Ovum

Adopting an Integrated Approach to Fraud and AML Compliance

Assessing best practice in tackling financial crime

Independent research commissioned by FICO

FICO® Fraud Security & Compliance

Contents

About the author

Daniel Mayo

As director of Ovum IT Data Tools & Insights, Daniel Mayo leads our work on the global tracking of enterprise-level ICT spending. He also serves as chief analyst in the Financial Services Technology team.

In his twin roles, Daniel oversees the development of Ovum's quantitative ICT market and sales intelligence tools for buyers and sellers in the enterprise tech market and vendor decision-making.

He also guides our coverage of technology strategy and investment in retail, corporate banking, wealth management, and buy-side institutions.

Summary

In brief

Financial crime, whether fraud against bank customers or use of the financial system to support criminal activity such as money laundering or terrorist financing, is an underlying challenge for the banking sector. Such activity is becoming ever more sophisticated and organized; the range and volume of attacks is diversifying, while banks face escalating pressure to tackle this crime from regulators, customers, and shareholders.

The resulting impact of these pressures is now leading institutions to consider a fundamental question: Is the current approach to tackling financial crime sustainable or should they seek a more integrated approach to fraud and anti-money laundering (AML) compliance in this area? To assess this, Ovum surveyed 114 retail banks on their priorities, challenges, and plans for financial crime, looking to assess the maturity of the sector in tackling financial crime and its ambitions toward integration.

Ovum view

While retail banks are concerned about potential regulatory fines and increasing costs, their primary goals are to protect the customer and safeguard their own reputations. Detection effectiveness is central for both fraud and AML compliance. However, the ability to manage financial crime is impeded by the lack of availability of skilled staff and the limitations of technology platforms. Banks struggle to deal with resulting workloads and ensure a positive customer experience.

As a result, the retail banking sector has reached an inflection point where it is actively seeking to adopt more radical approaches. Particularly from staffing and technology perspectives, banks are looking to drive synergies between fraud and compliance functions. Significantly, this seems to be driven from the functions themselves in recognition of potential effectiveness benefits and cost synergies.

Key messages

- Only a quarter of retail banks have adopted an integrated approach to financial crime systems, but active collaboration between functions is now the norm.
- Two-thirds of banks take a strategic approach to integration, driven by detection and scalability benefits in addition to cost synergies.
- Seventy percent of banks are looking to achieve integration synergies and are seeking to do so within three years.
- North American banks are typically more mature in their approach to tackling financial crime, driven by the strength of technology platforms.
- Key challenges with existing technology platforms are adaptability and speed, with banks looking to artificial intelligence (AI) to improve effectiveness in both AML compliance and combating fraud.

Enhanced effectiveness key to financial crime functions, but resulting workloads strain retail banks

Financial crime, whether fraud against banks and their customers or use of the financial system to support criminal activity (such as money laundering or terrorist financing), is an ongoing challenge for the banking sector. Pressure to tackle financial crime remains intense, driven by continuing regulatory and government scrutiny and customer expectations that banks should protect their money in all situations. Concurrently, criminal activity itself has become increasingly sophisticated and professional, resulting in ever-evolving and organized attacks that banks must defend against.

For banks, addressing financial crime is now a significant operational burden, with multiple functions involved in enhancing prevention controls and also in delivering detection, investigation, and reporting of

potential financial crime. Most banks have one or more fraud team(s), which focus on activity attacking customers, and separate compliance function(s), responsible for managing financial crimes such as money laundering and terrorist financing and for sanctions. In turn, these functions generally operate within or report to broader risk and/or compliance departments, supported by technology and security functions. All need to work alongside the bank's broader front-office and operations functions.

This approach has allowed banks to respond to various demands to tackle financial crime for each product type, channel, or regulatory requirement. But over time, it has compounded the operational challenges, from both an efficiency perspective, as the resource burden has increased, and an effectiveness perspective, as financial crime becomes more sophisticated, attacking institutions through multiple points.

To explore emerging best practice in combating financial crime and uncover whether institutions are taking a more integrated approach in both tackling fraud and AML compliance, Ovum conducted a primary research program. A total of 114 retail banks participated in a survey in April 2019. The survey was targeted at divisional heads of the main functions tasked with tackling financial crime, covering both fraud and AML compliance teams, as well as at overall risk, broader compliance, security, and technology heads. Respondents were directly involved in driving and/or supporting their institution's approach to financial crime activities. The program covered large and medium-sized institutions across North America, the UK, Germany, Austria, the Nordic countries, and South Africa. More in-depth details on survey demographics and methodology are provided in the appendix.

Given that terminology usage can vary across regions, it should be noted that reference to "financial crime" in this report includes both fraud management and compliance activities related to financial crime prevention. When addressed specifically, "AML compliance" refers to all regulatory requirements relating to financial crime (AML, counter-financing of terrorism [CFT], sanctions, including know-your-customer [KYC]/customer due diligence [CDD] requirements within these). For the purposes of clarity, reference to banking financial crime functions or activities refers to the sector's efforts against financial crime (rather than to the banks' being involved in committing fraud or money laundering themselves).

What drives banks' financial crime strategies?

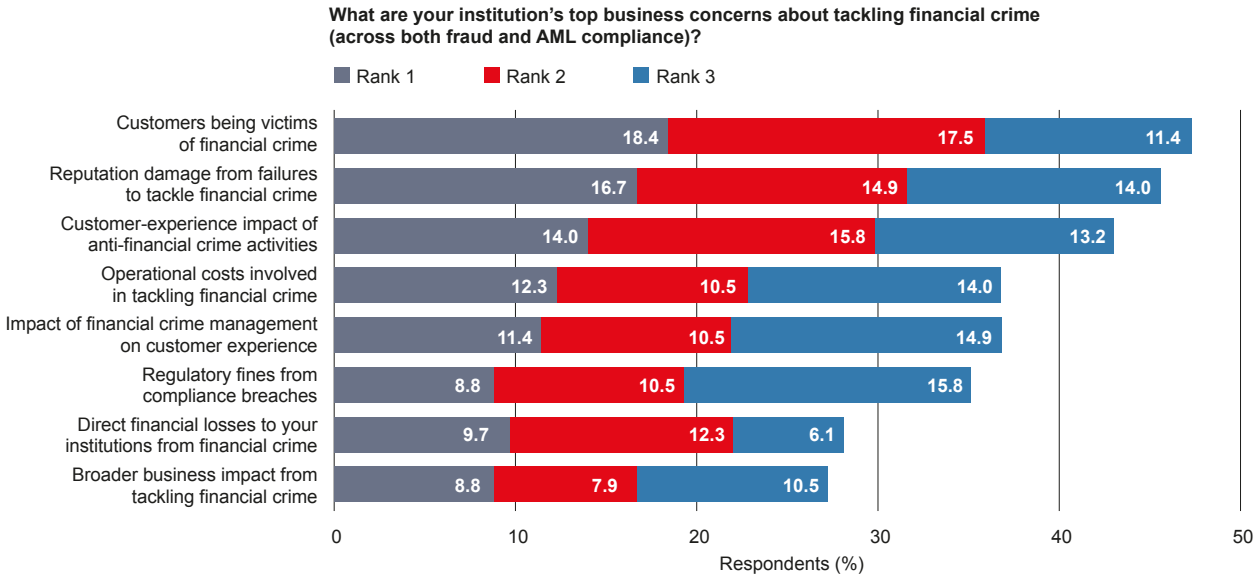
Since the financial crisis, regulatory fines for the global banking industry for compliance breaches related to AML or sanctions failures have total over $28bn. Some single fines have been as high as $8.9bn. Regulatory crackdown on financial crime compliance has been notable in the US, but recently large fines have also been levied in Europe. Significant fines drive financial crime prevention high up the executive agenda. However, this regulatory "stick" is only one driver for banks to tackle financial crime. Banks also wish to protect their customers and themselves.

However, while doing so, banks do not want to inhibit legitimate customers from conducting their rightful financial business, particularly if that results in an erosion of the customer experience and affects the bank's ability to meet its own objectives. Financial crime activities are a significant operational cost; with cost pressures in industry an ongoing challenge, banks need to both find resource and assess spend against investment in other functions.

Fines, operational costs, and financial losses drive financial crime functions, but protecting customers and reputation is the overarching concern

The balance of such business concerns was explored in the primary research study, with overall results shown in Figure 1. While concern about regulatory fines was certainly evident, it was only ranked as a top-three issue by just over one-third of retail banks surveyed. Instead, the top overall concern is actually protecting customers from being the victims of crime. The longer-term reputation damage from failures to tackle financial crime is a stronger driver than either fines or resulting losses suffered by banks. The other primary concern is enhancing the customer experience of financial crime activities, such as reducing the time taken to conduct and resolve fraud investigations. The impact of controls on the broader customer experience is evident but is a secondary concern.

Figure 1: Top business concerns in tackling financial crime



Source: Ovum

There are regional differences in the weighting of the business issues. Given the magnitude of fines in the US, relative are concerns over regulatory fines from compliance breaches is unsurprisingly higher for North American banks, as are challenges over the operational costs involved in tackling financial crime. However, the overall perspective is very much akin, albeit fears over reputation damage are the joint-top driver in North America (along with customers being the victims of financial crime), with the focus on the impact on customer experience relatively strong in Europe.

Divergence in objectives is rather more evident among the various business functions involved in tackling financial crime. Reputation damage is a much stronger driver for compliance, with relatively low concern for customers being victims. Similarly, regulatory fines are a much higher worry on the compliance side, while fraud divisions are principally driven by preventing customers from becoming victims of financial crime. Conversely, the main areas of commonality lie around the challenges of minimizing the customer-experience impact and managing the overall operational costs of financial crime operations.

Ensuring detection rates are high is a top challenge but causes major pain points when it drives increased false positives and alerts

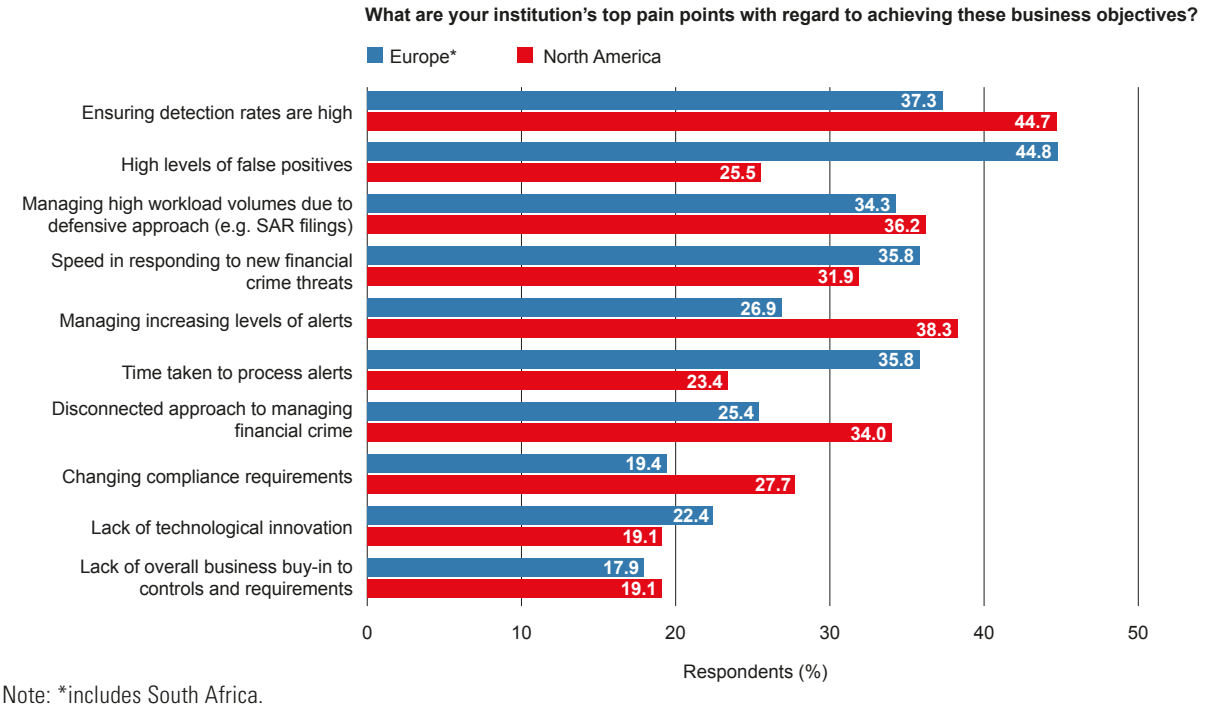
There is an array of business goals for financial crime functions. Figure 2 highlights the top pain points in achieving these objectives. The top objectives are to protect customers from being victims of crime and to prevent financial crime in order to protect the institution's reputation (as shown in Figure 1). It is unsurprising that the top pain point lies in ensuring detection rates are high. This pain is more pervasive in North America, where reputation concerns over detection failure were also more widespread, but this was consistently identified by retail banks as a primary challenge in all markets. It was also highlighted as a top pain point across the different business functions surveyed, although notably so by fraud, compliance, and security heads.

Ensuring a high rate of detection of financial crime creates major operational challenges in the subsequent operational workloads for financial crime functions. Particularly in Europe (and South Africa), institutions struggle to manage high levels of false positives, where suspected fraud activity is identified that subsequently turns out to be genuine. Institutions have sought to increase overall detection levels to ensure more actual financial crime is caught but have not been able to improve detection accuracy, resulting in increased investigation workloads. In comparison, in North America it is more simply the overall volume of alerts requiring investigation that is the challenge (whether the activity in question is illicit or not).

The research also found that all markets are struggling with compliance workloads, with fears over reputation damage and fines if breaches do occur. Institutions respond by adopting a highly defensive approach to reporting any potentially suspect criminal activity. Consequently, investigation and reporting

workloads have become onerous. This was only a slightly higher challenge for North American banks where regulatory scrutiny and penalties have been significant for many years, suggesting such pressure is now pervasive. Unsurprisingly, this is a markedly pervasive pain point for compliance functions, with fraud divisions more able to take an approach based on their own risk appetite.

Figure 2: Top pain points for retail banks in tackling financial crime



Note: *includes South Africa.

Source: Ovum

The impact of dealing with higher volumes has secondary challenges. For European institutions, which have a relatively high concern over the customer-experience impact of financial crime activities, the time taken to process alerts is a significant issue. Extended workloads mean banks struggle to investigate and resolve alerts in a timely manner (e.g., identifying false positives or being able to offer remediation when fraud has occurred), driving a protracted and more painful experience for customers affected.

Speed is a wider issue, highlighted particularly by the inability of fraud and security functions to respond to new threats in a timely manner. Financial criminals are increasingly sophisticated and professional, adapting and creating new attacks as banks become more effective in detecting existing ones; banks must respond quickly to emerging threats.

Resource requirements are an ongoing challenge for tackling financial crime, exacerbated by technology platforms

Managing the operational costs of financial crime activities was identified as a top-three concern by 37% of institutions (Figure 1). The need to improve detection rates and tackle increasing volumes is a key driver for increased operational cost. The study found overall operational expenditure on all financial crime activities increased by 9.3% between 2015 and 2019 (weighted average). This may initially appear somewhat undramatic; however, this growth is in a context of active reduction of the overall operating cost base for most institutions over this period, as banks have sought to improve their cost/return on equity ratios. It also follows a phase of sustained growth of expenditure on these activities since the financial crisis, with costs already significant for most institutions by 2015.

This average also masks a notable spread in the range of cost growth for financial crime functions. Very few retail banks (just over 5%) managed to decrease overall cost since 2015, but around half consider that they have managed to contain cost growth (at 0–5%), and a further fifth experienced relatively modest growth of

6–10%. In contrast, expenditure growth for retail banks in some markets has been far more marked. North American banks, in particular, have seen very high expenditure growth, with 22% of large banks (retail customer base over 5 million) in the region stating they have experienced growth above 20% since 2015 and more than a tenth experiencing growth of operating expenditure on financial crime above 50%.

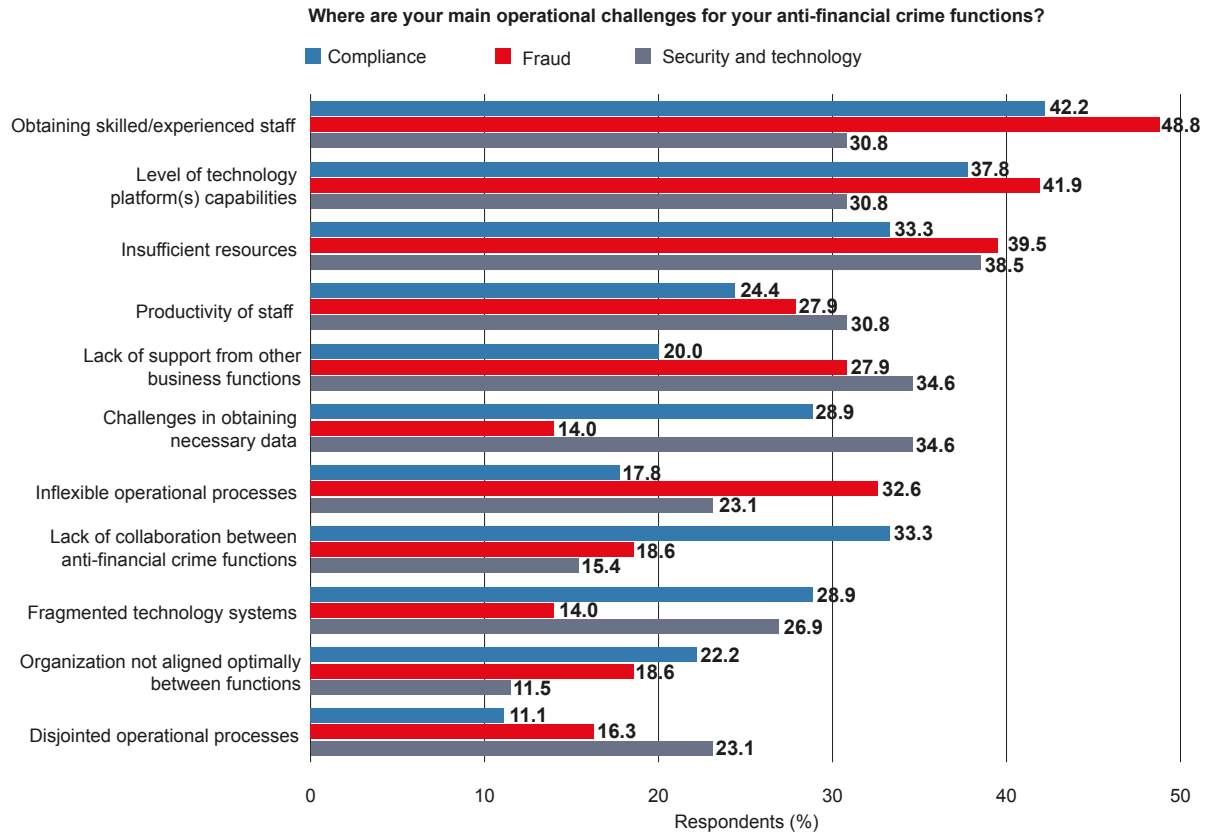
Technology platform capabilities and skilled staff are the core operational challenges across financial crime functions

With three-quarters of banks keeping operating expenditure growth below 10%, higher workloads mean lack of resources is a common operational challenge across all of the business functions surveyed. As Figure 3 shows, insufficient resources were identified as one of the top-three challenges across all business functions (note that head-of-risk respondents have been grouped with financial crime compliance). However, for both fraud and compliance functions, the main challenge is the difficulty of obtaining skilled and experienced staff, with the rapid expansion of financial crime departments across the banking sector over the last decade creating a talent-pool shortage.

This core operational challenge is compounded by the lack of capabilities of technology platforms supporting these staff, identified as the next key issue by both fraud and compliance. Interestingly, this was also ranked as the top challenge by technology heads supporting anti-financial crime (although seen as a less significant challenge by security heads). This lack of platform capability exacerbates the staffing challenge, with the inability of functions to increased staff productivity to cope with increase workloads a common problem across all functions.

Mirroring the higher pain point seen in Figure 2 by fraud functions around speed of adapting to new threats, inflexible operational processes were also identified as a key challenge by heads of fraud. However, overall, the dominant operational challenges seem to relate more to people and technology than to process and organization factors.

Figure 3: Main operational challenges for anti-financial crime functions



Source: Ovum

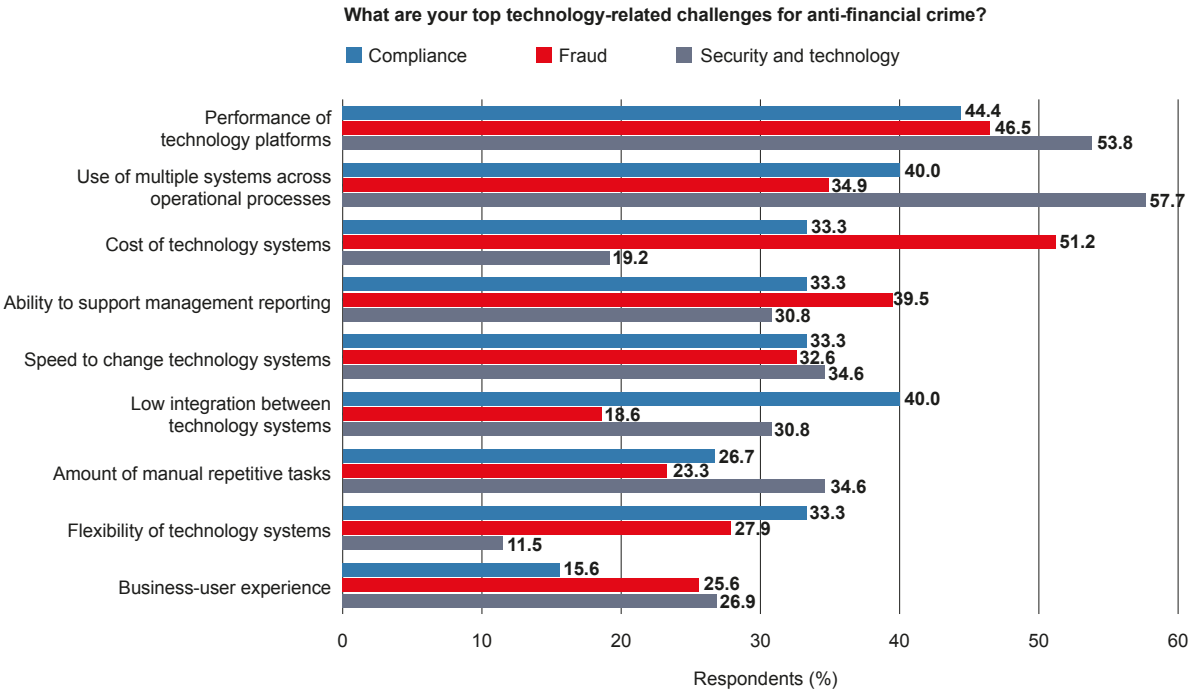
Performance is the underlying challenge, compounded by use of multiple systems and low levels of integration

Figure 4 drills down into the technology-related challenges by anti-financial crime function. Platform performance is identified across all functions as one of the most pervasive issues for retail banks. However, particularly from a technology-division perspective, this is compounded by use of multiple systems across functions as well as a low level of integration between systems within compliance.

Use of multiple systems creates multiple issues. Switching between systems across procedures impacts staff productivity, helping to create disjointed operational processes. It also drives higher overall cost, with duplication of functionality, extra maintenance, and additional integration workloads. It impedes adaptability, because changes require more testing and integration across multiple platforms, and makes management reporting challenging in more complex data extraction and standardization; both of these issues were identified across functions as significant secondary technology challenges.

Use of multiple systems across operational processes also exacerbates the underlying skilled-staff availability issue identified as the top overall operational challenge. Each system requires specific training and resource support, impeding the ability of banks to manage and transfer skills within and across functions. This was particularly a challenge on the fraud side: a quarter of institutions consider that this drives user-experience challenges for fraud investigations staff and is behind the staff productivity challenges identified in Figure 3.

Figure 4: Top technology-related challenges for anti-financial crime



Source: Ovum

Cost synergies and detection benefits drive an integrated approach to tackling fraud and AML compliance

Financial crime functions are battling the challenges of enhancing detection effectiveness, managing volumes, and being agile in responding to changing threats. This is against a backdrop of resource constraints, skilled-staff shortages, and platform-capability limitations. There is a fundamental question for the banking sector: Is the current approach sustainable? Does a piecemeal approach to tackling financial crime, driven by the evolution of separate functions to deal with threats by product, channel, or compliance requirement, work from efficiency and effectiveness perspectives?

While fraud and AML compliance have differences, particularly regarding the level of discretion institutions may have in setting policies, there are many areas of commonality. To drive efficiency and effectiveness synergies, we must consider the people, process, and technology levels. Obtaining such synergies demands answers to the question of whether strategy and organizational drive are enough to make this happen.

The primary research study explored this topic, looking at current approaches to integrated fraud and AML compliance as well as future ambitions.

Strong synergies already drive a high level of collaboration between fraud and AML compliance functions

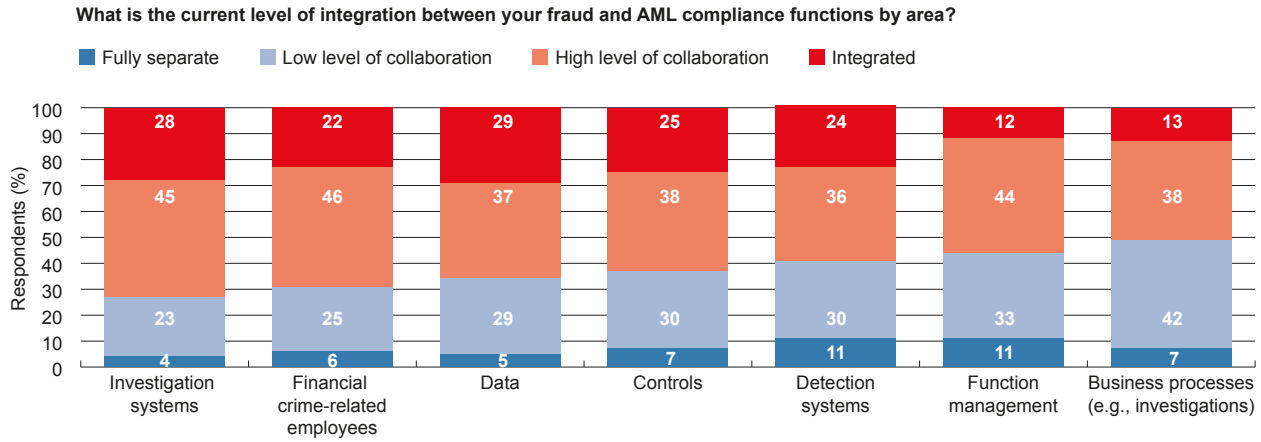
At an organizational level, the reporting lines for fraud and AML compliance are typically separate, with around two-thirds of retail banks surveyed stating that these reported into different business executives. Compliance, unsurprisingly, tends to report in through compliance and/or risk functions, whereas the organization of fraud functions is often more varied, reporting through the business units, risk, or compliance (albeit from a consumer-protection perspective), and, of course, most institutions will operate in a matrix structure.

That said, conversely, one-third of banks do currently have fraud and financial crime reporting into the same business executive. This is largely an institution-specific decision, with limited differences between banks grouped across the different countries surveyed, except in North America, where there is a polarization in approach between Canada, where 60% have common reporting lines, and the US, where only 25% do. There is only a small difference relative to respective size of bank, with 36% of medium-sized banks taking this approach compared to 30% of large banks, suggesting that scale is not a determining factor.

Only a quarter of retail banks have adopted an integrated approach to financial crime systems, but active collaboration between functions is now the norm

Drilling down from integration at the executive level, Figure 5 shows the approach to integration taken across people, processes, and technology (including data). In terms of organization structure, even fewer banks (12%) have integrated function management between the two areas. However, there is far stronger integration across several areas at a process and technology level. This is particularly true with respect to data and investigation systems, where 29% of retail banks are using centralized data and 28% are using an integrated platform, and the figures are only fractionally lower for control and detection systems. Interestingly, a fifth (22%) of institutions already have an integrated workforce across fraud and financial crime compliance. Integration at a business-process level itself is much lower (13%), and a similar proportion have integrated function management (unsurprisingly, there is strong correlation between the two).

Figure 5: Current level of integration between fraud and AML compliance by area



Source: Ovum

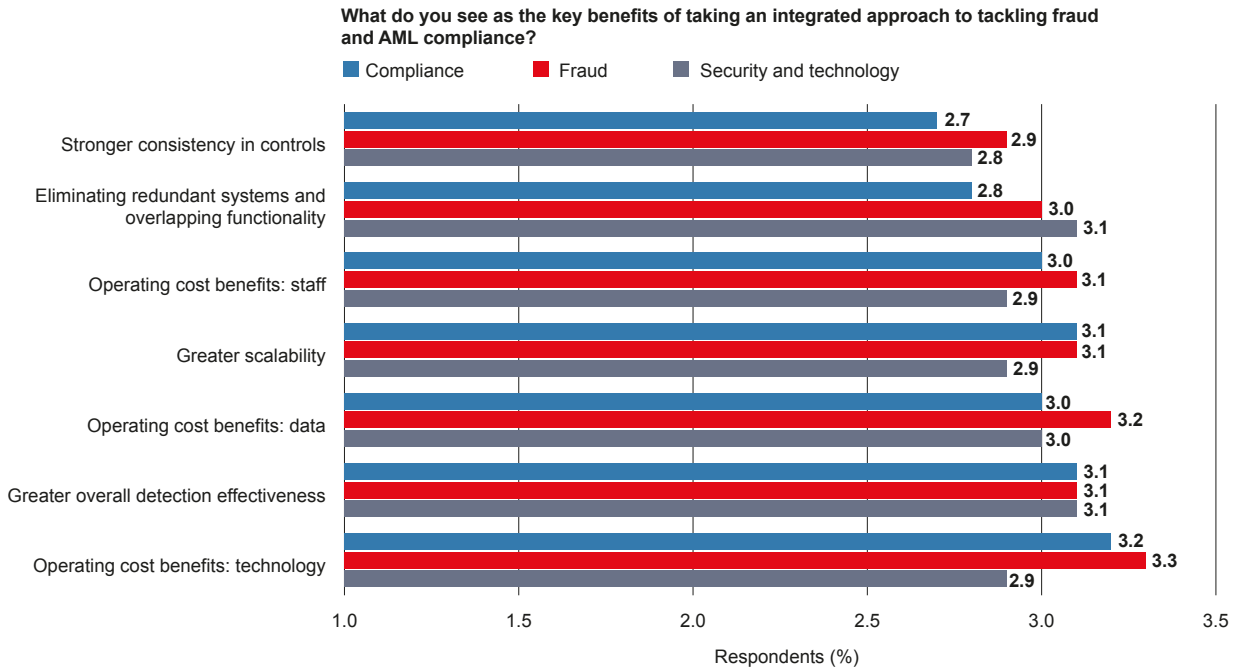
Averaging across these areas, only a fifth of institutions are currently integrated between fraud and AML compliance. However, as Figure 5 shows, banks are collaborating between functions. Fewer than 10% of banks stated that they were operating these functions completely separately. Indeed, on average across these areas, 40% of banks have a high level of collaboration, with the remaining 30% having some level of sharing between the two. Interestingly, a high proportion of banks are seeking synergies on the people side, including both the financial crime workforce and function management, with platform and data also strong. In contrast, the approach to obtaining business-process synergies is more 50/50.

At a regional level, this collaborative approach is broadly similar between North America and Europe. Intriguingly, there is only a relatively small difference in approach between Canada and US banks (compared to the difference in executive reporting lines). This suggests that this is being driven by bottom-up as well as top-down synergy benefits and led by executive management looking for cost savings.

An integrated approach is driven by detection and scalability benefits in addition to cost synergies

Figure 6 shows where institutions have seen or expect to see the key benefits from taking an integrated approach to fraud and financial crime compliance. Respondents were asked to rate the strength of benefits on a 1–4 scale (4 being a high benefit). A rating of over 2.5 suggests that institutions see the area as a benefit, whereas an average of over 3.0 suggests that it would be considered a significant benefit.

Figure 6: Benefits of an integrated approach to tackling fraud and AML compliance



Source: Ovum

While cost synergies are deemed significant, particularly on the technology side (although more strongly by the business than the technology functions), effectiveness synergies are consistently identified by all functions as significant. This mirrors the earlier observation that the move to an integrated approach is not just a top-down-driven cost-synergy play but also one driven more organically by the ability of functions to improve their overall effectiveness. This means both improving detection effectiveness (the top challenge for financial crime) and enabling scalability. The latter is key as institutions seek to manage growing workloads with limited resources.

Reflecting this is the finding that institutions do see benefits across a breadth of areas, with all of the potential benefits receiving average ratings above 2.5. Significantly, this is true across all business functions. Fraud heads as a whole perceive higher synergy benefits, but these are only fractionally higher than those seen by financial crime compliance or supporting technology/security heads.

It is interesting that technology functions do recognize significant value from eliminating redundant systems and overlapping functionality, even if they are perhaps more cynical about overall technology cost synergies.

Majority of banks have strategic and near-term plans to drive toward integration

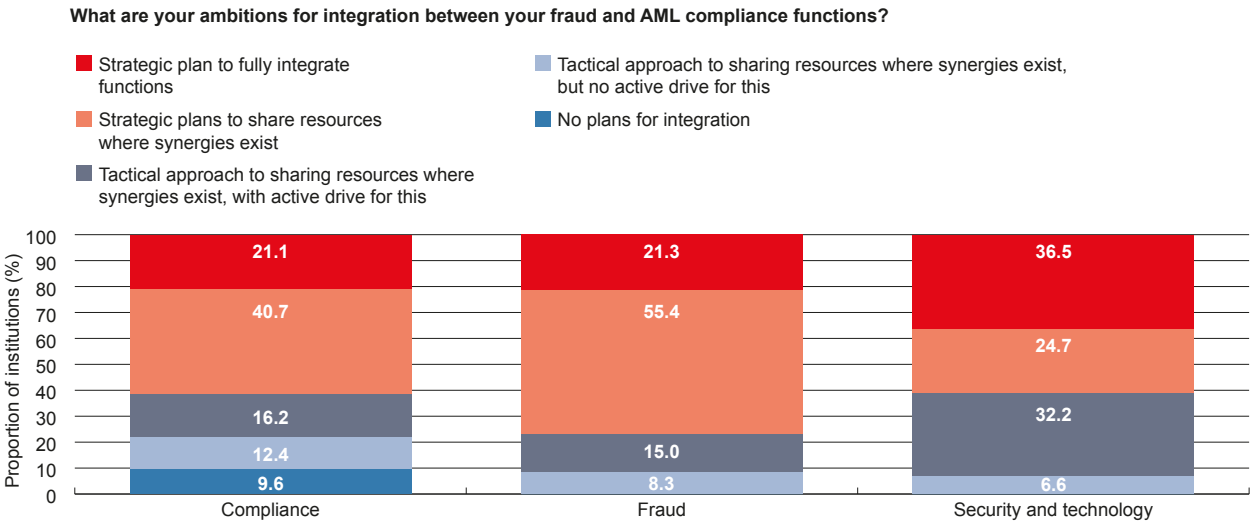
Given that collaboration between fraud and compliance is now the norm, driven by both effectiveness and efficiency benefits, what ambitions do institutions have to drive toward further integration in the future, and what are their timescales for this? Perhaps unsurprisingly, the trend is toward further integration, with business pressures resulting in two-thirds of the sector taking a strategic rather than tactical approach to this. Significantly, this strategic approach is translating into active plans. The majority of institutions that are actively looking toward integration seek to do it within three years.

A strategic approach to integration is the majority approach across all financial crime functions, particularly for fraud and compliance

Looking at long-term ambitions for integration between fraud and AML compliance, we see in Figure 7 the respective plans grouped by financial crime business function. Two-thirds of banks have strategic plans for further integration, either to fully integrate functions or to share resources where synergies exist, with a further 20% actively seeking to obtain synergies even if they are only taking a tactical approach.

At a business-function level, Figure 7 shows that the overall story is similar on all sides, although, perhaps reflecting the higher perceived benefits seen in Figure 6, the fraud side is more active overall (fewer than 10% of fraud heads have no plans or are not actively seeking synergies). The main reticence, where evident, comes from the compliance side, with just over a fifth of function heads here having no plans for integration or no active drive for this. However, even on this side this is the minority, with over 60% operating with strategic plans. The push for financial crime integration is being driven from all sides.

Figure 7: Ambitions for integration between fraud and AML compliance functions

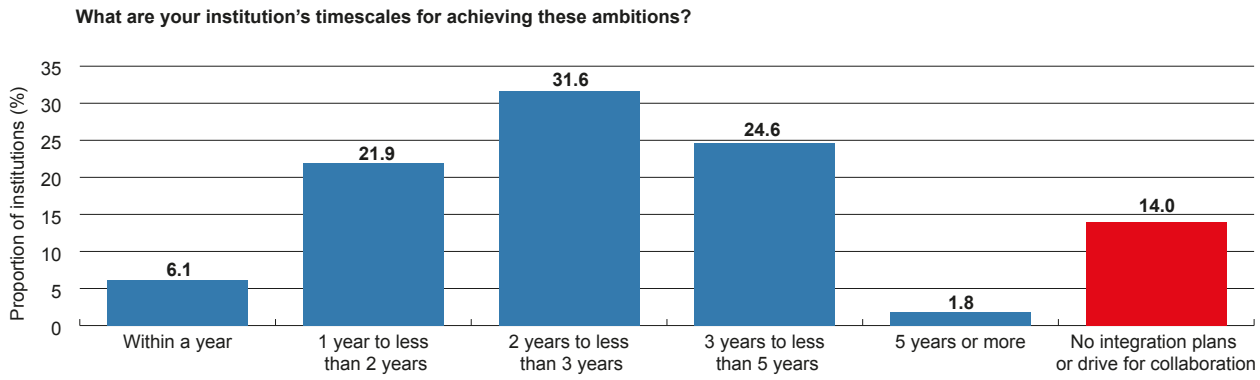


Source: Ovum

Across plans by size and region, the picture is very similar. Just over 70% of medium-sized and large banks in both North America and Europe (including South Africa) have strategic plans. At the country level, the UK and Canada are the most ambitious in moving toward a fully integrated model, with other markets centering around strategic plans for obtaining synergies without full integration.

More than 70% of banks that are actively looking to integrate fraud and compliance seek to do so within the next three years

Figure 8: Timescale for financial crime integration ambitions



Source: Ovum

Given ambition is not necessarily a full proxy for action, Figure 8 looks at the timescales institutions are operating on for achieving these ambitions. As a rule of thumb, objective timescales beyond three years tend to suggest that an institution is not actively engaged, even if it has "active" plans. From the responses, the majority actually seem to be actively pursuing synergies between financial crime functions. Excluding those that have no plans or drive for integration (i.e., the red bar shown in Figure 8), just under 70% of those that have active plans seek to implement them within three years. Indeed, of institutions that have strategic plans for full integration (as shown in Figure 7), over 75% plan to do it within three years. Longer time frames are more evident where institutions have tactical, rather than strategic, plans to seek synergies; here less than half seek to do so within three years.

Technological strength underpins the maturity of banks in tackling financial crime

There is widespread agreement that there are significant effectiveness and efficiency benefits from taking an integrated approach across fraud and financial crime compliance (Figure 6). However, as found earlier, there is notable variation across the retail banking sector in both the current level of integration and future ambitions toward integration (Figures 5 and 7). Despite tackling financial crime being a long-standing and mandatory requirement that has seen significant investment over the last decade(s), there remains significant variation in the maturity of banks in their approach to it.

To appraise this, the primary research program asked the responding institutions to self-assess against a maturity model, evaluating their progression against best practice across a number of dimensions deemed critical for tackling financial crime.

North American banks claim to be more mature in tackling financial crime than European counterparts

From an overall perspective, reflecting the mandatory nature of tackling financial crime, the average level of maturity is fairly high (in comparison to maturity evaluations Ovum has conducted in other areas). However, there is significant variation by market as well as by institution. If the results are taken at face value, North American banks appear to be generally more advanced than their European counterparts. While most banks are comparatively advanced at a strategy and organization level, disparity is primarily accounted for by the relative strength of technology platforms.

Best practice in tackling financial crime is driven by approach to strategy, organization, operations, technology, and data

The model Ovum devised to assess the maturity of banks' financial crime activities is structured around five pillars. These address the main dimensions of business execution, considering an institution's approach to tackling financial crime across

- strategy
- organization
- financial crime operations
- supporting technology platforms
- use of data.

For each pillar, respondents were asked to assess their institution against a series of statements (shown in Figure 9), focusing on the extent to which each statement applied to their institution. The statements address key elements of both current and emerging best practice within each pillar deemed by Ovum as essential for tackling financial crime.

From these responses, Ovum also created a maturity index that allows comparison of institutions between markets and lets institutions benchmark the maturity of their financial crime functions against the industry. The index was created using the study self-assessments of how true each statement was for the institutions, with the evaluation quantified into a 0–1 score based on relative progression. For example, an institution would receive a score of 1 when the statement was assessed as completely true for it.

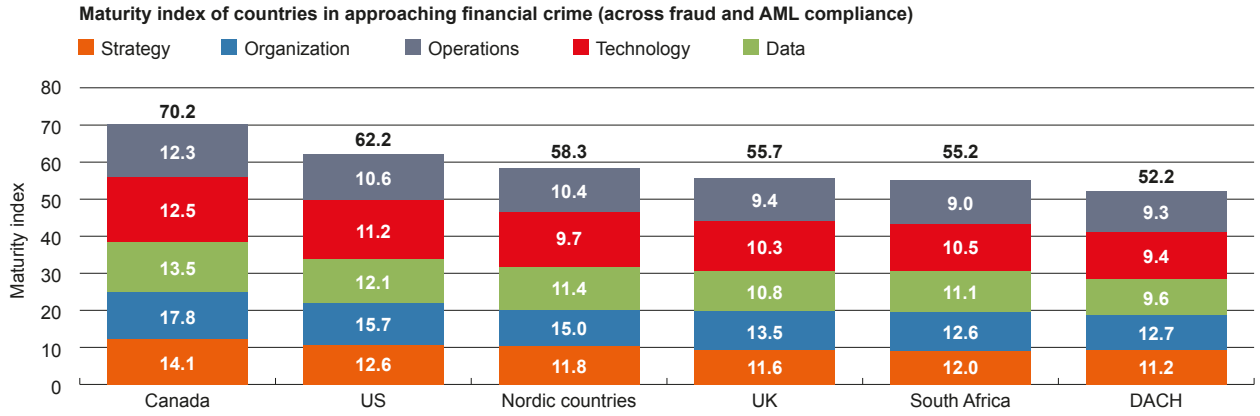
Pillar	Capability
Strategy	Financial crime initiatives are managed collectively as part of an overall roadmap Our institution has a detailed long-term roadmap across all our financial crime functions Our institution proactively searches for emerging financial crime threats Our institution is typically leading/exceeding regulatory requirements in financial crime
Organization	An integrated financial crime approach is championed at the highest level There is centralized ownership of financial crime reporting Anti-financial crime processes and capabilities are understood and executed across the organization Strong data, detection, and financial crime controls are valued as of high importance across the organization
Operations	Our institution has strong real-time detection capabilities that prevent high levels of financial crime pre-authorization Our institution has integrated teams for financial crime investigations/decisioning Our institution has a centralized team for KYC supporting fraud, financial crime compliance, and credit risk We operate with high levels of automation across our financial crime functions Our processes for tackling financial crime are highly flexible and adaptable
Technology	Our institution has centralized platforms for decisioning, scoring, and case management Business users in financial crime have a common interface and user experience across all systems Our technology platforms are highly flexible and adaptable Our institution is able to continually optimize modelling effectiveness Our platform takes advantage of latest practices in machine learning and artificial intelligence Our technology platform provides both advanced reporting capabilities at an aggregate level and explainability for individual decisions
Data	All relevant data sources are identified and used for financial crime detection purposes by our institution Data is available in real time for financial crime decisioning purposes We are fully confident in the quality of the data used for anti-financial crime purposes Data used to combat financial crime is used for all processes with no duplication or redundancy Our institution has high customer segmentation depth across multiple dimensions Our institution is able to rapidly incorporate and utilize new data
Source: Ovum	

Individual statement scores were then aggregated on a weighted basis within each pillar, with extra weighting applied for statements that the primary study revealed as being of particularly high importance to the industry. Finally, an overall index score (out of 100) was created based on a combination of the five pillars. To help conceptualize the index, a maximum score of 100 would indicate that all statements were completely true for an institution.

Canadian banks are most mature, driven by technology strength

Based on the self-assessments from the study, the respective average country group index scores are shown in Figure 10, with the total index score broken down between the five pillars for each market (DACH represents the average across Germany and Austria). From a regional perspective, it is evident there is a clear difference in maturity between the North American and European banking sectors, with the South African market aligning with European levels. Canadian banks have a relatively high level of maturity, with a notable gap beyond the US, which is itself is above European levels. In contrast, German and Austrian banks have the lowest relative maturity, scoring lowest in all pillars aside from strategy and technology.

Figure 10: Maturity index scores for tackling financial crime for retail banks by country



Source: Ovum

That said, it should be noted that overall scores in comparison to other maturity evaluations Ovum has carried out are relatively high. Overall index scores in the 20s to 30s would typically indicate an early maturing market, while scores in the 40s and 50s would suggest an average level of maturity, and scores above 60 would suggest a reasonable level of maturity is evident. While the self-assessments do indicate that moving to best practice in tackling financial crime is still a work in progress, in the main, banks are progressing toward this rather than lagging at early levels.

Drilling deeper into the pillars, it is interesting that while Canadian banks score strongly across all five pillars, their position is particularly driven by their high score in technology, followed by strategy. Central differentiators here are high flexibility and adaptability in their technology platforms, along with having detailed long-term roadmaps across all of their financial crime functions. A combination of agility and long-term planning gives the Canadian banks an advantage that appears to drive (or at least support) generally higher scores across other areas as well.

Indeed, disparities in the maturity of anti-financial crime is particularly driven by technology strength overall, with this pillar seeing most variation across markets. Here, highly flexible and adaptable platforms were the core differentiator. In contrast, variance in self-assessment evaluations among organization and data pillars was relatively low, with most banks achieving similar scores (particularly if Canadian banks are excluded). The strategy and operations pillars lie in between these and technology, with deviation in scores driven mainly by differences in having detailed long-term roadmaps on the strategy side and by the extent of having flexible and adaptable processes and strong real-time detection capabilities on the operations side.

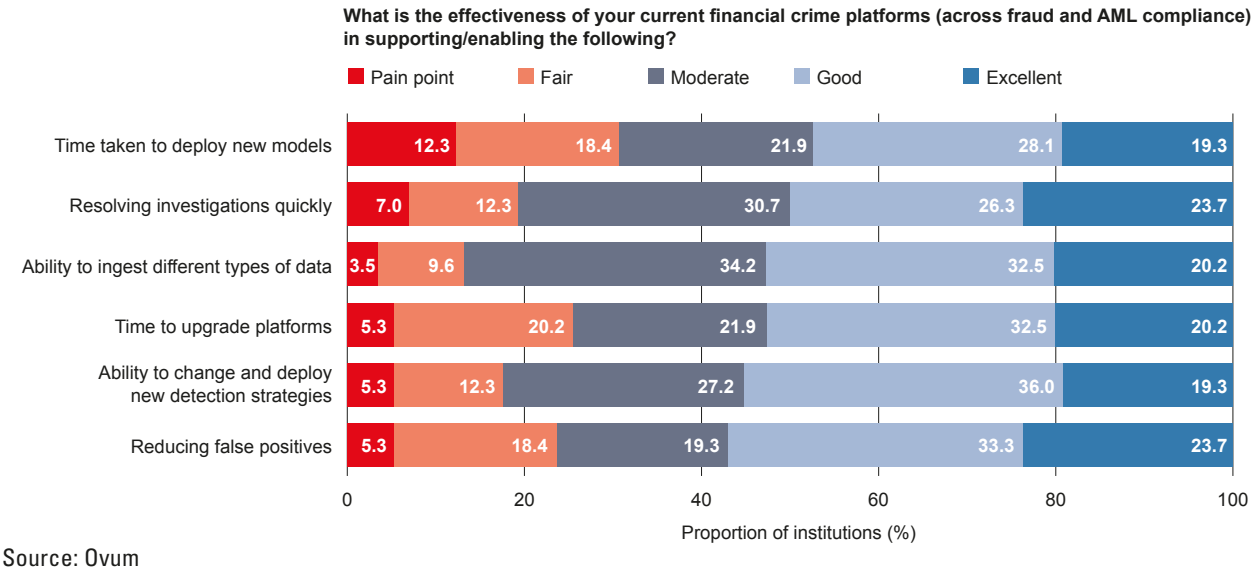
Key challenges with existing platforms lie in adaptability and speed, with banks looking to AI to improve effectiveness

The themes of challenges in flexibility and adaptability are common ones when we look into the effectiveness of current platforms in tackling financial crime. That and speed-related factors are the primary areas where there is significant variation between institutions in platform effectiveness. Perhaps unsurprisingly, these are also the areas where institutions are most looking to improve their effectiveness.

Despite significant investment in financial crime platforms over the last decade, there is a polarization in platforms' effectiveness across banks

As part of the primary research, institutions were asked to rate the effectiveness of their current financial crime platforms in supporting/enabling 24 different areas. These included capabilities around an institution's agility in tackling financial crime (e.g., overall process speeds or time required to make changes), factors that drive the customer experience, detection effectiveness, and abilities around specific payment areas.

Figure 11: Effectiveness of current financial crime platform in selected areas



Source: Ovum

Fascinatingly, despite technology platform capability being deemed one of the top operational pain points overall (Figure 3), most institutions rate their current platform effectiveness strongly at the aggregated level. Close to two-thirds of institutions considered their current platforms "good" or "excellent" on average across all factors in supporting anti-financial crime. Instead, rather than there being widespread weaknesses or capability shortfalls, challenges with current platforms are relatively specific for each institution. Institutions have invested significantly in their financial crime platforms in recent decades, and it is a small number of factors, rather than general poor performance, that is driving technology platforms to be an overall operational pain point. This could also suggest that even small shortcomings in platforms can color how banks rate overall performance.

Intriguingly, these weak points are not dominated by one or two areas across all banks; different institutions tend to have distinct pain points. That said, Figure 11 shows the factors which received the highest proportion of "ineffective" ratings (defined as receiving "pain point," "fair," or "moderate" scores). Aside from the ability to ingest different types of data, there is a common theme to these factors: speed and adaptability. Current platforms are largely effective, but the main weaknesses tend to lie in their ability to respond and make changes quickly. Challenges in supporting speed of investigations is related to this and to the use of multiple systems (identified in Figure 4).

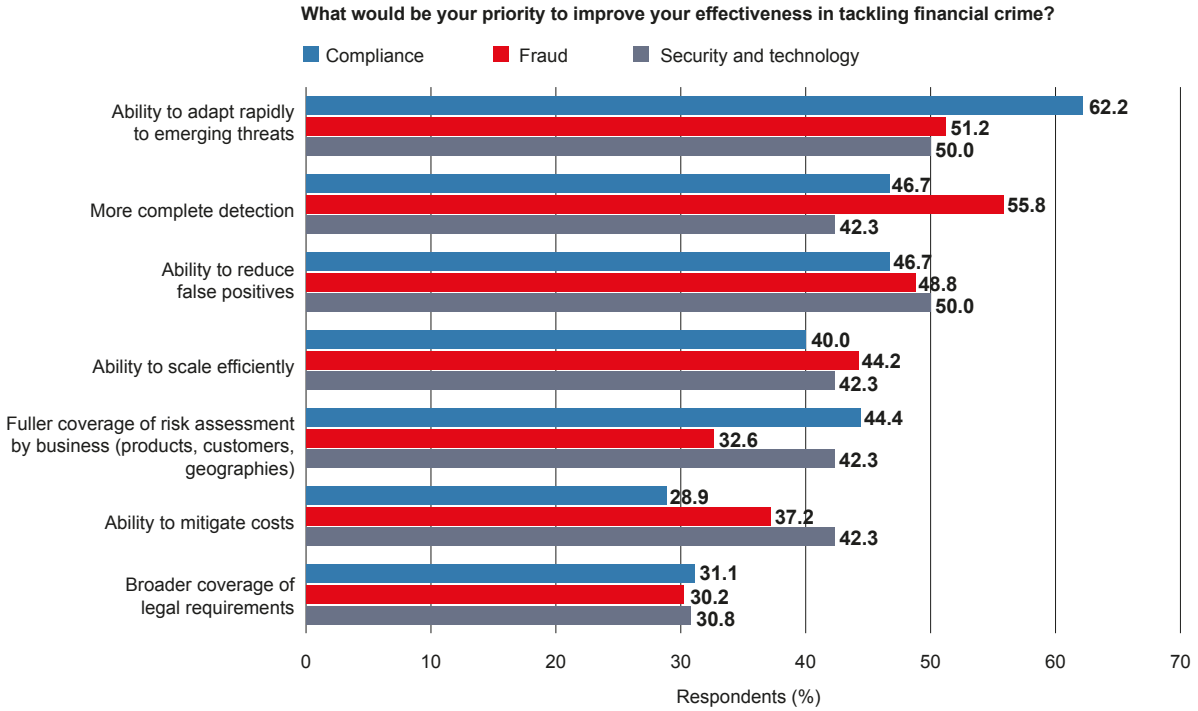
Ability to respond to emerging threats is a key priority to improve effectiveness in tackling financial crime

Given the pervasiveness of speed and agility as pain points, it is unsurprising that agility is a top priority for retail banks as they look to improve the effectiveness of financial crime activities. Figure 12 shows the rank of priorities in this area from the primary research, segmented by financial crime function. The ability to adapt rapidly to emerging threats is the top overall imperative across functions, notedly on the compliance side, but ranks alongside the ability to reduce false positives for the fraud function.

Comparing these future priorities with current pain points (shown in Figure 2), it is interesting to see that adaptability as a focus area is ranked more highly in the future view than detection effectiveness or volume/

cost factors (such as ability to scale efficiently). It is not that these latter factors become unimportant, but the ability to respond is, in the end, crucial to tackling financial crime on an ongoing basis. Becoming highly efficient and effective in tackling a specific type of financial crime is of limited value unless this can be adapted. Financial crime is an ever-evolving challenge, with criminals creating new attacks as soon as banks become effective in tackling existing ones.

Figure 12: Priorities for retail banks in improving effectiveness against financial crime

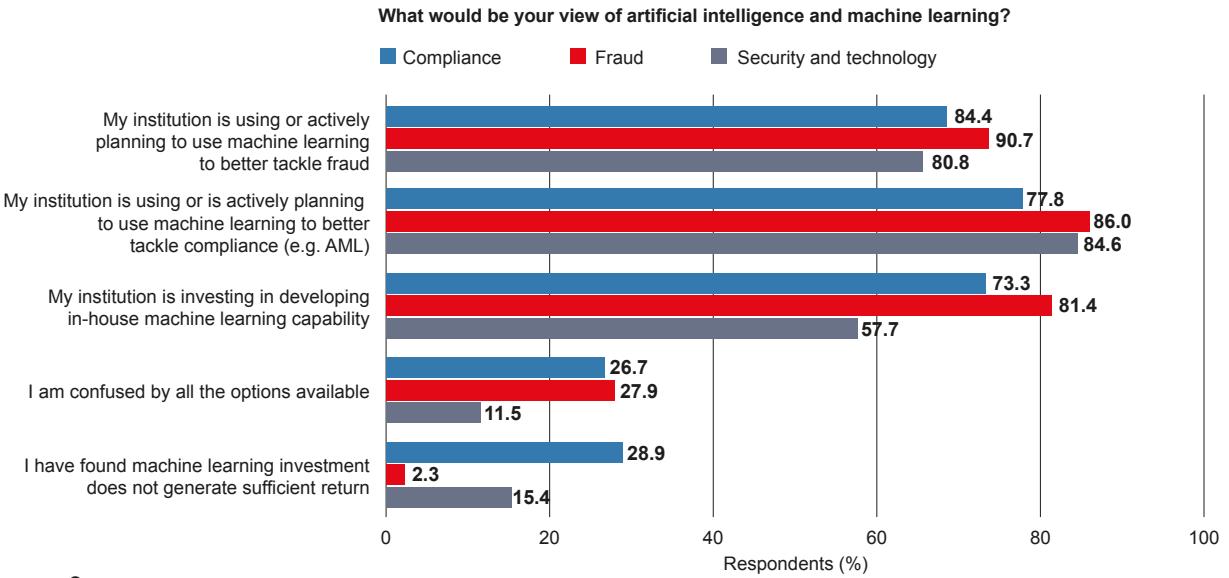


Source: Ovum

Banks increasingly turn to AI to tackle financial crime

One of the areas that has become mainstream in the search to drive more adaptability is the use of AI and machine learning (ML) technologies. Here the long-term goal is for detection capabilities to automatically learn, respond, and optimize to tackle evolving trends, with the use of AI techniques allowing new data sources (e.g., through natural language processing) and ML allowing models to be developed and optimized by platforms themselves.

Figure 13: Retail bank views on AI and ML



Source: Ovum

That said, AI as a broader concept is an area that has seen significant hype in recent years, leading to confusion in the market. Most vendors claim some level of AI capability, referring in fact to an array of different capabilities and analytical approaches. However, as shown in Figure 13, while some of this confusion is still present, particularly on the business side, understanding is generally high, with active interest in the use of AI and ML for tackling financial crime pervasive.

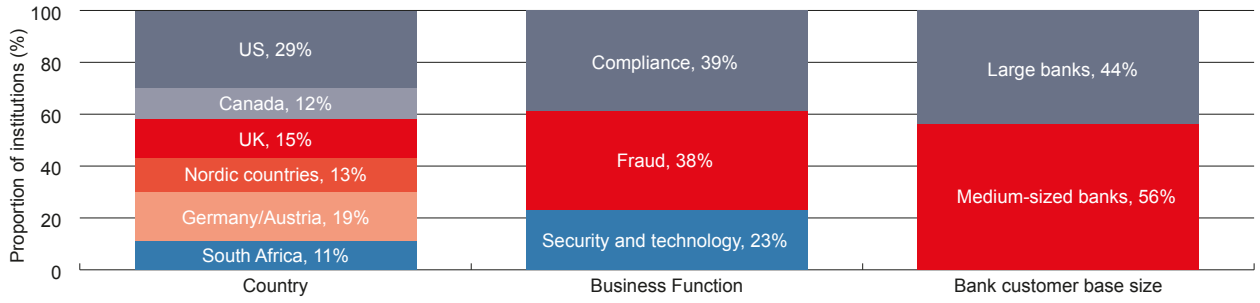
In many respects, fraud functions have been long-standing users of leading analytical approaches such as predictive analytics and ML, and for them to have an active interest in this area as it evolves is not too surprising. However, given that most AML compliance is rules-oriented, it is further evidence of the drive to seek synergies and share best practice that planned adoption of AI/ML is similarly high for AML. While there is some skepticism around the ability to generate a return on the compliance side, on the whole, institutions consider that this will be important for the future.

The main challenges here, particularly on the compliance side, are that "explainability" and responsible use are crucial. Regulators are reluctant to accept "black-box" approaches to compliance requirements, even if effectiveness is seemingly strong, particularly if this leads to undesirable outcomes.

Appendix

Methodology

Figure 14: Financial crime: composition of primary research interviewees



Note: n = 114

Source: Ovum

The primary research program involved interviews with 114 retail banks carried out over April and May 2019. Survey participants were screened to ensure that respondents were heads of their respective financial crime functions for either the fraud or AML compliance functions or heads of functions where respondents were directly involved in supporting the drive against financial crime, such as risk, compliance, security, or technology. This screening was based on job responsibility and job title. Participants were also screened to ensure their institution had significant retail banking business in their respective domestic market.

The composition of the study across various dimensions is shown in Figure 14. Compliance includes heads of financial crime compliance, as well as overall heads of compliance and risk functions where these have direct financial crime responsibilities. Note that bank-size tiering was based on size of retail banking customer base. Large banks are institutions with more than 5 million retail banking customers (in the domestic market). There was a minimum institution size for survey inclusion of 500,000 customers in large-population countries and 100,000 in small-population markets, while medium-sized banks were those with 100,000 or 500,000 (depending on population size) to 5 million customers.

How FICO helps

As you look to realize the benefits of moving your fraud and financial crime compliance departments closer together, we're here to help. We have built on our heritage of providing fraud and anti-money laundering solutions to offer both from a single platform. Falcon X is a cloud-based platform that allows you to manage fraud and financial crime with unified case management, machine learning analytics and flexible integration and orchestration of data. You can start using Falcon X to support one function or as a converged platform straight away.

FICO Falcon X for real-time payments

Falcon X enables you to design, simulate, and implement new fraud and financial crimes strategies. You can support all digital banking interactions across authentication, payments, and account maintenance. Falcon X gets you started by providing

- pre-mapped data integration for retail banking payments
- packaged real-time payments fraud rule set
- workflows including rules and machine learning orchestration.

Whether the threat comes via social engineering, phishing, or other sophisticated fraud techniques, Falcon X delivers the nano-profiling and historical context needed to protect against account takeover associated with P2P transfers, mobile payments, CH, and wires.

Falcon X for real-time AML

Around the globe, regulators are encouraging organizations to develop and embrace innovations that improve AML performance. FICO Falcon X provides a parallel path for next-generation and legacy technology to coexist. This allows you to complement your existing AML capabilities with

- complex variables and aggregations
- profiling of any entity, including beneficiaries
- machine learning models with explainable AI
- real-time screening and alerting
- unified alert and case management across fraud and compliance.

With Falcon X you can reduce the cost burden of unnecessary investigations by detecting suspicious behaviors for review, then automating manual tasks within a flexible, unified case manager.

OVUM CONSULTING

Ovum is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy.

Through our 150 analysts worldwide, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients to profit from new technologies and capitalize on evolving business models.

Ovum is part of Informa Tech, a B2B Information Services business serving the Technology, Media, and Telecommunications sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help your company identify future trends and opportunities, please contact us via

https://ovum.informa.com/contact/contact-us

consulting@ovum.com

https://www.linkedin.com/company/ovum/

www.twitter.com/Ovum