI/ML has been slow, which is entirely understandable in a highly regulated industry like financial services. Since 2021, adoption rates have grown, albeit marginally, and the appetite for AI is relatively high, given its novelty.

There are unsurprising differences between how quickly institutions of different sizes are adopting AI/ML solutions, though the gap isn't as big as you might expect. This could be down to the availability of low-code/no-code platforms, which give even smaller compliance teams the ability to manage their data using AI/ML tools within a single standardized environment.

Those embracing AI/ML are clear on the challenges it can solve and are forging ahead with plans to integrate their key compliance processes.

Of course, there is still plenty of work to be done to reassure those who have yet to adopt these technologies. The lack of regulatory imperative stands out as the biggest barrier so far. Yet, the light-touch approach from some regulators isn't a sign organizations should sit back and do nothing. Instead, it's an opportunity to innovate and form longstanding partnerships among internal teams, consultants, vendors and regulators. AI, in particular, can feel like uncharted territory. When applied responsibly, though, it has the potential to totally transform compliance processes.

Curious about the data? Explore the results at our interactive dashboard: **sas.com/amlsurvey.**

Learn more about how SAS can help your organization **combat fraud and financial crimes**

About ACAMS®

ACAMS is a leading international membership organization dedicated to providing opportunities for anti-financial crime education, best practices, and peer-to-peer networking to AFC professionals globally. With over 115,000 members across 200+ jurisdictions and territories, ACAMS is committed to the mission of combatting financial crime through the provision of anti-money laundering/counterterrorism-financing, anti-fraud and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals. It also offers CGSS certification for sanctions professionals, CCAS certification for AFC practitioners in the crypto space, and CAFS certification for anti-fraud professionals. ACAMS' 60+ Chapters globally further amplify the association's mission through training and networking initiatives.

Visit **acams.org** for more information.