Celent.

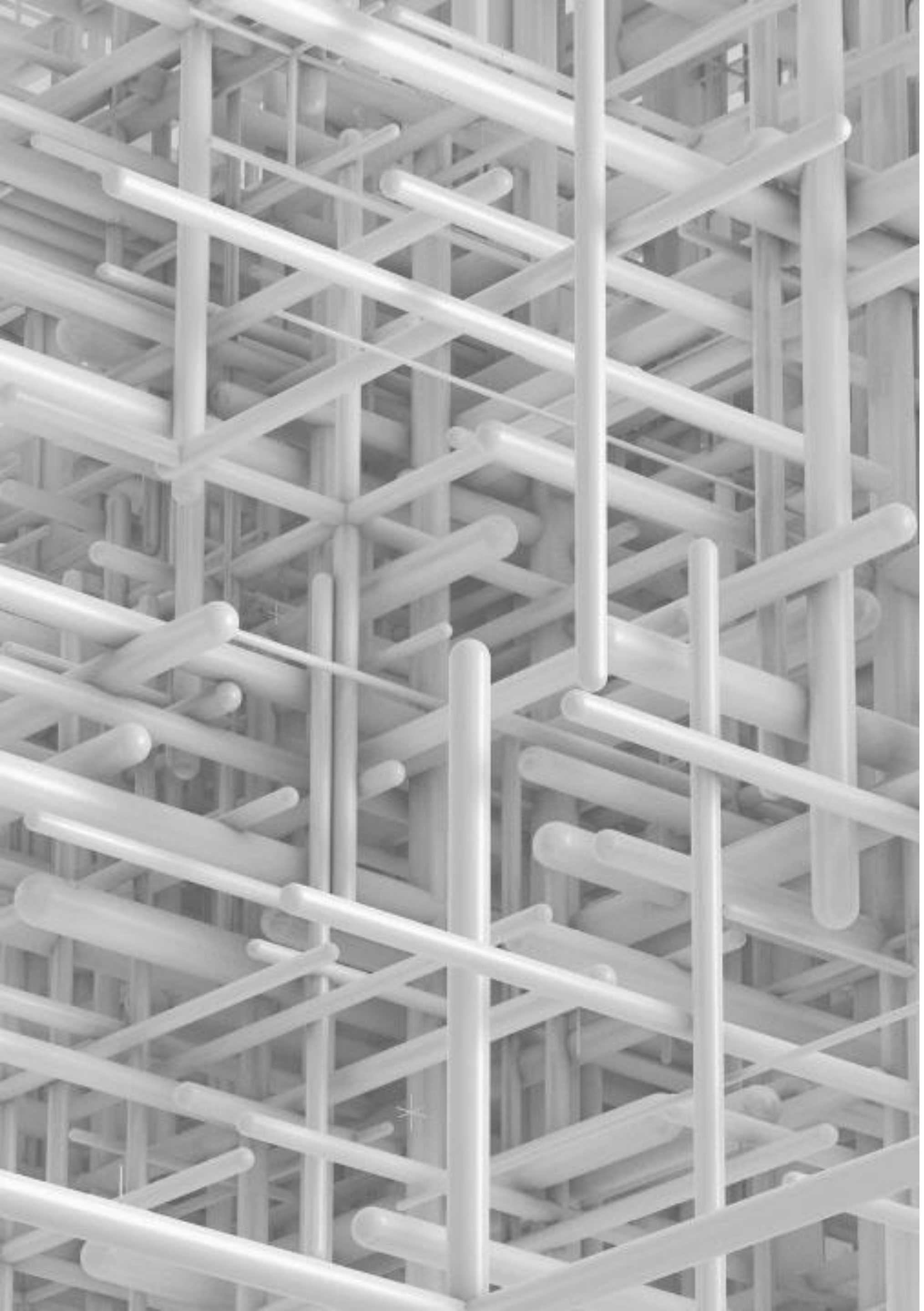
HAWK

TRENDS IN FRAUD & AML CONVERGENCE AT US MID-MARKET BANKS & CREDIT UNIONS

Celent Risk Team

April 2025

A part of GlobalData



CONTENTS

Executive Summary

Banks see the value in fraud and AML convergence, but need help getting there

“We have been actively working to increase the convergence between our fraud and AML operations.”

Vice President, Financial Crime Operations

Anti-fraud (fraud) and anti-money laundering (AML) operations within a bank have distinct business imperatives, processes, procedures and KPIs. At the same time, they are united around a common goal of detecting and preventing financial crime and use similar tools toward this end. And, while increased collaboration and convergence between fraud and AML can deliver efficiencies and lower costs, challenges remain.

Deeply siloed lines of business and complex system architectures have limited the potential for collaboration between fraud and AML at many top tier banks. The situation is very different at mid-market banks. Most banks want, and many to some degree already have, convergence of organizations, processes and systems for fraud and AML.

The way forward can be challenging, due to aging systems, operational and data silos and the initial investment required. As a result, the path to convergence requires vision, steadfastness and the right technology.

Celent surveyed mid-market banks; savings institutions and credit unions; and neobanks in the US to gauge the appetite for fraud and AML convergence and to understand the approaches they take.

This study presents the findings from an online survey of 30 fraud, compliance, operations and IT professionals, as well as insights from in-depth phone interviews with selected survey participants.[1]

Collaboration

80%

Have implemented some degree of collaboration between fraud and AML. 0% say they have no need for convergence

Shared systems

53%

Share part or all of their fraud and AML systems

Artificial Intelligence

100%

Use AI to support a range of fraud and AML use cases

Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30 1. See details on institutions and professionals surveyed in “About the Survey” on page 31.

Fraud and AML convergence rewards a methodical approach

Successful convergence requires coordination of people, processes and technology

Bringing together fraud and AML requires collaboration among teams and linking up data and systems, for example, by:

- Sharing data across fraud and AML to help mitigate risk
- Providing teams with cross-training to facilitate working across functions as needed
- Integrating data to enable fraud and AML teams to access a centralized data repository and analyze it collaboratively
- Maximizing the use of AI and machine learning, ideally on a single platform, to identify suspicious activity

67% agree that the term "FRAML" oversimplifies the complex processes needed to successfully align fraud and AML

Banks see the potential benefits

Banks can reap multiple benefits by coordinating fraud and AML programs. These include:

- Supporting a broader investigation context to provide a more holistic view of customer risk
- Increasing operational efficiencies and lowering costs
- Helping ensure that no financial crime slips through the cracks that exist between fraud and AML operational procedures
- Meeting regulatory expectations for enhanced coordination of fraud and AML efforts

63% say that fraud and AML convergence will increase operational efficiencies

Artificial Intelligence: Fighting fire with fire

Bad actors today are successfully exploiting machine learning and generative AI to commit financial crimes. Banks need to up their AI game in order to effectively respond by:

- Applying machine learning to large data sets to identify suspicious activity and anomalies
- Supporting process automation to reduce the risk of human error and perform repetitive tasks efficiently
- Moving from reactive, after-the-fact detection to proactive, predictive analysis

By leveraging the unified data and greater context that a FRAML approach can provide, AI can more effectively pinpoint risks and reduce false positives.

50% see the use of AI by criminals as one of their top challenges

1

Challenges in Fraud and AML

Why should banks converge AML and fraud?

The promise of FRAML

Regardless of the degree of convergence, fraud and AML rely on similar tools, data and processes to identify and mitigate financial crime risks.

Fraud departments focus on preventing theft, check and payment fraud and transaction fraud. AML operations are responsible for identifying attempts to introduce money obtained through illegal activities like corruption, drug trafficking and terrorist financing activities into the financial system. Both processes detect unwanted financial transactions that present risks to the banking system.

Banks, particularly mid-market banks, are increasingly looking to increase collaboration and convergence between fraud and AML in order to improve efficiency, support better outcomes and contain costs.

Convergence is not always linear, and 67% of banks surveyed think that the term "FRAML" oversimplifies the processes needed to successfully align fraud and AML.

Challenges of FRAML

While many banks seek to increase collaboration of fraud and AML operations and technology, there are a number of challenges.

Regulatory and compliance requirements. Fraud and AML have separate compliance protocols to follow, which can result in teams still working in silos rather than on a collaborative basis.

Aging technology. It can be difficult to integrate inflexible legacy systems, which complicate the integration of fraud and AML functions at the system level. Inflexible systems also make it difficult to add new technologies such as machine learning, biometrics and support for digital financial services channels.

Cost of transformation. While new technology can help, for mid-market banks the cost of technology transformation can be a hurdle.

> “
>
> I believe integrating our fraud and AML teams will be a total game changer for us. It will help us detect risks at an earlier stage so that we can take preventive measures and reduce financial crime effectively. It will even improve the overall regulatory compliance structure of the bank.
>
> Director of Fraud Monitoring and Analytics

Benefits of fraud and AML convergence

Celent’s research detected a trend at mid-market banks toward integrating their fraud and AML operations. Fraud and AML are linked at many banks from the organizational, process and systems points of view, and banks want to do more.

Running fraud and AML on a unified platform is common at small banks. At large banks, the size and complexity of their operations make convergence difficult. Mid-market banks have the most to gain from fraud and AML integration.

Increased collaboration and convergence between fraud and AML can benefit banks’ anti-financial crime efforts in multiple ways.

- Increased alignment of fraud and AML processes can enable faster risk identification, investigation and reporting
- Collaboration and information sharing can reduce duplication of effort, which can help contain human resources cost
- Integration of systems can support data sharing and analysis and potentially reduce maintenance costs
- Moving onto a unified fraud/AML platform provides an opportunity to choose modern technology that supports machine learning and process automation, increasing detection capability and operational efficiency

Top drivers of change in fraud and AML programs

Banks need to address a changing financial crime landscape while at the same time controlling costs

Financial institutions implement change in their fraud and AML programs for a variety of reasons, and there are often multiple factors driving change.

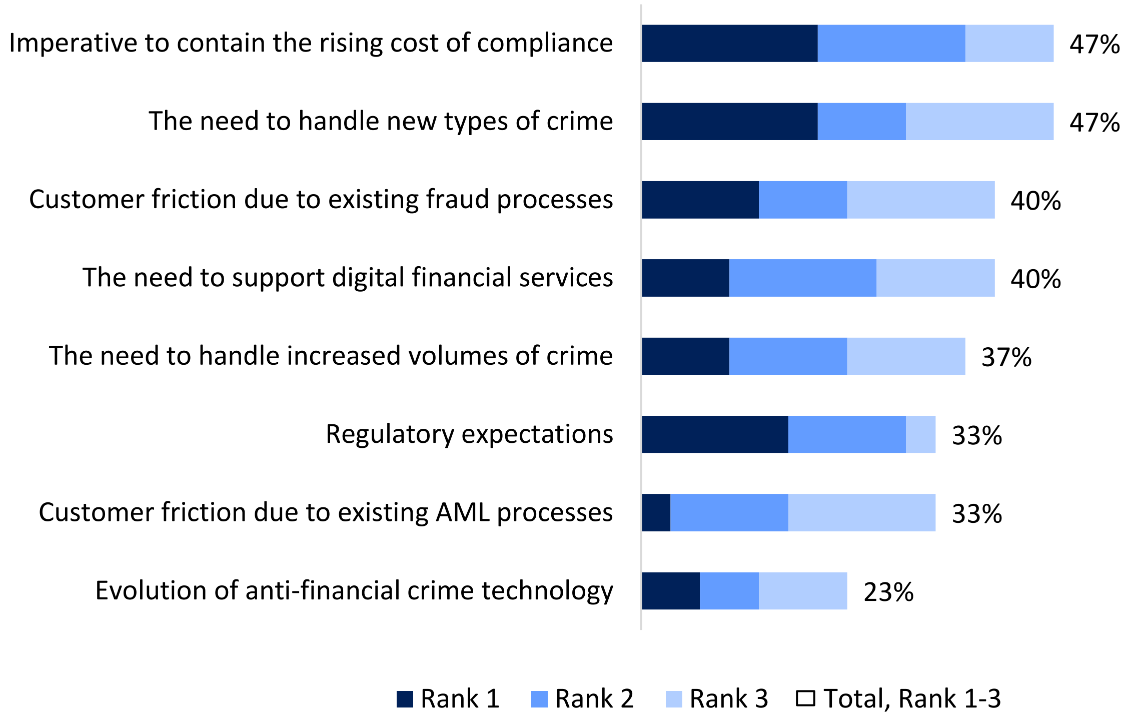
Banks face a rapidly changing financial crime landscape, with new fraud vectors and money laundering techniques emerging continuously. At the same time, the cost of combatting financial crime has skyrocketed, primarily due to process inefficiencies—read “high false positives rates”—arising from the limitations of legacy anti-fraud and AML technology.

Banks see these two challenges—the imperative to contain compliance costs and the need to handle new types of crime—as equally important. Both of these were cited as drivers for change by 47% of banks.

Banks also point to the need to control customer friction around, especially, fraud processes (apart from KYC requirements, AML processes are less likely to touch the customer directly), as well as the need to support digital services from the financial crime perspective. Both of these areas were noted as drivers for change by 40% of banks. Maintaining effective fraud controls while minimizing negative impacts on the customer experience is a concern of banks as consumers in the digital age have come to expect high levels of service.

Regulatory issues and AFC technology evolution were singled out as drivers of change by a smaller proportion of banks. Looked at another way, however, this may suggest that 33% of banks are facing regulatory scrutiny around their fincrime operations and 23% see the need to upgrade their fraud and/or AML technology in order to meet operational needs and regulatory requirements.

Top drivers of change in fraud and AML programs



Question: *Please rank the main drivers of change for your fraud and AML program?* Total of Rank 1, 2 and 3
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

Top challenges in anti-fraud programs

Staffing is a high priority issue for virtually all banks

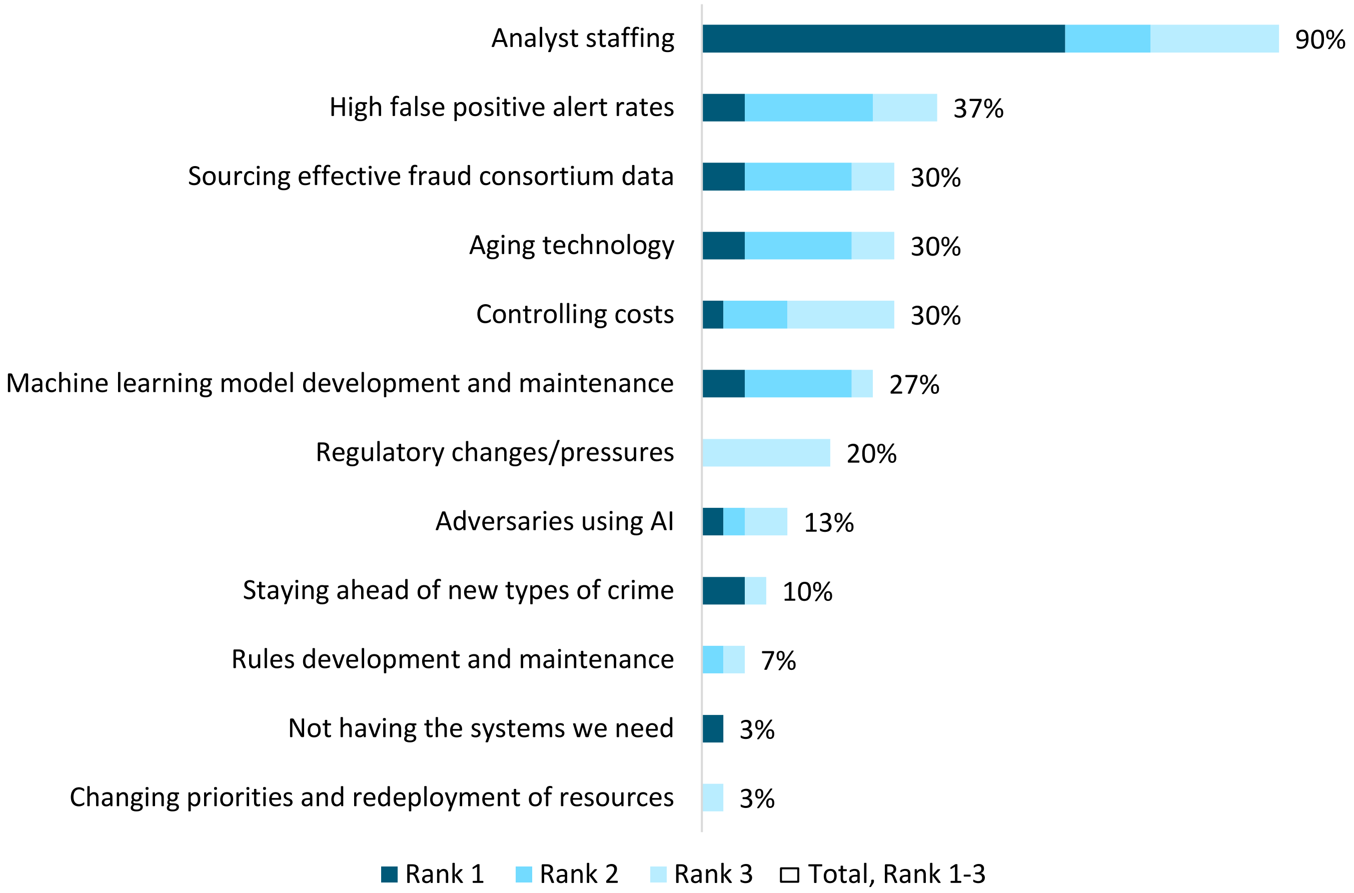
Banks face a broad range of challenges in their anti-financial crime programs. Looking first at their fraud programs, almost all banks point to the difficulty in maintaining adequate levels of well-trained analysts. Fully 57% of banks cite analyst staffing as the biggest challenge in their fraud programs and 90% cite it as a top 3 challenge.

False positives are as serious a problem for fraud operations as for AML and are cited as a top 3 challenge by 37% of banks. As fraud attacks grow in number, banks are increasingly challenged to maintain analyst levels sufficient to support anti-fraud operations.

These challenges are interrelated. Aging technology and the related issue of controlling costs are both cited as top 3 challenges by 30% of banks. In turn, legacy systems are a major cause of—and spiraling costs are in large part a consequence of—high false positive rates in fraud.

Consortium data and machine learning-based predictive analytics are important tools in the fight against fraud and are cited by 30% and 27% of banks respectively as a top 3 challenge. This suggests that many mid-market banks in the US need help in accessing high-quality data as well as sourcing effective models to support their anti-fraud operations.

Top fraud program challenges



Question: *Which issues or challenges are you facing in your anti-fraud program?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

Top challenges in AML programs

Analyst staffing, false positives, sourcing sanctions/KYC data and model maintenance are the top challenges

Turning now to their AML programs, analyst staffing is again the leading challenge. Forty-seven percent of banks cite analyst staffing as the highest priority challenge in their AML programs and 77% cite it as one of their top 3 challenges.

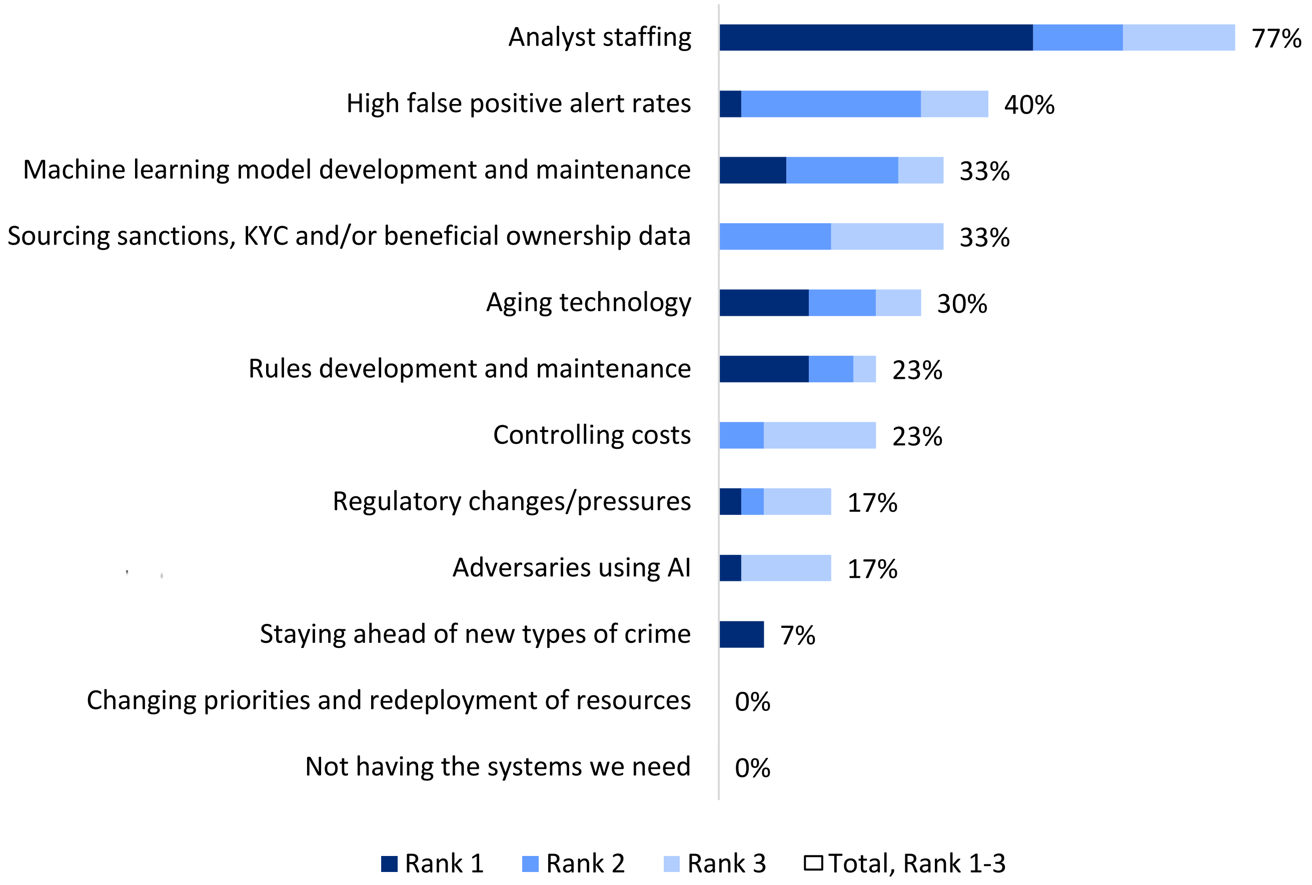
False positives, the second most-cited challenge, is closely related to staffing issues. The high rate of false positives generated by AML systems translates into more alerts for compliance analysts to investigate, which can lead to a need for more analysts to cope with the workload as well as analyst burnout.

In turn, legacy technology is a leading contributor to the false positives problem. Thirty percent of banks cite aging technology as one of their top 3 challenges.

Evolution in AML technology is helping and many banks are deploying AI to increase the accuracy of AML alerts and reduce false positives. Model development and maintenance has therefore become an issue for many mid-market banks, with 33% of banks citing this as a challenge.

Regulators place a high priority on banks adequately screening for customer risk and weaknesses in this area have been the target of numerous actions and fines. Reflecting this, 33% of banks point to sourcing KYC, KYB and sanctions data as a top 3 challenge.

Top AML program challenges



Question: *Which issues or challenges are you facing in your AML program?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

2

Trends in Fraud and AML Convergence

Collaborating across fraud and AML

Many mid-market banks share resources across anti-financial crime functions

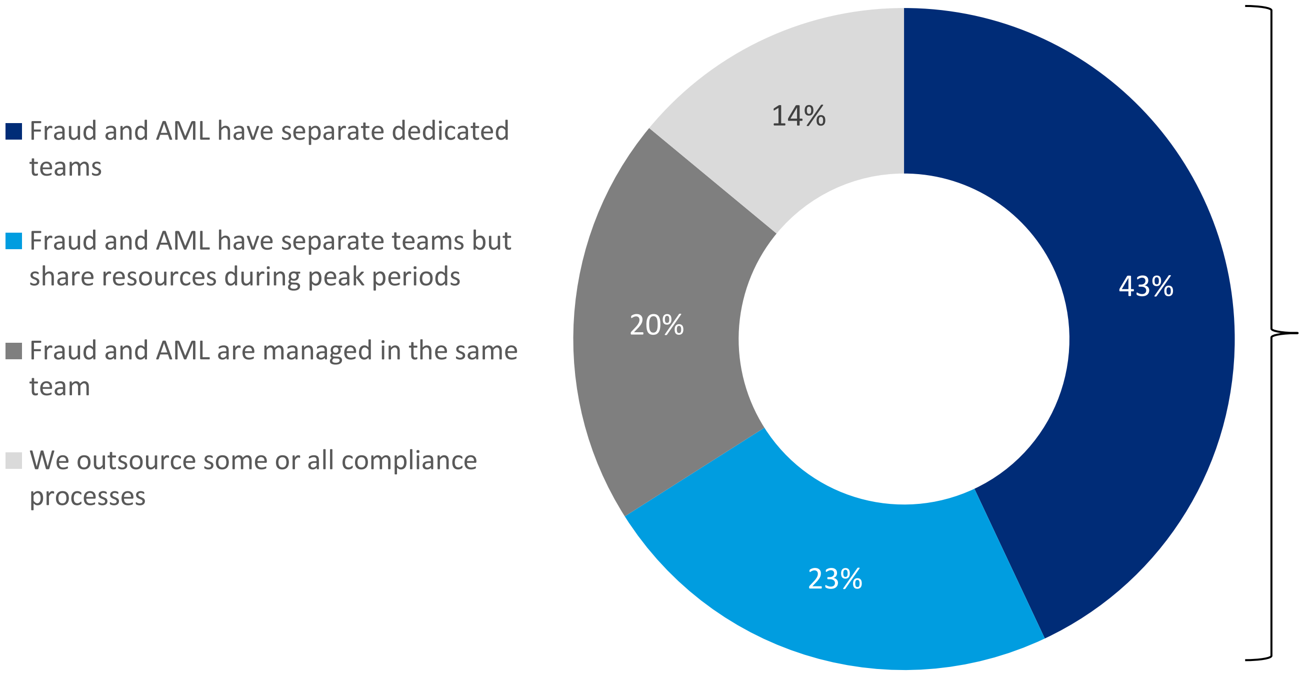
43% of banks share resources across fraud and AML teams

The majority of banks are facing staffing issues across their AML and—to an even greater extent—their anti-fraud operations. Factors contributing to these shortages include a general lack in the marketplace of well-trained AML and fraud analysts, limitations in fraud and AML systems that lead to high false positive rates, and rising levels of financial crime on the both AML and especially the fraud side.

Only 20% of mid-market banks in the US maintain a shared team to support both fraud and AML operations. A majority of banks—66%—have separate teams for fraud and AML. To address the staffing challenges that, as we have seen, affect both the fraud and AML functions, many banks—43% of the total—share resources across these teams as needed.

Another response to the staffing requirements of fraud and AML programs is to outsource these processes. Business process outsourcing of anti-financial crime functions has been a slowly building trend, and 14% of mid-market banks say they currently outsource some or all of their compliance processes.

How does your organization manage resource allocation for your risk and compliance verticals?



66% have separate fraud and AML teams

Question: *How does your organization manage resource allocation for your risk and compliance verticals?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

Pros and Cons of fraud and AML collaboration

Banks see increased efficiencies and reduced TCO as potential wins from increased collaboration

Pros

When considering a more collaborative approach to fraud and AML operations and technology, banks cite the potential for increased operational efficiency and a lower cost of ownership as the biggest win, cited by 63% and 53% of banks respectively.

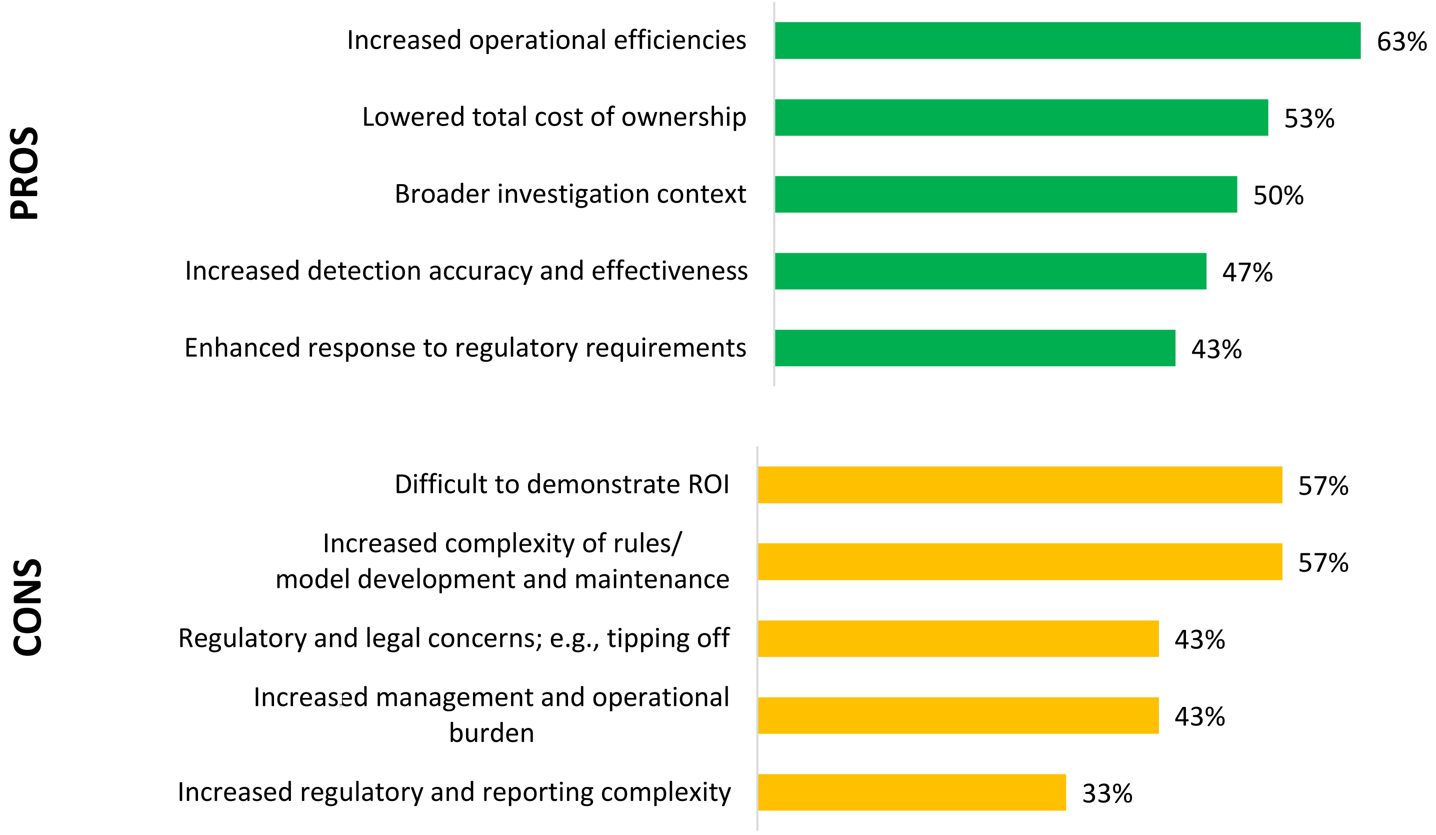
Gaining a holistic view of activity—a 360-degree view across both fraud and AML—to provide a broader context for investigation is seen as a benefit of fraud and AML collaboration by 50% of banks. Many banks also see fraud-AML collaboration as contributing to better detection itself (47%) and as a means to better meet regulators' expectations.

Cons

If banks clearly see the benefits of collaboration, they are also cognizant of the challenges in implementing a combined approach to fraud and AML. A major challenge is demonstrating return on investment to support the business case for change (57%). Banks are also wary of the added complexity of developing the rules and models needed to effectively support both fraud and AML (also 57%).

Interestingly, tipping off risk—e.g., that customer outreach around fraud could let an entity know they are under suspicion for money laundering—is also seen as a risk by many banks.

Pros and Cons of a collaborative approach to fraud and AML



Question: *When you look at a collaborative approach to fraud and AML, what do you see as the pros and cons?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

Appetite for fraud and AML technology collaboration is strong

None of the banks surveyed said they have no need for technology convergence

From a technology perspective, a majority of banks (60%) have combined some or all of their anti-fraud and AML technology.

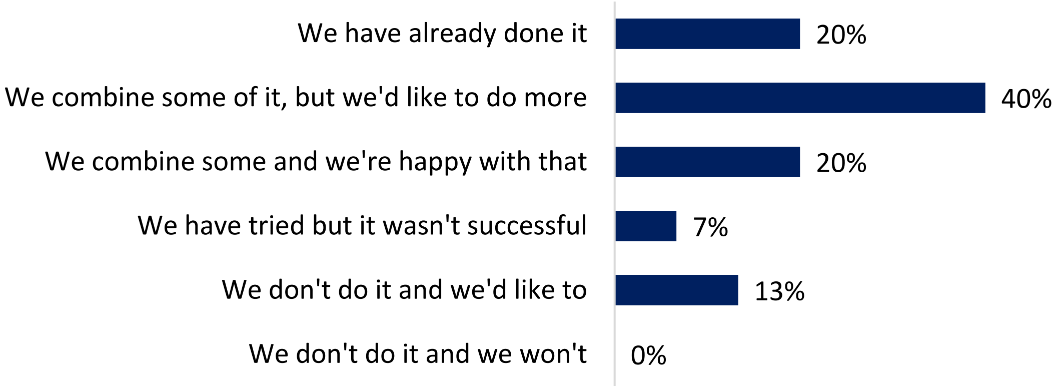
Moreover, a majority of banks (53%) that have partially consolidated their fraud and AML technology—or have not yet started on the journey—would like to do more.

Significantly, no banks assert they have no need for convergence.

Banks that have started on the journey report a number of benefits from a more collaborative approach to fraud and AML.

According to one bank,“one of the biggest advantages of this collaboration is our ability to detect suspicious activities much faster. Fraud cases often provide early warning signs of potential money laundering, while AML investigations sometimes uncover fraud schemes that wouldn’t have been obvious to the fraud team alone. By collaborating, we can connect the dots and identify the origin of the threat.”

Appetite for a more collaborative approach to fraud and AML technology



> At the end of the day, our bank can also benefit from the convergence of fraud and AML, resulting in a better customer experience. For example, a single risk-based approach may improve decision-making and reduce unnecessary friction.
>
> Senior Fraud Risk Manager

Question: *Which statement best describes your appetite for a more collaborative approach to fraud and AML technology?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

Potential and realized cost savings from Fraud and AML collaboration

Banks that have not fully merged their fraud and AML operations still expect they would reap hard dollar benefits

A hard dollar measure of the potential benefits of merging fraud and AML operations and technology is the cost savings that banks expect that they would save.

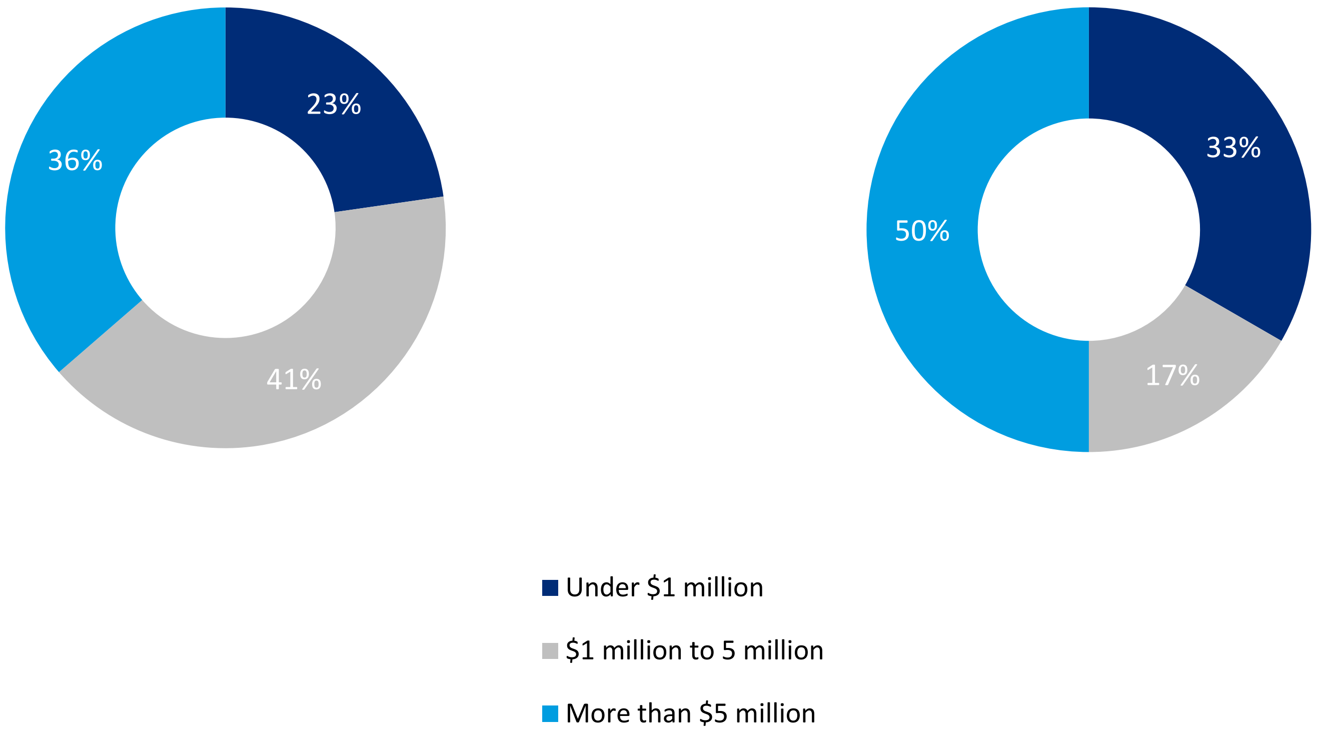
Most banks that have only partially consolidated their fraud and AML program or that have not yet started the journey—41%—estimate they could save between $1 and $5 million over five years if they were to merge their programs. Another 36% expect they would save more than $5 million over five years.

These are high expectations for a mid-sized bank. Even so, the smaller proportion of banks that have successfully merged their fraud and AML programs report even greater benefits, with 50% saying they have saved more than $5 million each year by consolidating.

Here is one bank's experience: "*We have saved a significant amount of money through the integration of our fraud and AML operations, generally by making our core operations more effective and efficient. By the convergence of fraud and AML, both teams share customer data and use similar technological tools to run independent analyses. This is more cost-effective than running different operations within individual fraud and AML teams.*"

How much money could you save over 5 years?
(asked of banks that have started consolidating fraud and AML systems or would like to)

How much money have you saved annually?
(asked of banks that have already consolidated fraud and AML systems)



Questions: *In your best estimate, how much money could you save over 5 years by merging fraud and AML together?* N = 22
In your best estimate, how much money have you saved annually by merging fraud and AML together? N = 6
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025

Cautionary tales: Why some initiatives don't succeed

Failure to stay on time and on budget and higher-than-expected run time costs have sunk some FRAML projects

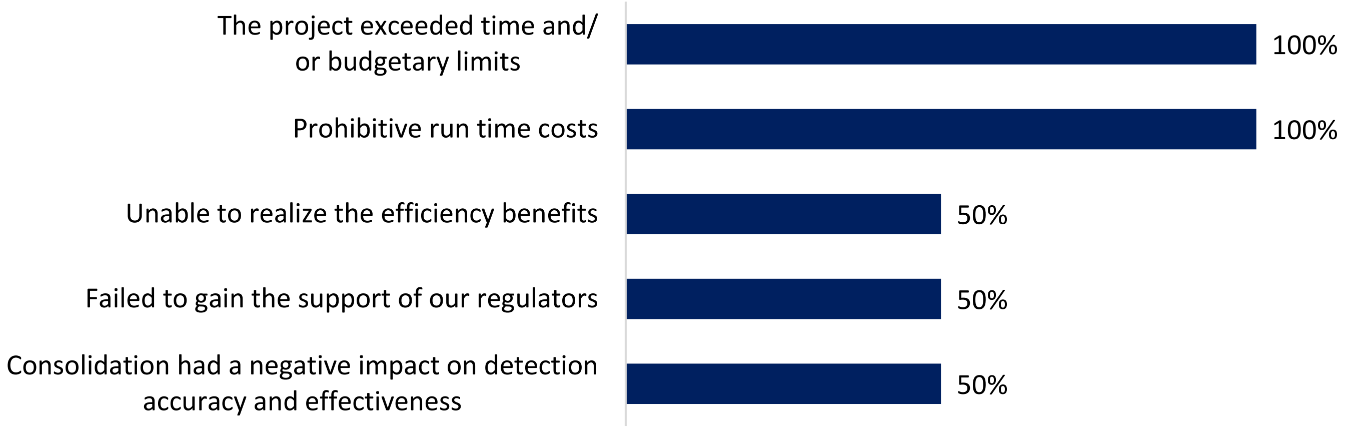
Only a few banks—7%—have tried to combine their anti-fraud and AML technology and not succeeded.

Commonly experienced reasons for this include failing to bring the project in on time and/or on budget, as well as prohibitive run time costs. Part of this challenge lies in the higher cost of modern, more capable technology as compared to legacy systems, as well as the data management costs involved in supporting advanced analytics.

Some banks report they were unable to achieve expected efficiencies or that consolidation had a negative effect on accuracy and effectiveness. One challenge here is the gap between the batch-oriented processes of AML and the real-time operations of fraud. Trends toward real-time AML and customer-centric investigations are already beginning to break down this barrier and will continue to do so over the mid- to long-term.

Speaking more broadly, fraud and AML have developed distinct skill sets and tools which need to be reconciled in order to support successful integration of the two disciplines. Legacy organizational structures mean that merging fraud and AML teams requires a cultural shift, new networks, and new technology integration, all of which require careful planning and proven partners.

Reasons why fraud and AML consolidation efforts were unsuccessful



> "Fraud and AML teams use different technologies; fraud teams use real-time AI models, while anti-money laundering team uses rule-based transaction monitoring. So, full convergence requires significant investment in unified platforms, which many banks are hesitant to implement immediately.
>
> Senior Fraud Risk Manager

Question: *Why was your initiative to consolidate fraud and AML technology not successful?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 2

Perceived barriers to consolidating fraud and AML systems

Banks see establishing a solid business case for change and system/process incompatibility as the biggest challenges

Most mid-market banks in the US see the benefits of taking a more collaborative approach to fraud and AML and are keen to move more in this direction.

At the same time, as with any change management program, merging fraud and AML is not always a slam dunk.

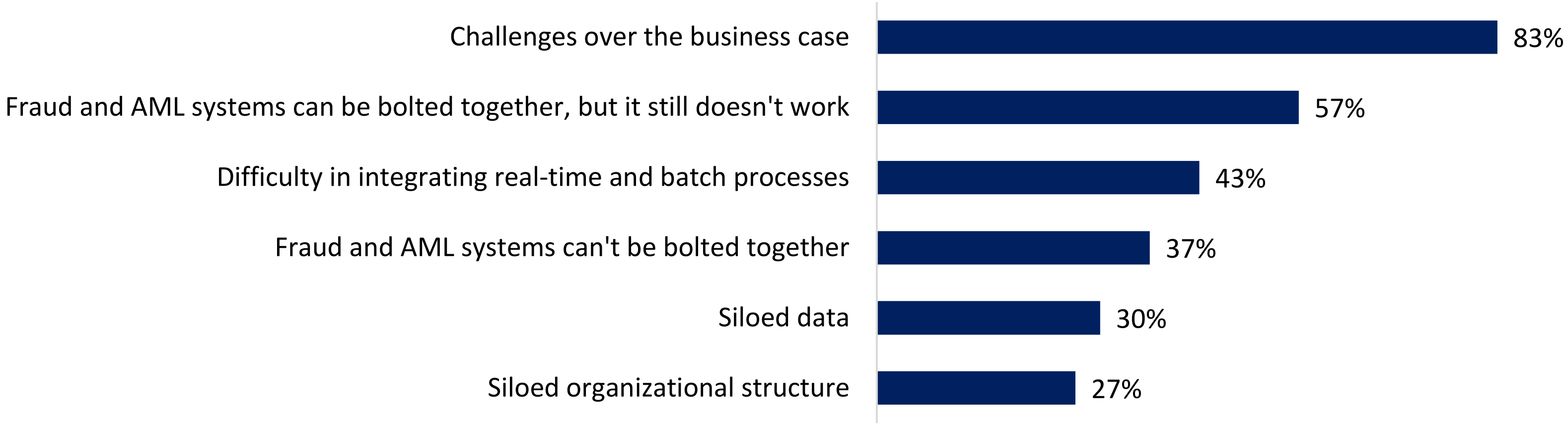
One of the most promising areas for realizing lower TCO is rationalizing fraud and AML technology systems. Yet banks are aware of potential roadblocks to consolidating systems.

Most banks (83%) see challenges in proposing a solid business case as a hurdle to be overcome. Yet, as we have seen, banks that have merged systems report significant cost savings.

Many banks (57%) are skeptical that merging fraud and AML systems can work. A related concern is the perceived difficulty of integrating the real-time processes of fraud with batch-oriented AML.

Choosing a technology partner that offers a strong value proposition around fraud and AML collaboration can put banks on a strong footing to overcome these obstacles.

Barriers to a more collaborative approach to fraud and AML technology



> “ The biggest hurdle was technology, or more specifically, data orchestration. Our fraud team is focused on real-time transaction monitoring, while AML is more retrospective in nature. Merging these approaches into a single system that meets both needs has taken time and a significant investment.
>
> Director of Fraud Operations

Question: *What are the main barriers to a more collaborative approach to fraud and AML technology??* Total of Rank 1, 2 and 3
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

3

Elements of FRAML: People, Processes and Technology

Collaboration relies on the alignment of three key areas: people, processes and technology

People

- While 27% of mid-market banks surveyed have completely separate fraud and AML organizations, 23% of banks have fraud and AML under one department or have merged parts of their organizations
- For banks that have merged parts of their organizations, the main areas of collaboration are KYC, transaction monitoring and EDD
- Regardless of how they are organized, many banks see the value in collaboration between their anti-fraud and AML teams
  - 50% share information between their fraud and AML organizations
- Collaboration and information sharing is often on an as-needed basis, limited to high risk or exceptional cases
  - This is a starting point for banks to think about further convergence of processes on a BAU basis

Processes

- 60% of mid-market banks have merged their fraud and AML processes to some degree
  - 47% have merged parts of their fraud and AML processes and 13% have merged all or most processes
- Convergence is most common for the cluster of processes around KYC and the related domains of CDD, sanctions screening and EDD—essential processes for assessing customer risk
  - Many banks also collaborate around alert investigation processes
- Collaboration helps identify complex schemes that might go unnoticed when fraud and AML operations are treated in isolation

Technology

- The sharing of systems across fraud and AML mirrors process collaboration, with almost as many banks (56%) sharing at least some systems as have merged processes
- Still, the 43% of banks that are currently running separate systems for AML and fraud are potentially missing out on the benefits of sharing data and tooling
- The most common areas of system consolidation are KYC (65%) and EDD (53%), followed by case management (47%) and transaction monitoring (41%)
  - Sharing systems in these areas supports holistic analysis of customer risk and efficient tracking and escalation of suspicious activity

Approaches to fraud and AML collaboration: People

The most common form of organizational collaboration is information sharing between fraud and AML teams

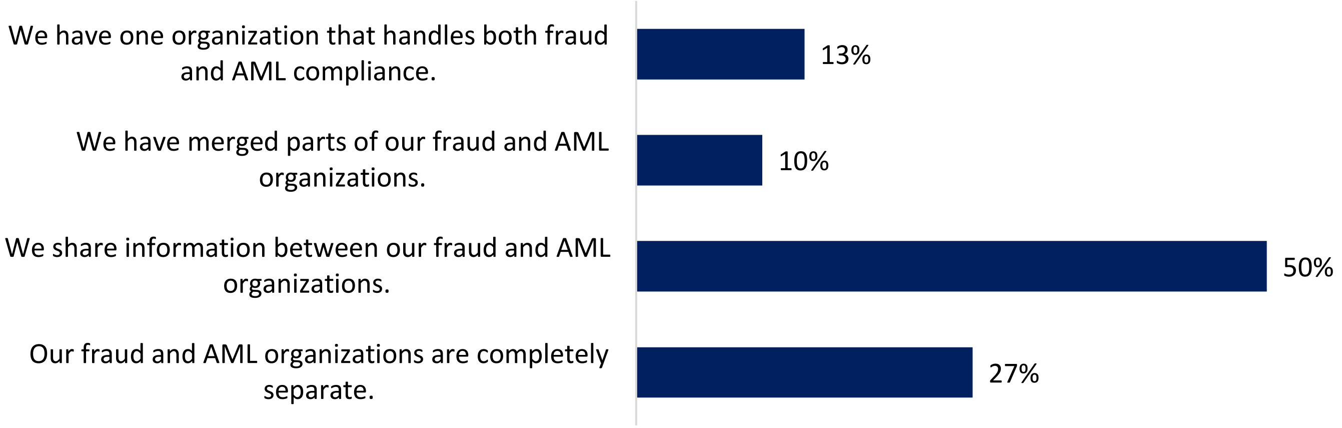
Most banks see the value in collaboration between their anti-fraud and AML programs. Many have implemented collaborative approaches and a significant proportion of banks say they have a fully realized approach to FRAML where fraud and AML sit within one organization.

This section takes a closer look at the nuts and bolts of how mid-market banks have moved forward with their fraud and AML programs.

Both fraud and AML require specialized expertise. Fraud teams focus on real-time fraud attacks, such as account takeovers, authorized push payment fraud and synthetic identity fraud; AML teams specialize in identifying financial crime networks, often working with law enforcement and regulatory bodies. The need to ensure they maintain these specialized capabilities is a primary reason most banks keep their fraud and AML organizations separate. Only 23% of banks have partially or entirely merged their fraud and AML organizations.

Accordingly, the most common form of collaboration is sharing of information between the two organizations (50%).

Fraud and AML organization



> “Our fraud prevention and anti-money laundering teams work closely together because, in many ways, we’re fighting the same battle but just from different sides.
>
> Director of Fraud Operations

Question: *Which of the following statements best describes fraud and AML organization at your bank?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

Information sharing between fraud and AML organizations

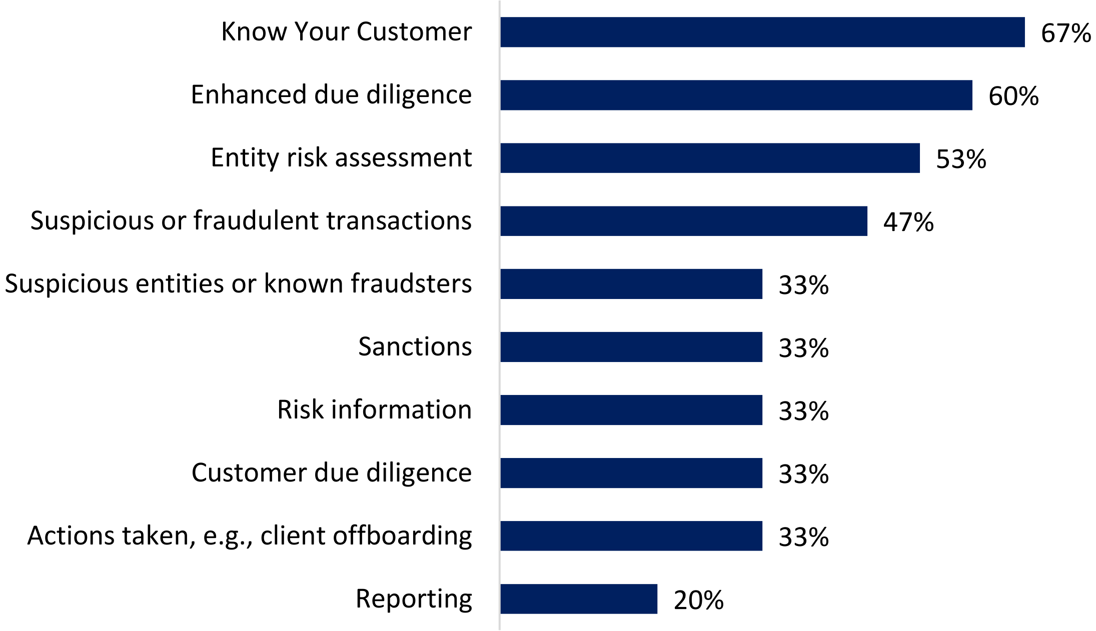
KYC, EDD and entity risk information are the most common touchpoints between teams

For the 50% of mid-market banks that share information between their fraud and AML organizations, most (47%) are sharing AML information with their fraud team, while 33% of banks use fraud information to inform their AML operations. At 20% of banks, information is shared bilaterally between both teams.

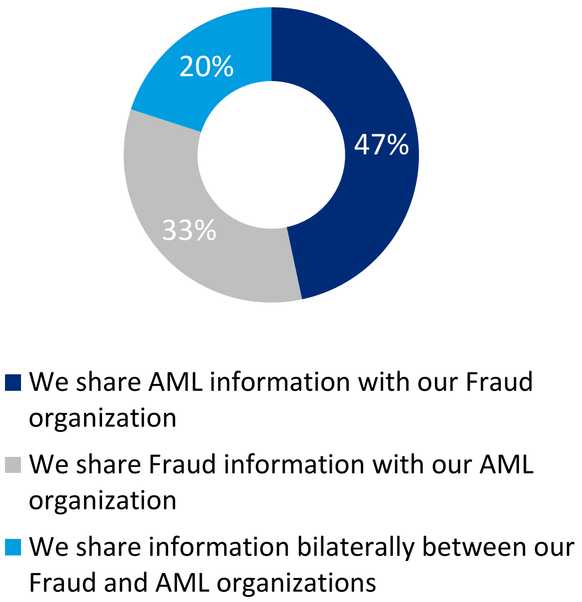
At many banks, KYC screening has become an integral step in the fraud value chain, in addition to AML, and the most commonly shared information is around know your customer (67%). KYC is followed by the related areas of enhanced due diligence (60%) and entity risk assessment (53%).

Many banks (47%) also share notes around suspicious activity. According to one bank, a key driver for information sharing is supporting the ability to recognize the overlap in emerging financial crime typologies, mainly those that involve digital channels and cryptocurrency.

Information shared across fraud and AML organizations



Direction of information flow



Questions: *In which areas do you share information between your fraud and AML organizations?*
In which direction do you share information between your fraud and AML organizations?
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 15

Focus areas for merged fraud and AML organizations

The three pillars of KYC, transaction monitoring and enhanced due diligence are common areas for shared teams

For banks that have merged some but not all of their fraud and AML organizations, the main areas of collaboration are know your customer screening followed by transaction monitoring. Enhanced due diligence, closely aligned with KYC, is also a common area for merged organizations.

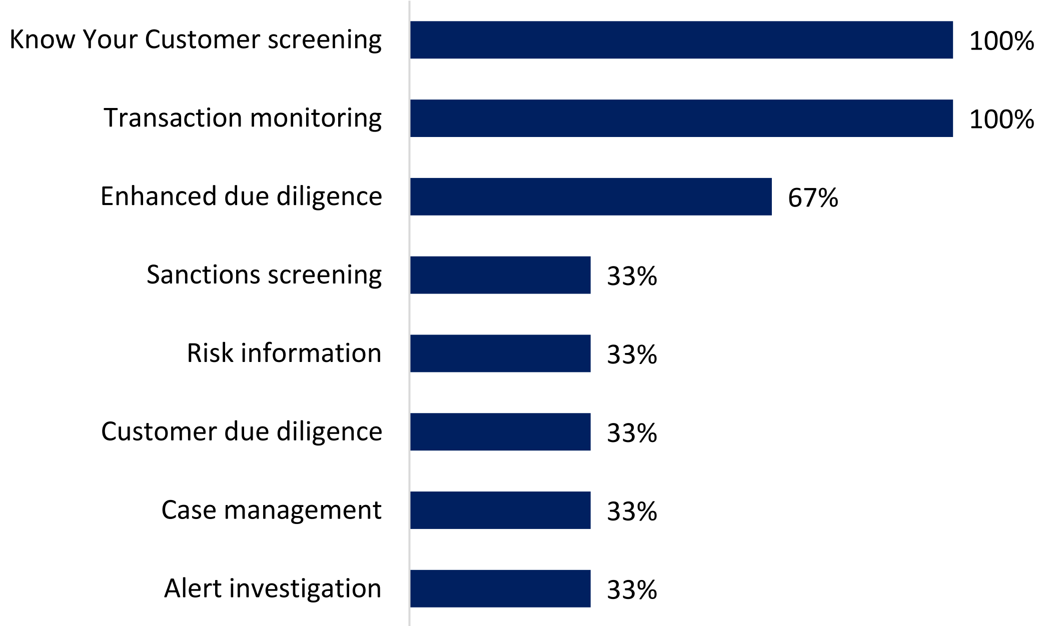
These three areas constitute a core workflow in both fraud and AML:

- KYC for assessing entity risk, particularly at customer onboarding,
- Transaction monitoring to keep an eye on suspicious activity and
- Enhanced due diligence to support investigation into suspicious actors.

By grouping these pillars of anti-financial crime operations, banks can efficiently and effectively support KYC risk assessment and gain insights into risks and suspicious signals emerging from both sides, AML and fraud.

According to one bank, “We try to get a 360 view of customer behavior, so our fraud and AML teams have to interact. But it's not like we are interacting all the time with every client; it's on an as-needed basis.”

Collaboration across fraud and AML organizations



> Complete integration of Fraud and AML would not only strengthen our defense against financial crime but also align with regulatory expectations for enhanced compliance and risk management practices.
>
> Deputy Financial Crimes Officer

Question: *Which parts of your fraud and AML organizations are merged?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 3

Approaches to fraud and AML collaboration: Processes

Sixty percent of banks have at least partially merged fraud and AML processes, especially for KYC and related processes

Collaboration between fraud and AML processes at banks looks very different than their organizational set-ups. 40% of banks separate their fraud and AML processes, although, as we have seen, many of these banks will share information across their fraud and AML teams.

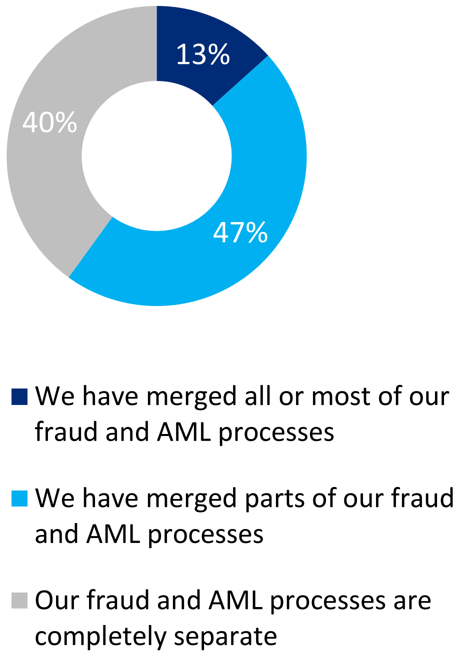
At the same time, the majority of banks (60%) have merged processes. A significant 47% of banks have merged parts of their fraud and AML processes and an additional 13% have merged all or most.

Reflecting the emphasis on information sharing around know your customer, KYC is the most common area of collaboration (56%). The closely related areas of CDD and sanctions screening (44% each) and EDD (39%) are also frequent areas of collaboration.

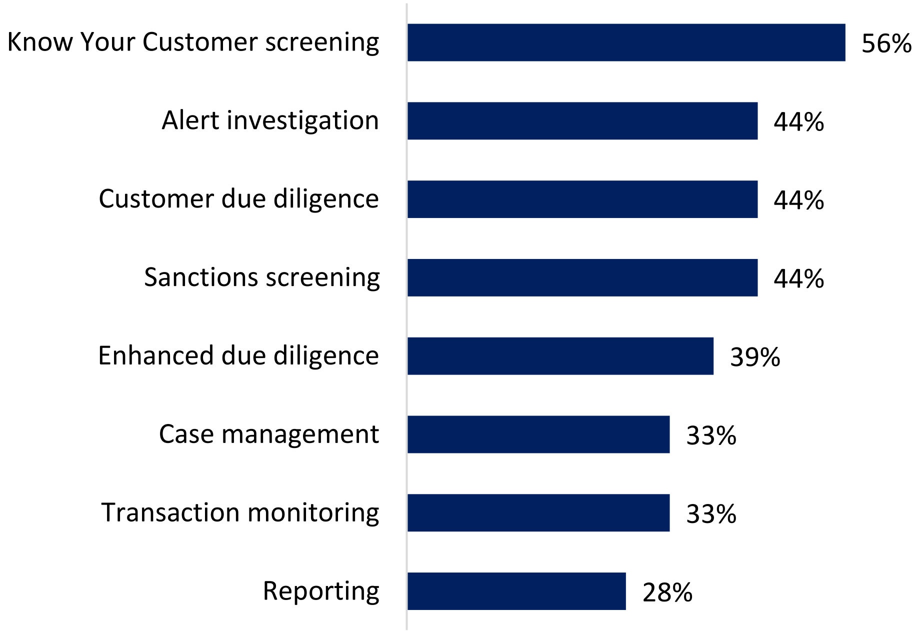
Many banks also collaborate around alert investigation processes (44%). Banks point to the enhanced ability to capture risks when investigating from both sides of the AFC equation.

Challenges to be overcome include the difficulty in training teams to understand both fraud detection and AML compliance methodologies.

Fraud and AML process collaboration



Shared fraud and AML processes



Questions: *Which of the following statements best describes fraud and AML processes at your bank?* N = 30
Which parts of your fraud and AML processes are merged? N = 18
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025.

Approaches to fraud and AML collaboration: Technology

Fifty-six percent of banks share at least some fraud and AML systems, especially systems for KYC, EDD and case management

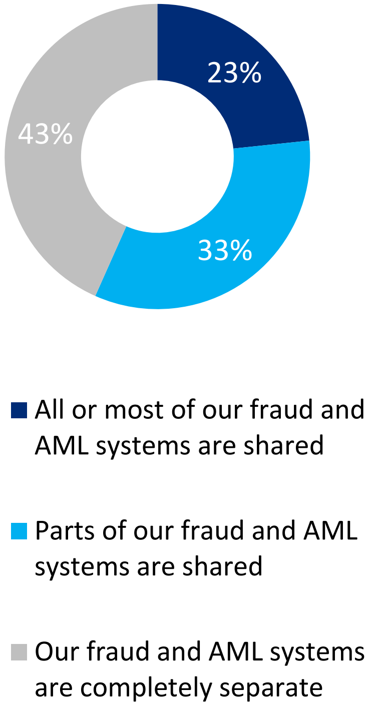
IT systems are the engine that drives anti-financial crime programs at banks and technology evolution is making advanced tools such as artificial intelligence (AI) more available to smaller banks.

The sharing of systems across fraud and AML mirrors process collaboration, with almost as many banks (56%) sharing at least some systems as have merged processes (60%, see previous slide). However, this means that 43% of banks that are currently running separate systems for AML and fraud are potentially missing out on the benefits of sharing data and tooling.

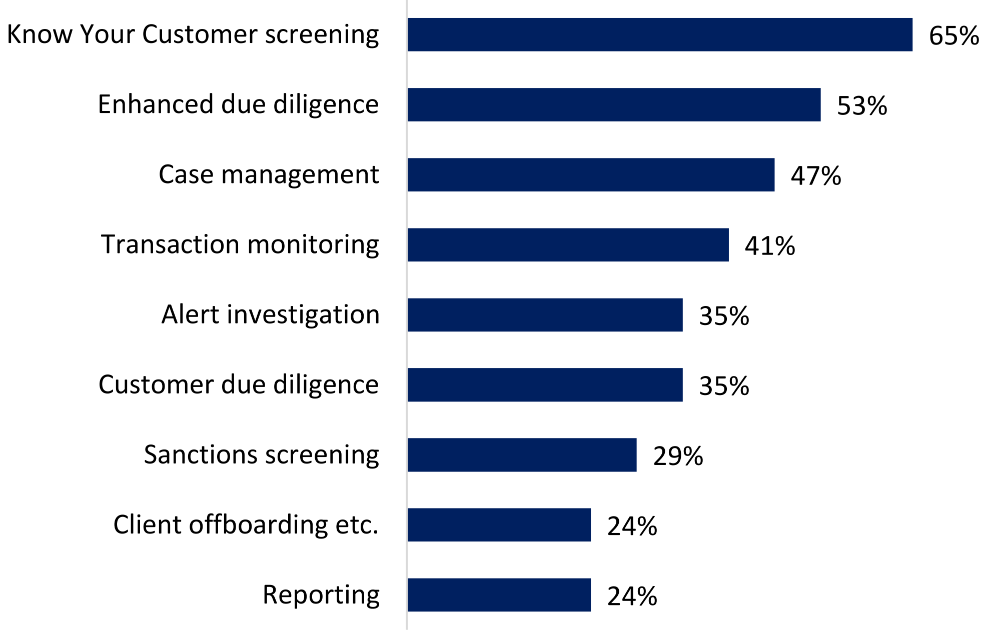
More banks share all or most of their fraud and AML systems (23%) than collaborate across all or most processes. This reflects the availability of technology systems that support both fraud and AML as well as the feasibility of a consolidated architecture to support both these pillars of AFC.

The most common areas of system consolidation are KYC and EDD, followed by case management and transaction monitoring. As several banks told us, sharing these systems would support holistic analysis of customer risk, transaction history and customer behavior, allowing teams to more effectively and efficiently track, escalate and ultimately report suspicious activity to regulators.

Shared fraud and AML systems



Shared fraud and AML system areas



Question: *Which of the following statements best describes the AML and fraud technology systems at your bank?* N = 30
In which areas do you share your fraud and AML systems? N = 17
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025.

4

Leveraging AI for Fraud and AML

Leveraging AI for fraud and AML use cases

False positives reduction and preparing data for consumption by fraud and AML systems are the leading use cases today

Anti-financial crime technology has evolved considerably over the past five years. In particular, AI is coming of age and delivering benefits to banks in the form of enhanced insights, improved accuracy and greater efficiency. Our interviews showed that mid-market banks looking to consolidate fraud and AML systems see this as an opportunity to upgrade to an AI-enabled platform that can deliver better results for both fraud and AML.

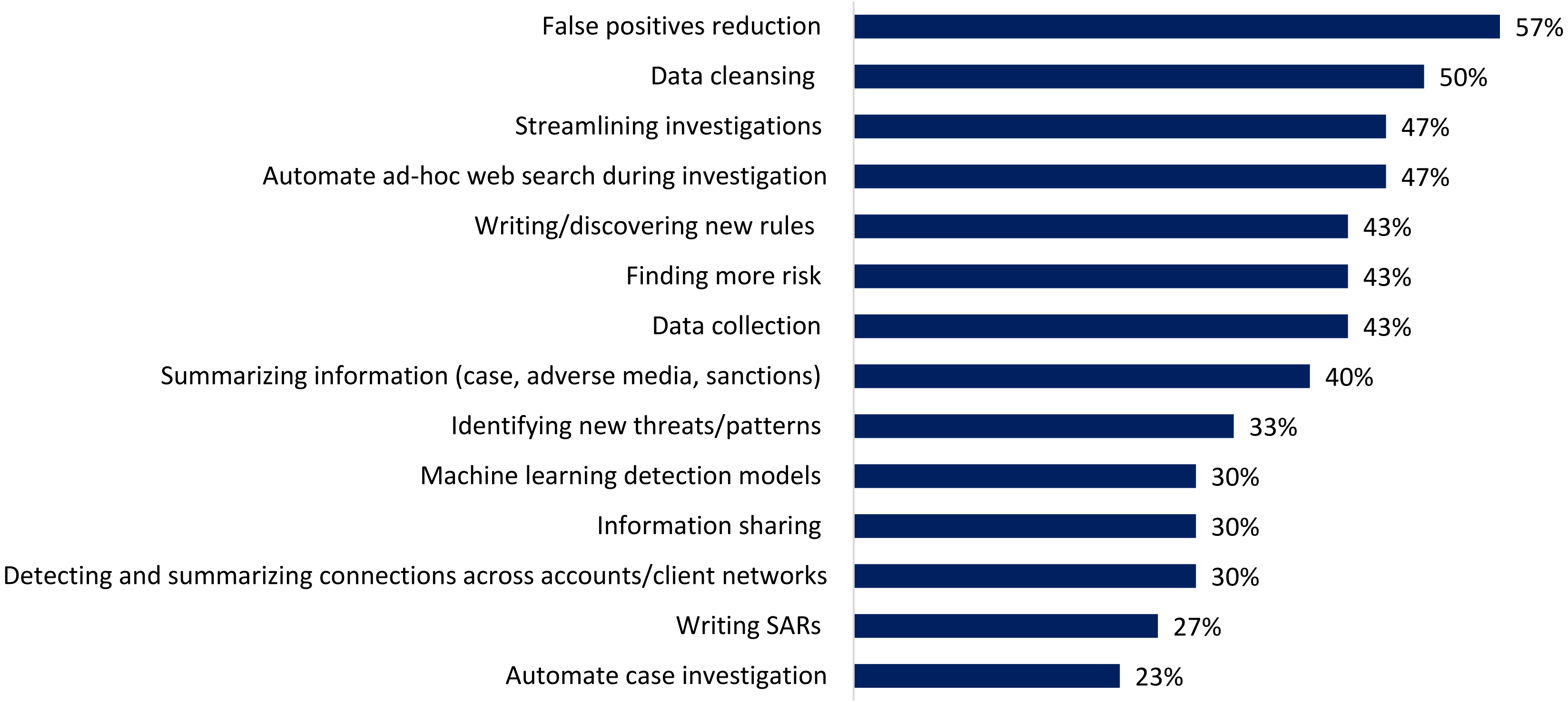
Many mid-size banks, with the help of their technology partners, are capturing the benefits of AI across a range of tasks and functions today.

Using AI to increase efficiency is key. Banks are using AI for false positive reduction (57%), streamlining investigations (47%) and writing SARs (27%). Banks are also using AI to increase effectiveness, with finding more risk at 43%, identifying new threats at 33% and detecting connections across networks at 30%.

Data cleansing, used to optimize consumption and analysis by fraud and AML applications, is the second most cited application of AI in anti-financial crime.

Many institutions are also leaning on AI to support the investigation value chain, including for finding more risk, web searches, data collection and summarizing alert and case information.

Current use of AI in fraud and AML



Question: *Which use cases do you use AI for today?*
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

Future impact on fraud and AML: Machine learning and generative AI

Mid-market banks clearly see more value coming from AI in the next 12 to 18 months, both from machine learning and generative AI.

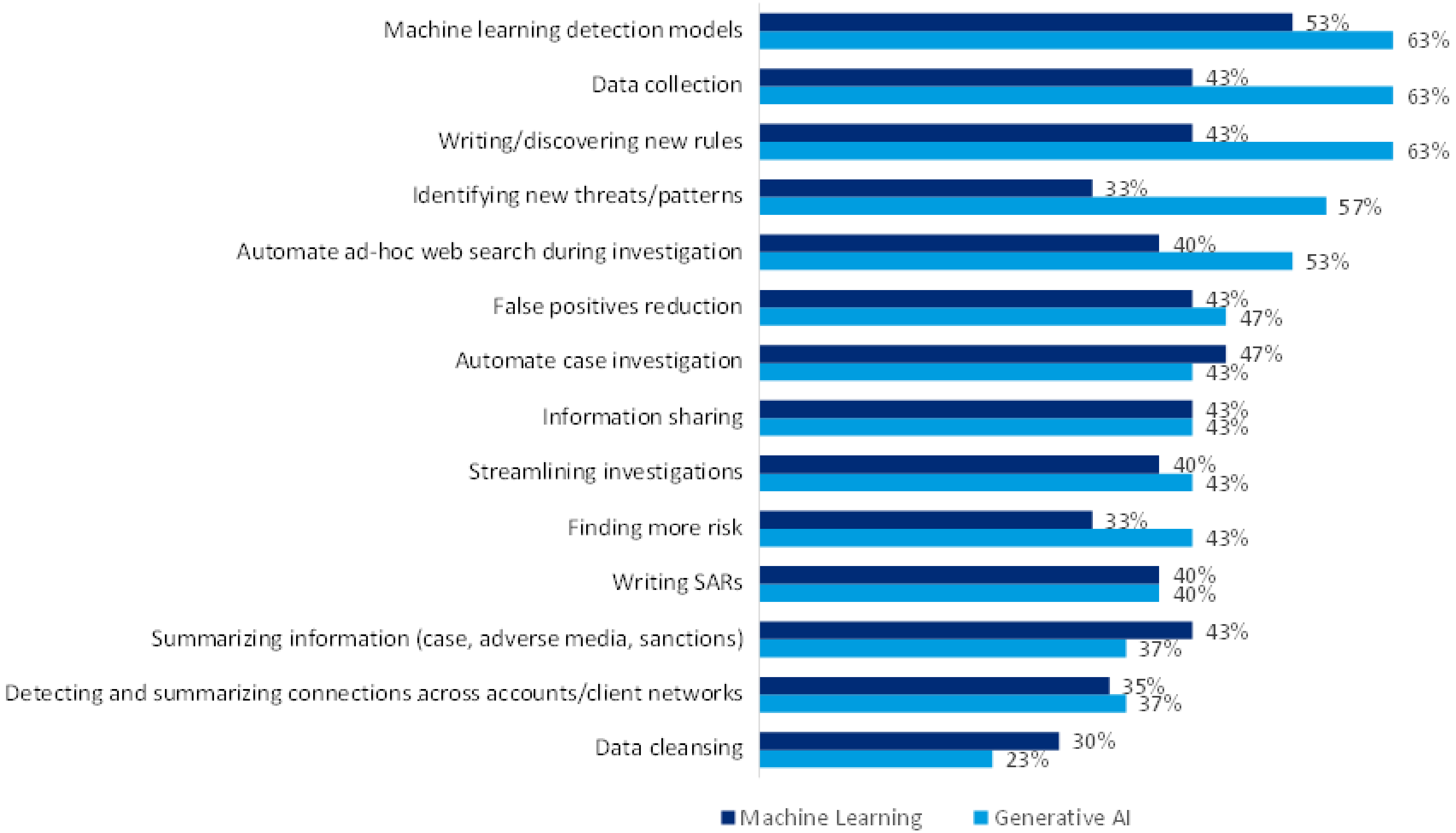
Generative AI in particular is seen by almost two-thirds of banks as having the greatest potential for impact in building machine learning models, writing new rules and data collection.

Again, we see a solid balance between effectiveness and efficiency, with AI delivering stronger abilities to detect and prevent financial crime while also, by automating and streamlining investigative tasks, lowering the load on teams working to achieve this.

One bank highlights the importance of AI in supporting fraud and AML detection: “Right now, a lot of fraud detection is reactive, which means that fraud is detected after it has already been committed. However, the future lies in preventative measures, such as using AI and behavioral analysis to spot potential fraud before it even happens. That's something we're actively working toward.”

In our interviews, mid-market banks had less to say about generative AI in concrete terms, suggesting they are still exploring the potential for this new technology.

Impact of Machine learning and generative AI on fraud and AML use cases: Next 12-18 months



Question: *Which use cases do you think machine learning and generative will have the greatest impact on over the next 12-18 months for mid-market institutions like yours?*
Total of “Significant Impact” and “Moderate Impact” responses
Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey*, 2025. N = 30

5

Conclusion

Building blocks for fraud and AML collaboration

Benefits of fraud and AML collaboration

Fraud and AML share a common aim in protecting the institution from financial crime. At the same time, they have significant differences. Fraud operations focus on preventing and detecting deceptive acts of personal gain, whereas the core focus of AML operations lies in preventing the use of financial institutions to launder illegal funds or finance terrorism.

One of the biggest advantages of collaboration is the ability to detect suspicious activities much faster. Fraud cases often provide early warning signs of potential money laundering, while AML investigations sometimes uncover fraud schemes that wouldn't have been obvious to the fraud team alone. By collaborating, banks can connect the dots and identify the origin of the threat.

Next steps for alignment

Bringing together fraud and AML requires collaboration and convergence of people, processes and technology. A preliminary roadmap could include:

Collaboration across people and processes
Steps to enhance collaborative processes between teams:

- Sharing data across fraud and AML to enhance detection and increase efficiency
- Cross-training for teams to facilitate working across functions as needed
- Providing holistic fraud and AML risk data to CROs and compliance teams to support comprehensive anti-financial risk strategies

Technology convergence
Technology architectures to support fraud and AML convergence:

- Unifying fraud and AML detection on a single platform
- Leveraging AI and machine learning capabilities to identify suspicious activity and patterns and support process automation
- Data integration, such as via a data lake, to create a centralized repository to support collaborative analysis of fraud and AML

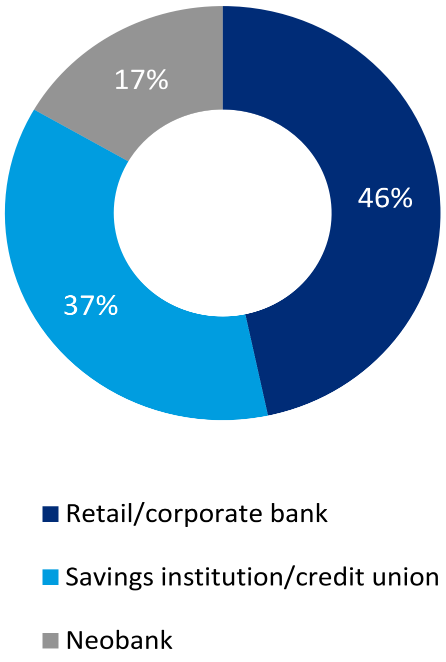
About The Survey

About the Survey

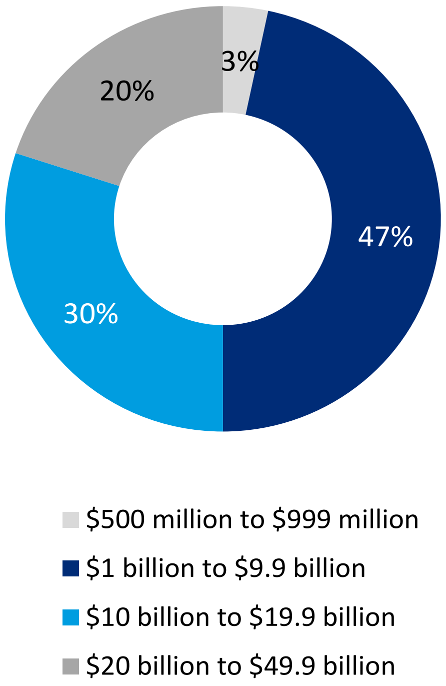
This survey on organizational, operational, and technology trends in fraud and AML convergence was designed by Celent and Hawk. The survey was fielded in February and March 2025. A total of 30 anti-fraud, compliance, operations and IT professionals at US institutions completed the survey. The distribution of survey respondents by type and size of institution and respondent's role is shown below.

In addition, anti-financial crime professionals sat for in-depth interviews on fraud and AML trends. Their institutions are described in the body of the report.

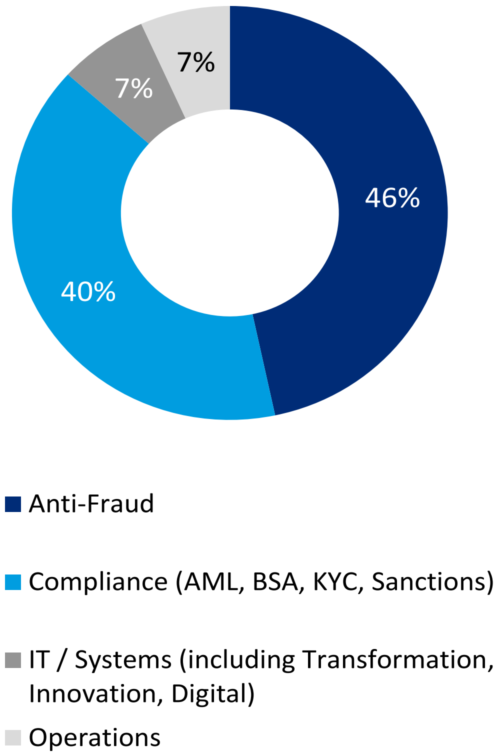
Institution type



Asset size, USD



Area of responsibility



Source: Celent/Hawk *Trends in Fraud & AML Convergence at US Mid-Market Banks & Credit Unions Survey,* 2025

About Hawk

HAWK

Hawk is the leading provider of AI-supported anti-money laundering, screening and fraud prevention technology. Banks, fintechs and payment providers globally use Hawk's modular platform to pinpoint financial crime risk with precision, cut fraud losses, and ensure regulatory compliance. Hawk's holistic, real-time approach to transaction monitoring, payment and customer screening, customer risk rating, and fraud prevention enables financial institutions to significantly increase the effectiveness and efficiency of their anti-financial crime operations, responding to threats at speed. For more on Hawk, please visit www.hawk.ai.

Interested in learning more?

Celent Research, Risk

Dimensions: Risk & Compliance IT Pressures & Priorities 2025 Edition

Generative AI – What are the Risks?

Resourceful Resilience: How Operational Resilience Regulation is Leading GRC Transformation

IT and Operational Spending on Financial Crime Compliance: 2024 Edition

Financial Crime Compliance Technology: AML Transaction Monitoring Edition—2023 XCelent Awards

Dimensions: Financial Crime IT Pressures and Priorities 2024

GenAI-oneers in Risk & Compliance: Cross-Sector Survey and Spotlights

IT Spending on Risk Management in Banks: 2024 Edition

IT and Operational Spending on Fraud: 2024 Edition

Financial Crime Compliance Technology: Watchlist Screening Edition—2024 XCelent Awards

Copyright Notice

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

Celent.

A part of GlobalData