Publication date:
March 2021
Author:
Daniel Mayo

Fraud and AML compliance platform strategies

Assessing an integrated approach to AML compliance and fraud in the wake of the pandemic

In partnership with:
FICO

Brought to you by Informa Tech

Contents

Summary

In brief

The fight against financial crime (including both anti-money laundering [AML] compliance and fraud) very much continues in the wake of the pandemic. Regulators remain intent on enforcing AML compliance, and turbulent changes to society often present exploitation opportunities for financial criminals. With banks also forced to make dramatic changes to their operational practices with lockdown restrictions, the challenges for banks in meeting financial crime management objectives are as acute as ever.

To get a view on how COVID-19 has impacted both AML compliance and fraud strategies, Omdia conducted a study of 110 banks, interviewing senior executives from across compliance, fraud, and supporting security and technology functions. The study examined how institutions are responding to challenges in tackling both areas of financial crime in the wake of the pandemic—in particular assessing whether institutions need to take a more centralized intelligence approach across AML compliance and fraud—and whether new artificial intelligence and machine learning technologies offer genuine benefits in tackling financial crime.

Omdia view

The pandemic has exasperated the challenges banks have in tackling both AML compliance and fraud, impacting fraud volumes and catalyzing higher false positives as existing models struggle to adapt to changing customer behavior. Dealing with higher workload volumes has concurrently been impeded by the switch to remote working, with platforms across many banks not effective in supporting changing demands. That said, it hasn't changed the fundamental nature of tackling fraud and financial crime, with the ability to achieve, and importantly maintain, high detection levels in the face of changing threats the core requirement. Here institutions are looking to adopt a centralized intelligence approach to fraud and financial crime to improve detection and provide workload synergies. Institutions are also seeing benefits in meeting this from machine learning; the main challenge here is in ensuring current platforms can effectively support deployment of such models.

Key messages

- The pandemic has not just driven volume impact, but challenged control effectiveness and driven dramatic behavior changes, impeding the effectiveness of existing models.
- Some 69% of institutions now have strategic plans to integrate functions or share resources between AML compliance and fraud; 50% have plans to do so within three years.
- Artificial intelligence and machine learning technologies drive fuller and more complete detection, but also offer rapid adaption to new threats and false positive reduction.

COVID-19 has exasperated financial crime challenges around platform adaptability and staffing

The economic and social shock from the COVID-19 pandemic has been generational in magnitude, creating significant challenges for the banking sector. This is both in its external impact, on clients and the wider operating environment, as well as internally, on the impact on employees and ability to interact with customers. While government stimulus and furlough schemes have indirectly alleviated some of the short-term economic impact, authorities have not relaxed regulatory requirements on banks around tackling financial crime—around protecting customers from financial fraud and in ensuring banking systems are not used for illicit purposes (such as money laundering). The onus on banks to tackle financial crime is as acute as ever, but dramatically changing environments can often be a boon for financial criminals in facilitating new avenues of attack and impeding existing detection techniques.

To assess how strategies around both fraud and AML compliance have evolved in the wake of the pandemic, Omdia conducted a primary research study with 110 institutions in 4Q20 interviewing executives from both the fraud and compliance sides, as well as security and technology leaders directly involved in supporting these functions. The study explored priorities, challenges, and the impact of COVID across both financial crime functions, as well as effectiveness of current technology platforms in enabling resulting requirements. It also builds on previous research in this space conducted by Omdia in 2Q19, which looked at whether financial institutions are taking a more integrated approach to tackling fraud and AML compliance.

The study covered institutions across a selection of markets in Europe (Germany, Nordics, and the UK), as well as Brazil, and North America (U.S. and Canada), covering a mixture of large and medium-size financial institutions (based on customer base). Full study details are provided in the appendix. Given terminology usage can vary across regions, it should be noted the term “financial crime” in this report includes both fraud management and AML 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).

Protecting customer and the institution's reputation drive anti-financial crime functions, but ensuring effectiveness has created a major workload burden

Given the economic fallout from COVID-19 pandemic, some outside the compliance world may have assumed regulators would have cut banks some slack in 2020. In contrast, regulatory enforcement of AML compliance continued unabated with over $10bn in fines, a more than 25% increase on an already significant 2019 figure. While this high figure itself was heavily driven by the 1Malaysia Development Berhad scandal (which saw over $6.8bn in collective fines), regulatory bodies across the globe have continued to remain heavily focused on AML and sanction breaches, with substantial fines across both Europe and Asia Pacific in recent years (in addition to the historically dominant North America region in respect to fine magnitudes). With the FinCEN leak in September intensifying media and government focus on AML, this is likely to remain the case in 2021.

This has unsurprisingly kept compliance high up on the executive agenda regardless of the ongoing challenges from the pandemic. However, the threat of regulatory enforcement is only one driver for banks in tackling financial crime. Banks also wish to protect customers and themselves. The latter including reputational damage from being associated with enabling criminal activity as well as any direct financial losses.

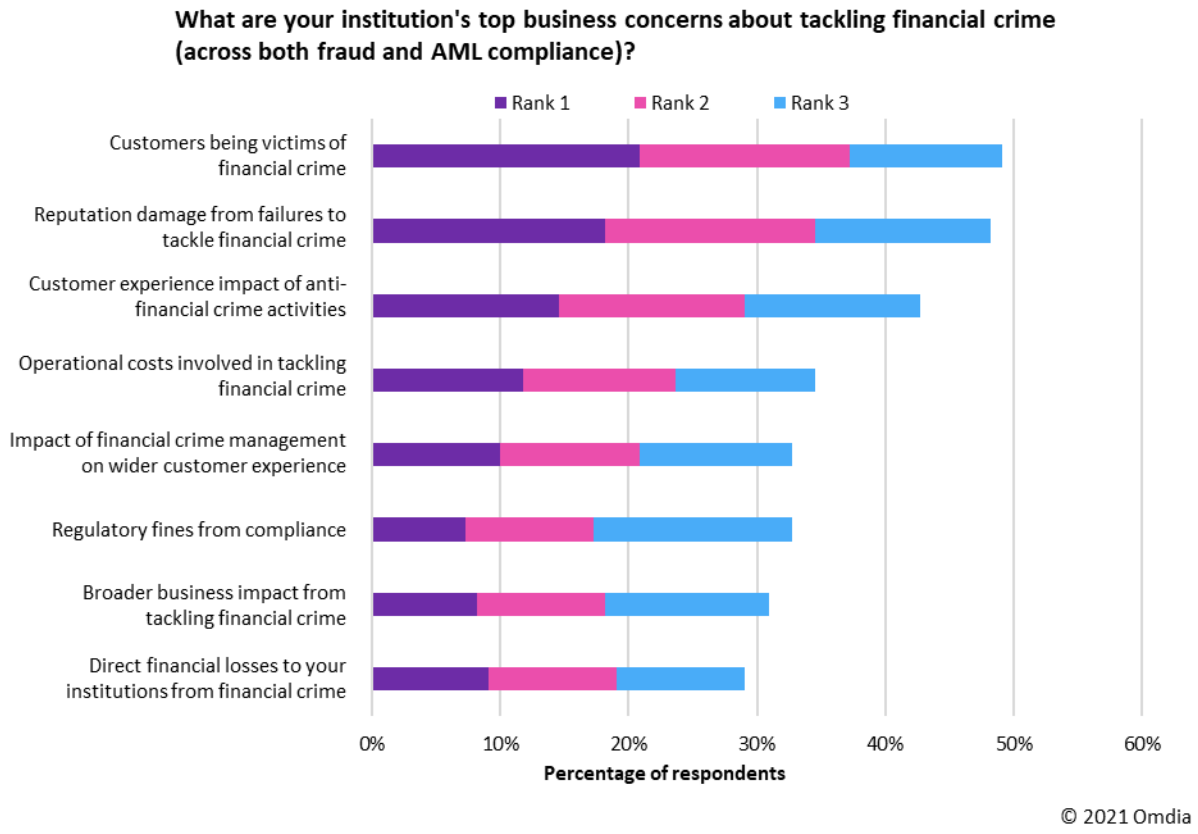
The challenge for most institutions is that while these drivers create an imperative to raise the effectiveness of financial crime detection and prevention (across both AML compliance and fraud), institutions simultaneously want to minimize the impact of this on legitimate user activity. Here banks want to provide a strong customer experience, in ensuring that any investigative activity around financial crime is resolved quickly and accurately, but also in limiting the impact of controls themselves in the customer experience (such as making ID checks easy and fast). Conversely, cost always remains a consideration, with operating costs associated with AML compliance and fraud management now a significant overhead for most banks.

The primary objectives for fraud and AML compliance lie in protecting the customer and institution while providing a strong customer experience; regulatory threats and direct losses are secondary concerns

The balance of these business concerns in tackling financial crime is illustrated in Figure 1. This shows responses from the study, asking executives to rank their top-three business concerns in tackling financial crime (across both AML compliance and fraud). Interestingly for most institutions, the threat of regulatory fines is largely a secondary, albeit still significant, concern. Rather the top priorities for most institutions concern protecting the customer as well as the bank's reputation, with reputation more important than any direct financial loss. Within this, fraud executives have a stronger relative focus on the customer protection, with compliance executives relatively focused on guarding the bank's reputation. However, both priorities were consistently ranked as top issues by executives across all functions.

The other priority for both fraud and compliance executives is in ensuring that their financial crime operations provide a strong customer experience. This is in relation to the direct operation within the executive's control, such as speed of investigations and resolution of any suspect fraud. While the compliance side doesn't directly liaise with the customer (suspect money laundering cases are sent to authorities rather than the potential money launder), providing a strong customer experience during know-your-customer (KYC) process is important. Financial crime executives are also interested in the wider impact of their activities on the customer experience and the broader business, but these are generally secondary concerns (like the threat of regulatory enforcement).

Figure 1: Top business concerns in tackling fraud and AML compliance



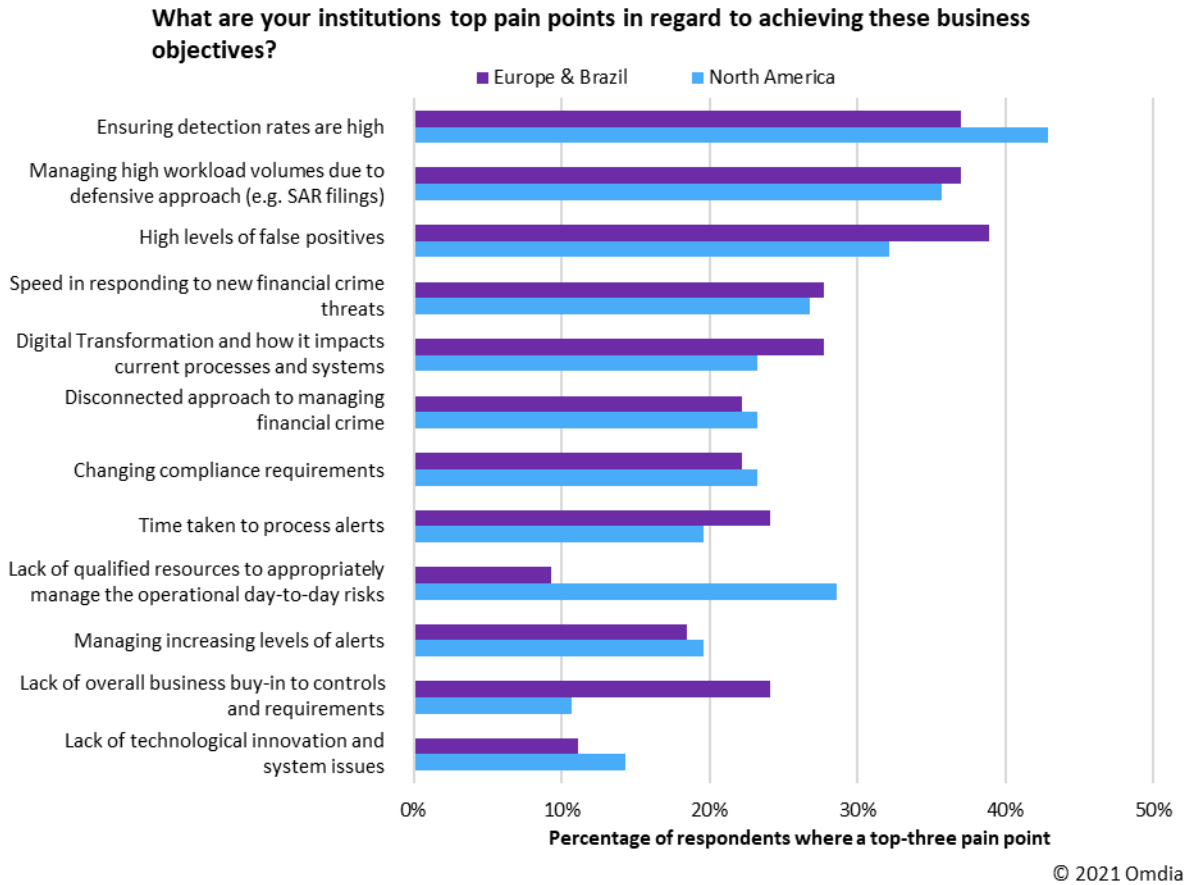
Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

These business concerns in tackling financial crime have remained constant in the wake of the pandemic. Omdia's previous fraud and AML compliance study in 2Q19 asked executives the same question with ranking responses then almost identical (aside from a switch in position of the last two options). While the pandemic has created additional challenges for institutions in tackling financial crime, it has not driven a shift in overall objectives.

Maintaining a high level of financial crime detection is the ongoing challenge, resulting in high levels of false positives and significant workload pressure

Figure 2 illustrates the top pain points institutions have in tackling financial crime (across both AML compliance and fraud) by region. Perhaps unsurprisingly, the most pervasive pain point across regions is the primary goal of financial crime management itself, that is ensuring that financial crime activity is detected. For most institutions ensuring that detection rates are, and importantly continues to be, high is an ongoing challenge. Financial crime activity on both the fraud and money laundering sides is increasingly driven by highly organized and quasi-professional players, who are active in seeking out weak links in any control systems as well as opportunistically responding to new situations (such as presented by pandemic). Tackling financial crime is an ongoing challenge with financial criminals shifting and evolving attacks as banks improve their capabilities. In this, banks need to ensure that detection rates are high and that they are quick in responding to new financial threats, so they remain so.

Figure 2: Top business pain points in tackling financial crime across fraud and AML compliance



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

The issue for most banks is the costs with ensuring high detection. With regulators across the globe continuing their focus on anti-money laundering, banks across all regions covered in the study are often taking a defensive posture to AML compliance, providing suspicious activity reports (SARs) even for relatively low-level suspicious activity. This has resulted in high workload volumes in terms of investigations and reporting caseloads. This approach is to a degree mirrored on the fraud side, with a focus on ensuring actual fraud detection rates are high resulting in a high level of false positives—activity assessed as potentially fraudulent that turns out to be legitimate. Here institutions are erring on the side of caution in flagging suspect fraud to ensure actual fraud is captured, but in doing so they also flag a high number of genuine transactions.

As Figure 2 shows, these pain points are common across regions, although the challenge of dealing with false positives is relatively acute in Europe (particularly in the UK and Germany), while ensuring high detection levels was more pervasive in the US, although this was also notably dominant in Brazil. Interestingly, the key region difference seems to be on the staffing side, with North American institutions (significant in both Canada and US) struggling with qualified staff availability—with staffing an issue that has very much been exasperated by COVID pandemic and its resulting impact on the workforce.

Pandemic has increased staffing challenges, driving higher fraud volumes and new behavior patterns

This high workload has translated into increased operational costs for banks in tackling financial crime. Executives were also asked how much their institution's overall operational expenditure on anti-financial crime activities (across both fraud and AML compliance) changed in 2020 compared to 2019. For over 70% of institutions, operational expenditure continued to increase in 2020, with over half of this seeing significant spend growth. This follows a period of sustained expenditure growth over the decade. The previous financial crime study in 2Q19 found that 77% of institutions had experienced expenditure growth since 2015.

The challenge for most is that this spend growth has taken place is an environment of overall cost management, with many banks actively looking to reduce their operating cost base. This has been exasperated by the pandemic, which has impeded both revenue and profitability, creating even an stronger imperative on institutions to tackle their operating costs.

Underlying challenges in tackling financial crime revolve around staffing, platform capabilities and general resource constraints, with the pandemic exasperating staff and platform challenges

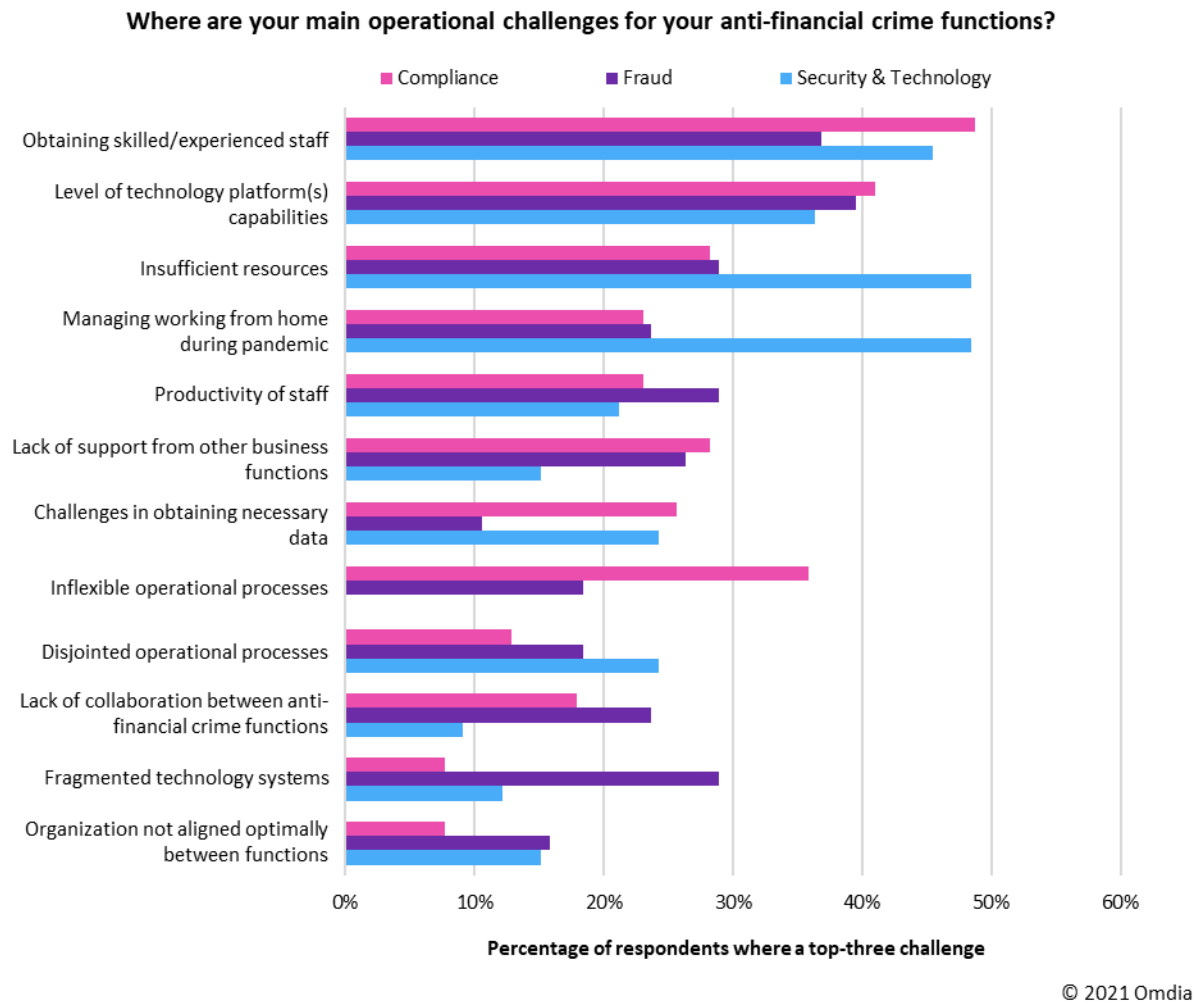
Despite this expenditure growth, the demands on AML compliance and fraud functions have been such that resource constraints are a significant operational issue, particularly for supporting security and technology functions which must balance demands across the wider business. This is illustrated in Figure 3 which shows the top operational challenges for institutions in tackling financial crime, segmented by responses and by executive function.

While resource constraints are a notable challenge, for compliance executives the top pain point is on the staffing side. The availability of skilled and experienced staff is a widespread challenge across

the sector, with executives in all markets aside from the Nordics identifying this as a pressing issue. Demand for financial crime staff has increased over the decade as workloads have grown; however, this has led to shortages in the workforce pool, particularly in the availability of experienced hands. Given well-publicized scandals and regulatory investigations in the last couple of years in the Nordic region, it is likely that this will become more pressing for Nordic institutions as well.

Staffing is also an issue for fraud executives; however, the top pain point here is the performance of technology platforms used to support financial crime functions. This is a consistent top issue across markets and one that is also identified strongly by the compliance and supporting security and technology executives.

Figure 3: Top operational challenges in tackling financial crime



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

This is driven by several factors:

- The underlying performance of technology platforms used to support both detection and investigations processes is found wanting by many executives. Platforms are often inflexible and require significant time to change, impeding the ability of functions to adapt to new/evolving financial crime threats.

- Many institutions use multiple systems across operational processes, often with low levels of integration. This hinders staff productivity at the individual workload level (with staff required to switch between systems within a process), but also in the ability to effectively share and optimize staffing across financial crime functions as whole.

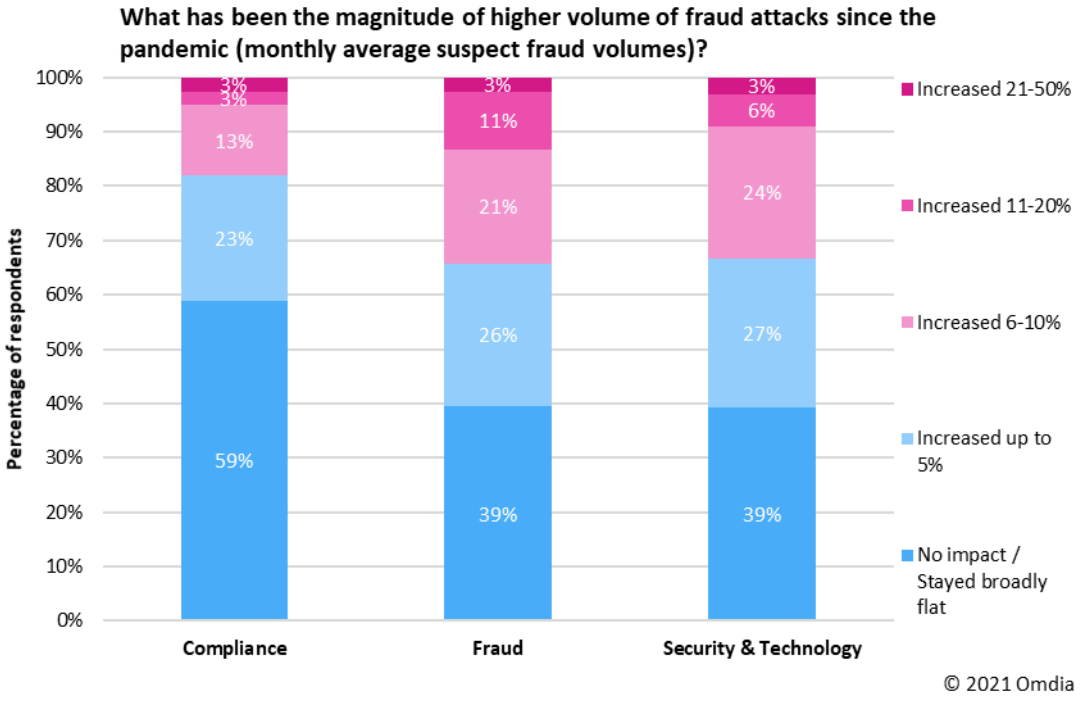
- Overall automation levels across wider operational processes are low, with staff often required to conduct low-level manual repetitive tasks (again lowering productivity levels).

Both staffing and technology platform pain points have been exasperated by the challenges of the pandemic, with the forced switch to home working in particular causing major headaches for financial crime functions. Identified strongly across North America, as well by institutions in Germany and the Nordics, the use of multiple systems as well as the ability of these platforms to facilitate home working models is creating significant issues. As shown in Figure 3, technology executives are particularly struggling here, with many institutions using on-premise platforms, rather than cloud-based ones that can easily be accessed across locations and devices.

Impact on pandemic on volumes has been felt stronger by fraud functions, with significant impact for over a third of institutions

The pandemic has also catalyzed a wider impact, driving growth in attacks volumes. Financial criminals often seek to take advantage of significant societal change, such as lockdown restrictions or rollout of COVID testing, with new practices and uncertainty around these often resulting in people being more vulnerable to fraud attempts. The impact of the pandemic on fraud attacks in illustrated in Figure 4, showing how monthly average suspect fraud volumes have evolved since the pandemic.

Figure 4: Impact of pandemic on financial crime activity volumes



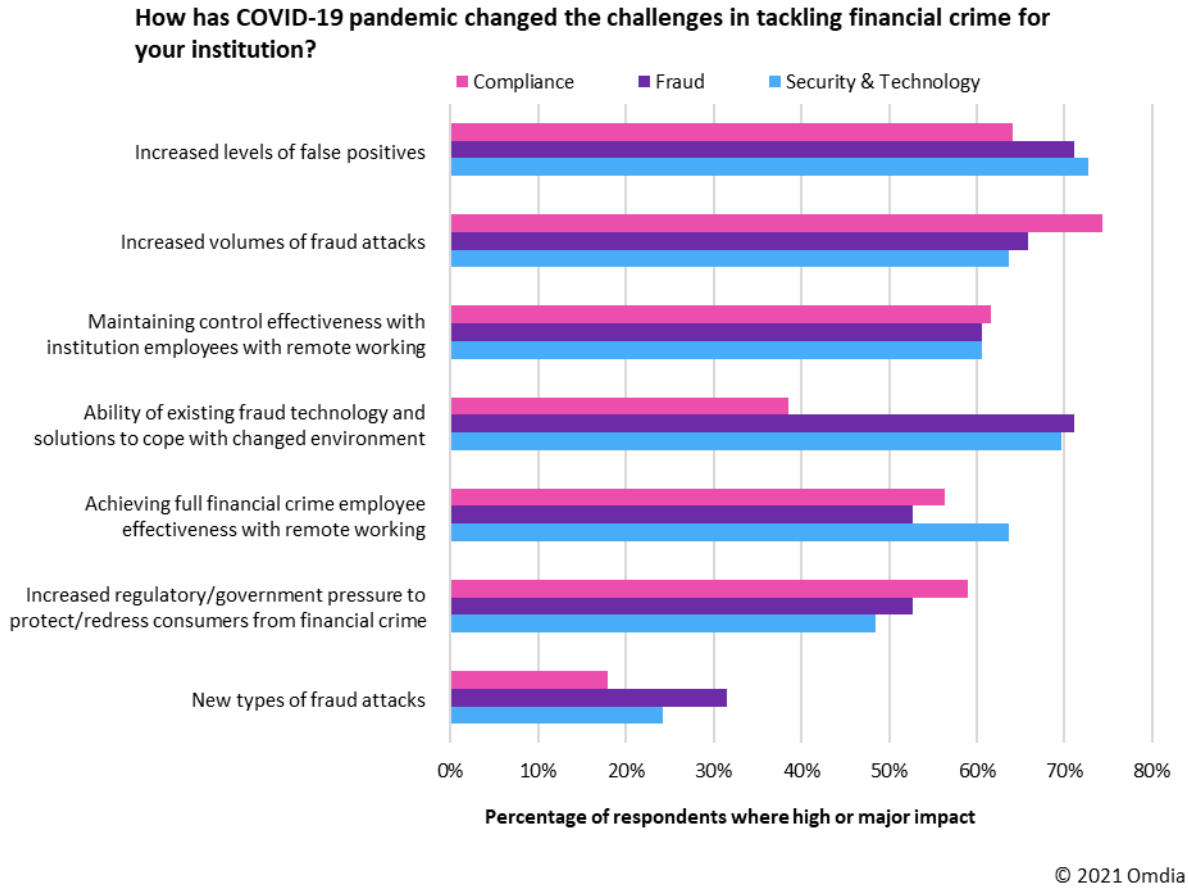
Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

The most impacted market appears to be Brazil, where more than two-thirds of institutions have seen some growth, and where over a quarter of institutions have seen a strong shift (10%+ growth). In contrast, over 70% of UK institutions have seen no notable change in fraud attacks since the pandemic. Interestingly, Figure 4 also shows that fraud attacks have been more prevalent from a fraud than compliance perspective, with a proportion of executives seeing significant growth, almost double for fraud executives compared to compliance ones. While the impact has not been spread evenly, the pandemic effect appears to be stronger on fraud over money laundering.

Pandemic has not just driven volume impact, but challenged control effectiveness and driven dramatic behavior changes, impeding the effectiveness of existing models

While the impact of the pandemic on fraud volumes in the sector is relatively concentrated, it has exacerbated wider challenges. Figure 5 illustrates where executives identified a high or major impact from COVID.

Figure 5: Impact of COVID-19 on financial crime challenges



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

As well as volume effects, COVID-19 has worsened the false positive issue for over two-thirds of institutions (69%). A key challenge for many institutions is that the significant change in consumer behavior from lockdowns (e.g., dramatic shift in shopping behavior from physical to online site or stockpiling in some markets) has often resulted in existing fraud rules and detection systems wrongly identifying legitimate behavior as suspected fraud, as changed actions appeared unusual compared to historic patterns. Thus, while fraud attack volume did not increase uniformly across the sector, most institutions ended up with a higher investigation burden regardless.

In addition to model effectiveness the other key impact has come from the enforced workforce shift to remote working. This has impeded overall employee effectiveness and created challenges in ensuring financial crime control effectiveness. As shown in Figure 5, this has been a common challenge across financial crime functions. Compounding all of this, governments and regulators have generally enhanced consumer protection demands since the pandemic, creating increased pressure on institutions to rapidly redress financial fraud (regardless of higher workload volumes and employee workforce challenges).

While the pandemic has created new opportunities for financial criminals, for most banks this has seemed to drive higher volumes of existing fraudulent attempts, rather a dramatic change to new types of fraud. Again, the impact of new fraud resulting from the pandemic seems to be stronger on the fraud over AML compliance side, with a third of fraud executives flagging as a strong pandemic impact compared to just over a sixth of compliance ones.

An integrated approach to AML compliance and fraud drives detection and operational benefits

The pandemic has exacerbated the ongoing challenges that financial crime functions across both the AML compliance and fraud sides are facing. Both functions are seeking to enhance detection effectiveness, while managing growing volumes, and being agile to evolving financial crime threats. This is against a backdrop of resource constraints, skilled-staff shortages, and platform-capability limitations. For many institutions, this has created fundamental question for banking: is the current approach sustainable? A potential remedy here, which Omdia also examined in its 2Q19 financial crime study, is whether institutions should seek to drive a "centralized intelligence" approach to financial crime bringing together AML compliance and fraud capabilities, with a single integrated platform and a collaborative and/or shared approach to workforce and data resources.

On this topic, the 4Q20 financial crime study further explored institution's approaches to integration, looking at current integration levels and whether future ambitions in this area have evolved in response to the pandemic.

Institutions have moved to actively collaborate across AML compliance and fraud, driven by cost and effectiveness benefits

At an organization 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.

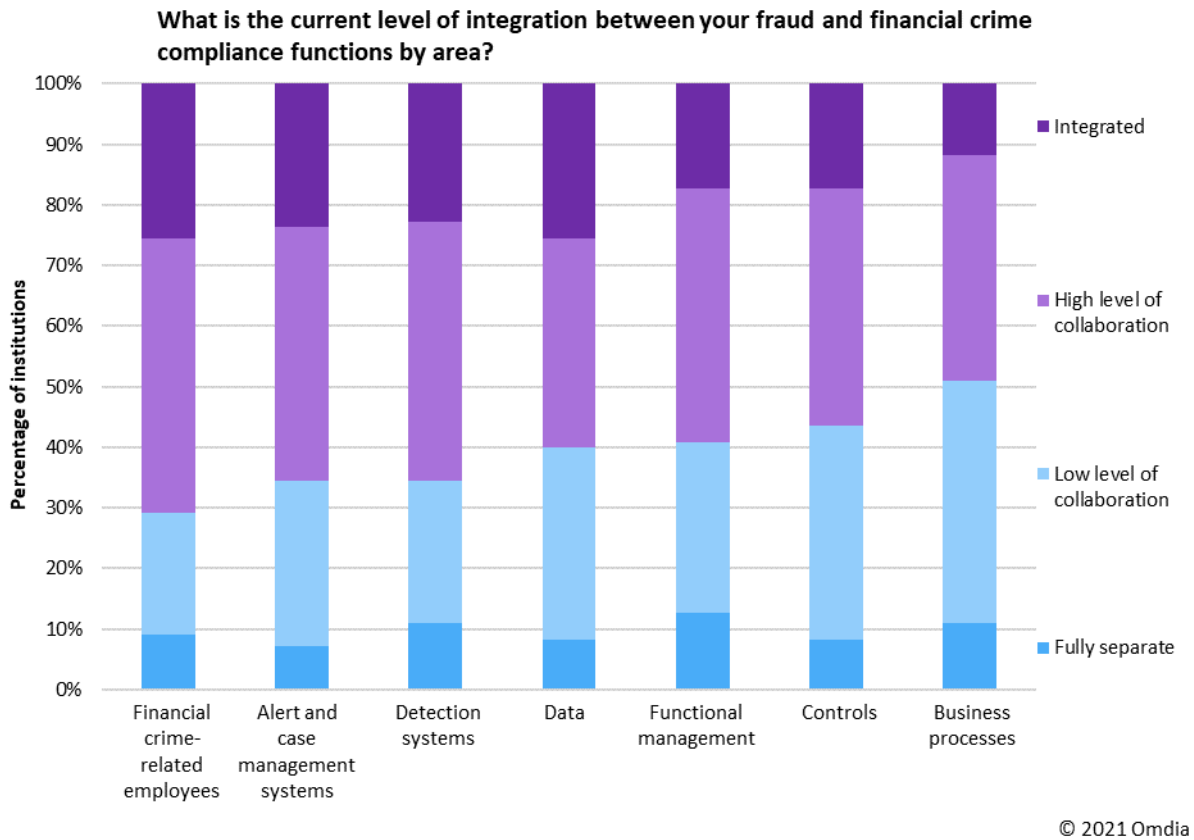
Conversely, one-third of banks do currently have fraud and financial crime reporting into the same business executive. This is largely an institution-specific decision, with limited differences between banks grouped across the different countries surveyed, except in North America, where there is a polarization in approach between Canada, where 45% have common reporting lines, and the US, where only 28% do. Scale doesn't appear to be a determining factor, with 33% of medium-sized

banks taking this approach compared to 35% of large-sized banks. The pandemic has unsurprisingly not driven any real change in reporting structures, with data here very much consistent with the pre-pandemic picture.

Collaboration between direct financial crime staff, technology systems, and data is already well established across AML compliance and fraud functions

Drilling down from executive reporting lines for the different financial crime functions, Figure 6 shows the current levels of integration between fraud and AML functions across people, business processes (such as investigations or customer onboarding), and technology (including data).

Figure 6: Current integration between fraud and AML compliance by area



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

Looking across these factors, integration is a minority strategy, with a fifth of institutions on average operating on an integrated basis. The most established area is with the financial crime workforce. While this is only adopted by a quarter of institutions this area has seen a small positive movement since the pandemic (moving from just a above a fifth of respondents in 2Q19). The proportion of institutions with single integrated technology systems (for case management or detection) as well as

using integrated data is at a similar level (22-25%), although this remains broadly in line with previous pre-pandemic levels.

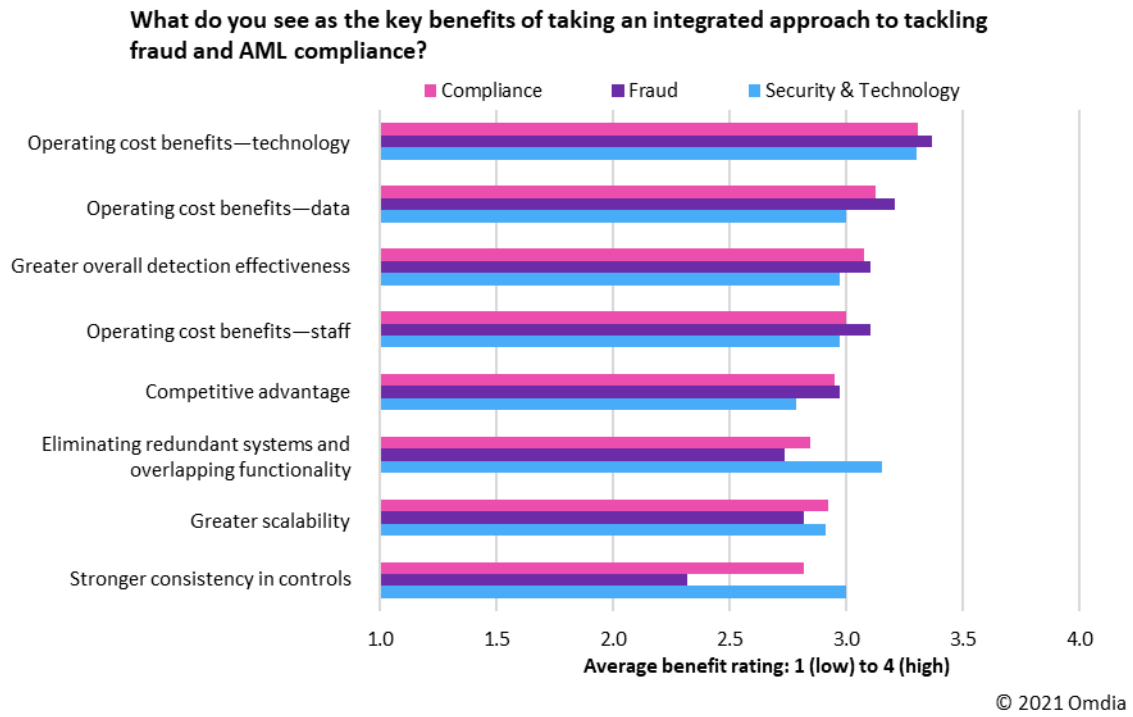
Rather the drive for most institutions to get synergies between AML compliance and fraud has been led by a focus on collaboration, with the broadest approach across all areas (outside of business processes) is that of seeking high levels of collaboration. Here the main change since the pandemic has been a small positive shift for both financial crime-related employees and technology platforms (across both alert and case management, and detection systems). The main area that has negative shift away from collaboration is with controls, perhaps reflecting the increased challenge in maintaining control effectiveness with home working during the pandemic.

Interestingly, there is no statistical differences in approach to integration or collaboration between financial crime functions and the executive reporting approach (i.e., whether fraud and AML compliance leaders report into the same overall business executive). This suggests that the drive for collaboration is being driven by bottom-up synergy benefits, rather than executive management imposing top-down demands led by cost savings.

Both fraud and AML compliance functions see integration benefits on both the cost and effectiveness side

On this point, Figure 7 shows where institutions have seen or expect to see the key benefits from taking an integrated approach to fraud and AML compliance.

Figure 7: Benefits of taking an integrated approach to fraud and AML compliance



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

Respondents were asked to rate the strength of benefits on a 1 to 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 over 3.0 suggests that it would be considered a significant benefit.

Accordingly, the key significant benefits from taking a centralized intelligence approach are driven by expected cost benefits. This is across technology, data, and staff benefits (average score was over 3.0 for all three), with technology executives also identifying significant benefit from reducing use of multiple systems. Importantly institutions also see a significant benefit in taking an integrated approach in driving greater overall detection effectiveness. Given this remains the primary challenge for institutions in tackling financial crime, this also suggests that the drive for collaboration and integration is driven by real bottom-up effectiveness synergies in addition to cost benefits.

Interestingly the average benefit rating by both compliance and fraud executives for competitive advantage is also very close to 3.0 benchmark, suggesting that many function executives also believe this can provide broader business advantage as well. Medium-sized institutions particularly saw this as the case. Similarly, most institutions expect some scalability benefits from bringing to AML compliance and fraud functions, although conversely this was rated more highly by large institutions (particularly by those in Canada and the UK).

In contrast, perspectives on whether integration provides benefits from consistently in controls is more mixed. Banks in Brazil, Canada, and the UK rated this below 2.5, with fraud executives perceiving weak benefits (average rating of 2.3). This has perhaps been aggravated by the challenges in maintaining control effectiveness since the pandemic, given the expected control synergy benefits by executives in the 2Q19 study was relatively strong (2.9 rating by fraud executives).

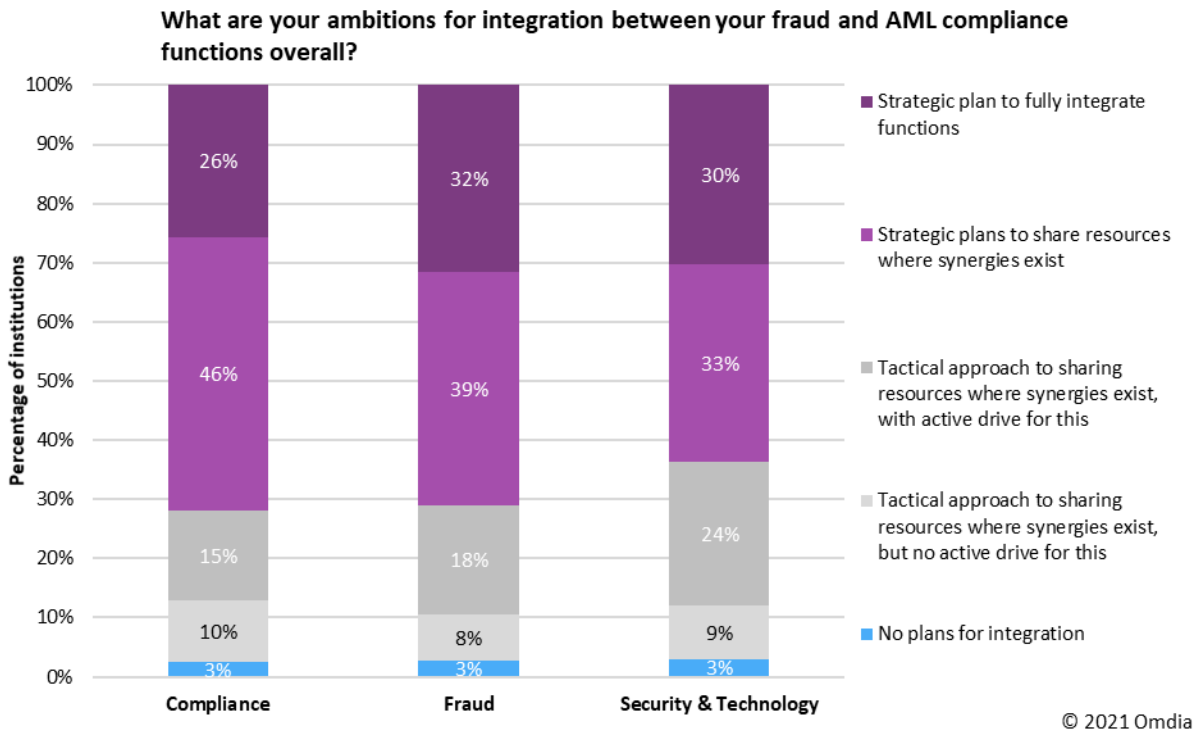
Institutions are widely taking a strategic approach to integration, with over half with active ambitions

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 over two-thirds of the sector taking a strategic rather than tactical approach to this, marking a small positive shift since the pandemic. Significantly, this strategic approach is translating into active plans, with institutions that are actively looking toward integration generally seeking to do so within three years. However, in contrast to positive impact on driving a more strategic approach to integration, the pandemic has had a small negative impact in pushing out timescales.

Some 69% of institutions now have strategic plans to integrate functions or share resources between AML compliance and fraud

Looking at long-term ambitions for integration between fraud and AML compliance, we see in Figure 8 the respective plans grouped by financial crime business function.

Figure 8: Ambitions for integration between fraud and AML compliance



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

Some 69% banks have strategic plans for further integration, either to fully integrate functions or to share resources where synergies exist, with a further 19% actively seeking to obtain synergies even if they are only taking a tactical approach. Ambitions have seen a small positive shift towards strategic approaches compared to pre-pandemic plans, led by compliance executives (shifting from 62% to 72%) while ambition perspectives on the fraud side remained unchanged. Interestingly, relative ambitions between functions are now very much in line now, whereas before the pandemic integration ambitions were strongest on the fraud side.

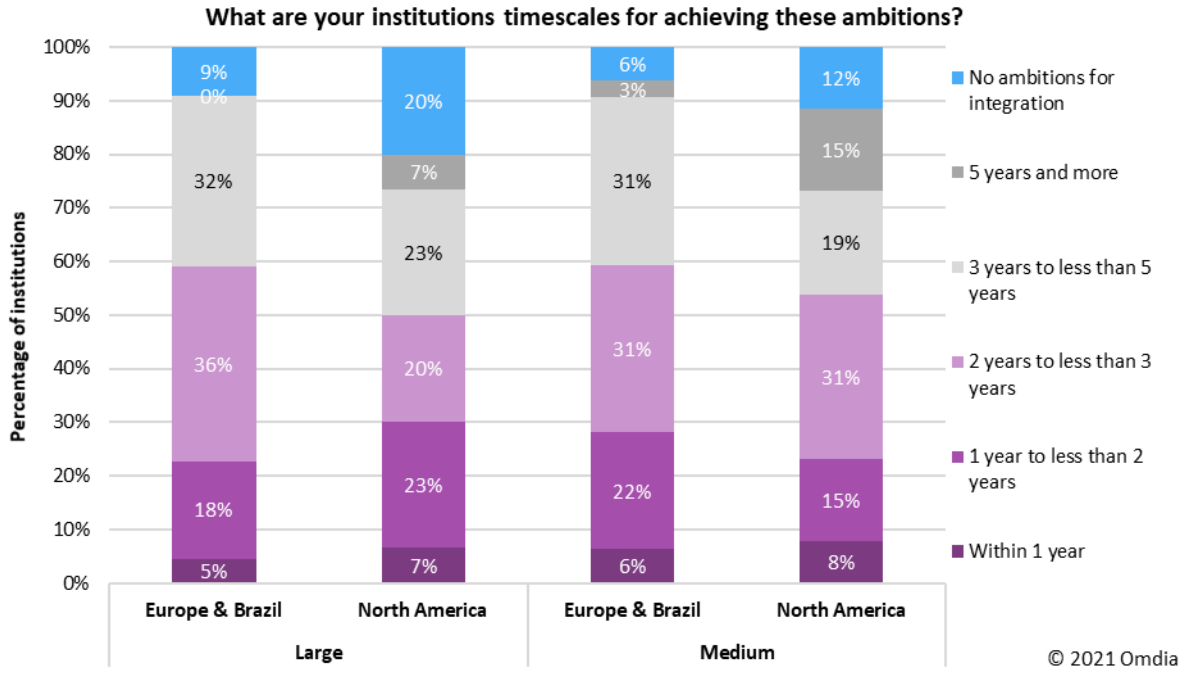
There has also been a shift within the “strategic” options with plans to fully integrate functions increasing from 24% to 29% average overall. Here there was notable growth in ambitions from both compliance and fraud executives, while in contrast security and technology executives have shifted towards sharing resource where synergies exist over integration.

At a regional level, the North American market is more polarized in approach. There is a larger segment than for Europe and Brazil looking to fully integrate functions (40% compared to 23%), but conversely 37% have tactical or no ambitions for integration (compared to just 14% for these segments in Europe and Brazil). Ambitions across Europe and Brazil are more consistent, with the majority taking a strategic approach to share resources where synergies exist.

Across both regions and tiers, at least 50% of institutions have plans for integration within three years

Given ambition is not necessarily a full proxy for action, Figure 9 looks at the time scales institutions are operating on for achieving these ambitions by tier and by region grouping.

Figure 9: Timescales for fraud and AML compliance integration



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

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 are actively pursuing synergies between financial crime functions. Excluding those that have no ambitions for integration (the pink segment shown in Figure 9), just under 63% of those that have active plans seek to implement them within three years. This represents over half of the overall sector (55%). This has decreased compared to the pre-pandemic plans, with 70% of those with active plans seeking to implement within three years (representing 60% of the overall sector). While the proportion with no ambitions has fallen slightly over the period, the pandemic has extended integration timeframes out.

Again, the North American region is relatively polarized, particularly in planned timescales for large-sized institutions. This segment has the highest proportion of institutions across regions and tiers looking to integrate within the next two years but is also the segment with highest proportion with either no plans or plans beyond the three-year horizon. Within the Europe and Brazil region grouping, Brazil is most active market, with 85% of institutions planning to enact integration within three years—the UK was also high (64%). In contrast, only 38% of Nordics institutions had active plans, with 46% of institutions rather planning this within the three- to five-year timescale.

Existing platforms have focused on detection effectiveness, but struggle to adapt and leverage new technologies

The strength of supporting technology platforms is a major determiner in an institution's overall effectiveness in tackling financial crime. Platform performance is one of the top operational challenges for the sector, with platforms critical in detecting suspect financial crime (be it fraud or anti-money laundering), in driving the productivity of workforces in managing alerts and investigations, and in delivery strong outcomes (for the customer or enforcement bodies).

To assess current platform effectiveness, Omdia's Fraud and AML Compliance study asked executives to evaluate the strength of their existing platforms in supporting current and future regulatory, business, and operational outcomes. It also explored this from a technology perspective, looking at whether existing platforms are able to effectively utilize advances in areas such as artificial intelligence and machine learning to develop their future capabilities.

Institutions are looking to improve detection and adaptability, but completeness has often come at expense of agility with existing platforms

Looking at future priorities for financial crime executives, there are two primary objectives. The first is in achieving more complete detection. The second is to be able to adapt rapidly to emerging threats, which is relatively elevated compared to current concerns. Key secondary objectives lie in reducing false positive levels and improving operational effectiveness.

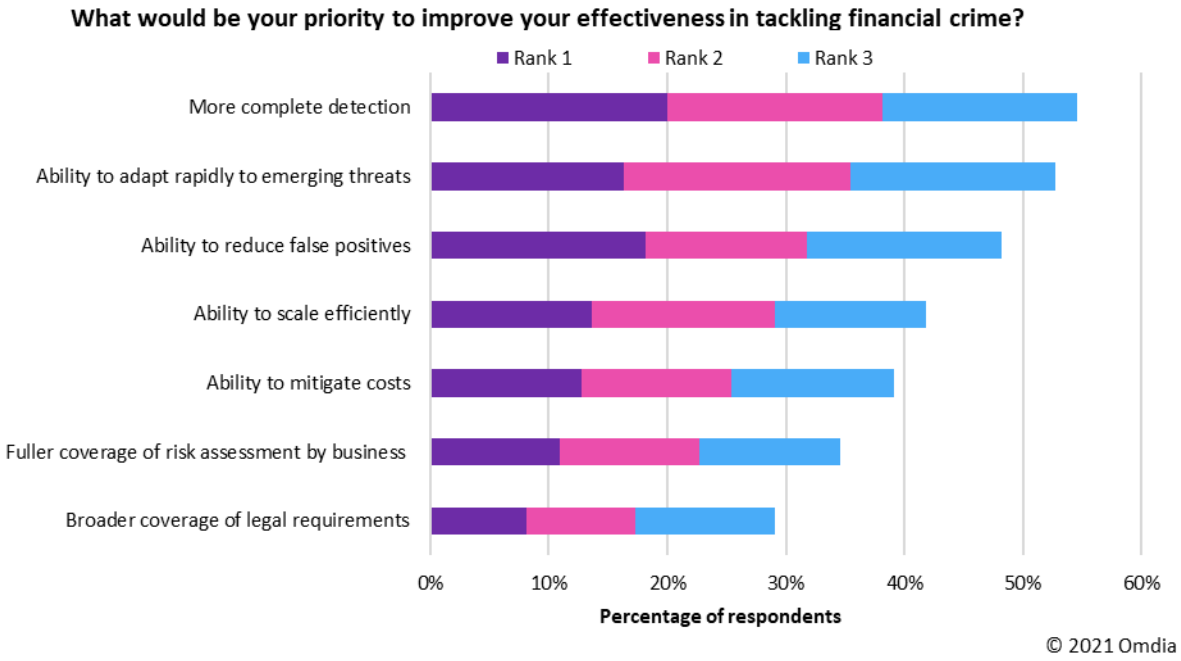
Assessing platform effectiveness in enabling these objectives, just under 70% of executives believe their platforms are good or excellent in ensuring detection completeness and detecting financial crime. However, only half consider their platform effective in being able to identify emerging financial crime threats. An even lower proportion consider their platforms effective in enabling fast investigations or supporting operational changes (such as working from home). The significant investment in financial crime functions in recent years has largely enabled institutions to meet the

primary regulatory objective of detecting financial crime, but for many this has come at the expense of platform agility and its ability to support scalable productivity.

Ensuring detection completeness is top of future priorities, but closely balanced with desire for adaptability, ability to reduce false positives, and ability to achieve scalability

Figure 10 shows a ranking of executive priorities for improving effectiveness in tackling financial crime, illustrating the allocation of the top three ranked priorities from across all business functions.

Figure 10: Priorities for improving effectiveness in tackling financial crime



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

Future priorities are largely in line with current ones with detection completeness, reduction of false positives, and scalability identified strongly (akin to current concerns highlighted in Figure 2). The main difference is in the ability to adapt rapidly to emerging threats, which is positioned close to detection completeness as the top priority.

While ensuring more complete detection levels of existing threats is of course important, given the dynamic nature of the financial crime, this is of limited value over time if institutions don't adapt, as criminals will change strategies to exploit new weaknesses. As a consequence, both completeness and adaptability were identified as the top improvement priorities by executives on the AML compliance and fraud sides (with negligible differences between functions).

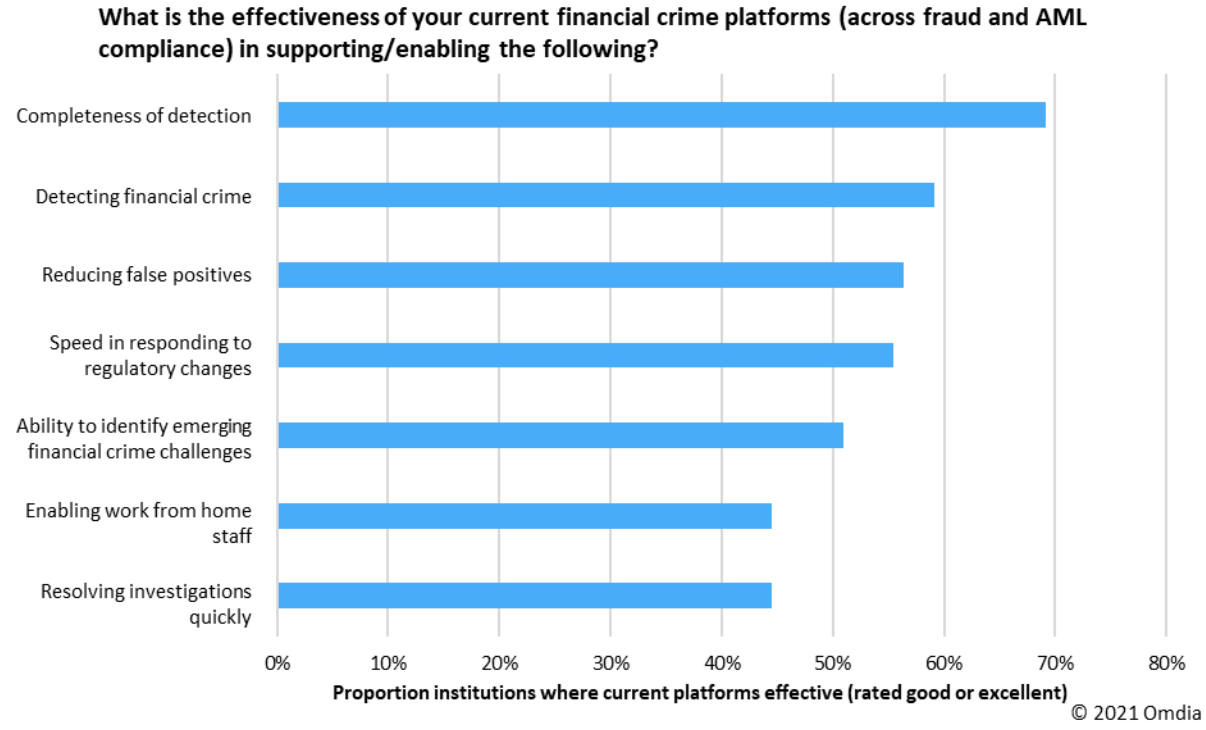
This ranking picture is also similar across regions, although institutions in Europe & Brazil allocated the top ranking to the ability to adapt to emerging threats, led by firms in the Nordics, the UK and Brazil. Rather regional differences occur in relative secondary improvement priorities, with cost

mitigation relatively important in Europe compared to North America (driven by institutions in the Nordics and UK).

Many financial crime platforms have focused on detecting financial crime, but are weaker in accuracy, their ability to adapt quickly, and enabling fast resolution

The effectiveness of current platforms (across fraud and AML compliance) in supporting financial crime across a number of dimensions is illustrated in Figure 11. For this set of questions, respondents were asked to rate effectiveness of their existing platforms on a 1 to 5 scale, with 4 being good and 5 excellent. The chart shows the proportion of institutions where current platforms are considered at least good in supporting that area, indicating that executive do consider their platforms effective in meeting requirements.

Figure 11: Effectiveness of current financial crime platforms



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

Over two-thirds of institutions (69%) do consider their current platforms effective in completeness of detection, with Canadian and UK institutions particularly confident in their platform capabilities (85% rating their platforms good or excellent). Compliance executives rate slightly higher than their fraud counterparts (74% versus 68%), although detection completeness is perceived as a strong suit for current platforms relative to other dimensions capabilities by all business functions. Similarly, the effectiveness of existing platforms in detecting financial crime is also relatively high. Here 63% and 62% of fraud and AML executives respectively rate their platforms as effective, with security and

technology executives having lower confidence (which brings down overall average shown in Figure 11). Given detection is a primary objective across financial crime functions, and the significant mandatory investment that has occurred in the sector over the last decade, this broadly pervasive strong performance is not that surprising; although conversely over 30% of institutions still have platforms that are not that effective.

However, other aspects of financial crime management are not as strongly supported by many platforms. The ability of these platforms to effectively support regulatory change and identify emerging threats is less widespread. This is particularly the case on the compliance side where half of compliance executives assess their platforms as effective in supporting regulatory change and only 41% see their platforms as good or excellent in tracking new challenges.

The performance of these platforms is even worse in supporting key operational demands, with most institutions having ineffective platforms for enabling fast investigations (with use of multiple systems likely a strong contributing factor). Mirroring challenges with home working seen in Figures 3 and 5, current platforms have not been effective in meeting this challenge for 45% of institutions, with the fraud side seeing particularly challenges here (less than a third rated their platforms effective).

It appears that for many institutions, investment in platforms over recent years has enabled them to support primary financial crime objectives, but this has come at expense of agility and broader operational effectiveness. In the medium- to long-term this is likely to drive both a regulatory and competitive advantage for institutions that have platforms that are effective across all dimensions, as well as in short-term benefits in dealing with the immediate shock from the pandemic.

Artificial intelligence has strong potential to drive financial crime goals, but existing platforms struggle to harness effectively

One of the most exciting areas of technology innovation in recent years has been development of artificial intelligence (AI), as well as maturing of machine learning (ML) to implement this within a commercial setting. This includes developments in natural language processing (NLP) and computer vision, which enables institutions to make use of wider data sources, as well as analytical techniques through machine learning or machine reasoning, that can help identify light or hidden signals for financial crime or automated optimization of detection models. Importantly, recent advances have improved the ability to provide decision outcome “explainability,” addressing the “black-box” challenge of ML approaches which has been an issue for regulatory support.

As a result, the previous Omdia Fraud and AML compliance study in 2Q19 found that there was a widespread interest from both the compliance and fraud sides in using such technologies in tackling financial crime, with well over 80% of institutions either using or actively planning to use new techniques. The innovation maturity curve in this respect has generally moved from the innovator/early adopter phases to early maturity.

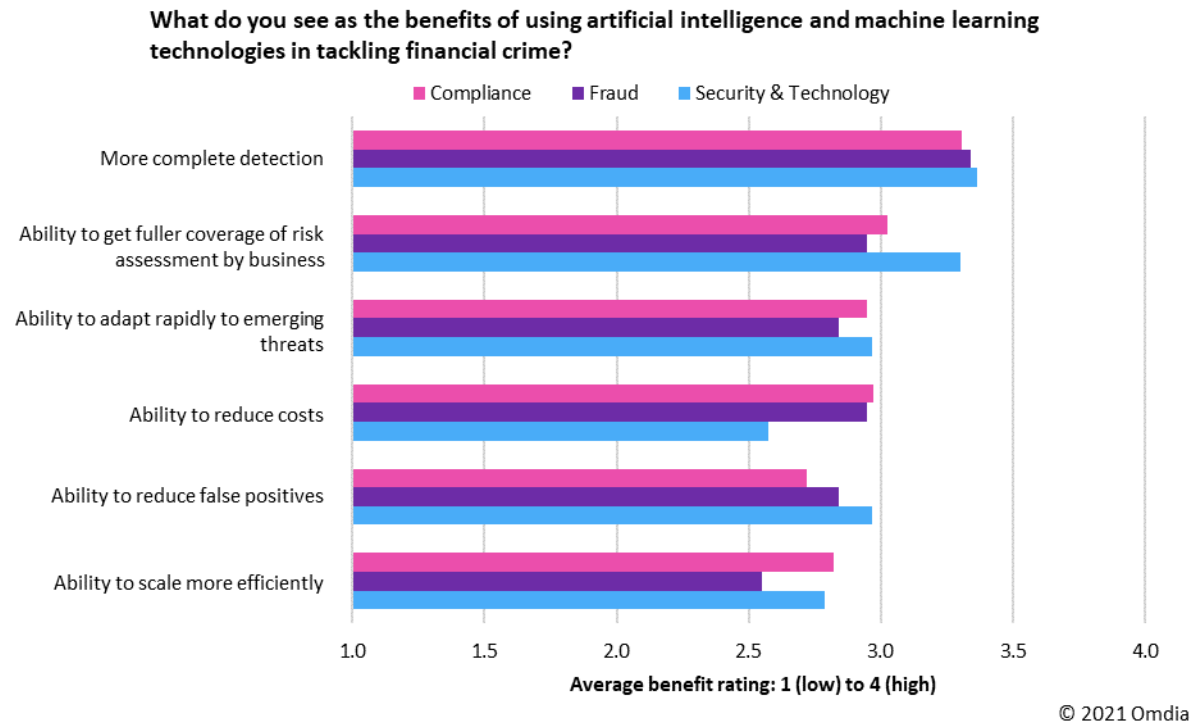
Reflecting this, the current study focused on assessing the benefits of using such technologies. Here artificial intelligence and machine learning are providing benefits in driving fuller and more complete detection coverage, but also in allowing institutions to rapidly respond to emerging threats. This aligns well with the future priorities for improving tackling financial crime (as shown in Figure 10).

The challenge for institutions is that many of the technology platforms of today are not strong in supporting these new approaches. Particularly weak is the ability to design and deploy machine learning models built in-house, with just over a third of institutions having platforms that effectively support this.

Artificial intelligence and machine learning technologies drive fuller and more complete detection, but also offer rapid adaption to new threats and false positive reduction

The benefits seen from using artificial intelligence and machine learning in tackling financial crime are shown in Figure 12. Executives were asked to rate benefit on a 1 to 4 rating, with 4 being a high benefit. A rating of over 2.5 suggests that institutions see the area as a benefit, whereas an average over 3.0 suggests that it would be considered a significant benefit.

Figure 12: Benefits of artificial intelligence and machine learning in tackling financial crime



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

A clear take-away from Figure 12 is that more complete detection is seen as a significant benefit by all financial crime functions. AI and ML extends the ability for institutions to collate and harness far wider data sets, as well as allow institutions to detect patterns and relationships that may be hidden

with more traditional approaches. This appears to allow institutions to obtain more complete detection, with 82% of institutions rating this with a 3 or 4 score. Alongside this, it appears that institutions have also benefited from AI and ML in the ability to get fuller coverage of risk assessment by business, which got an average benefit rating of 3.1.

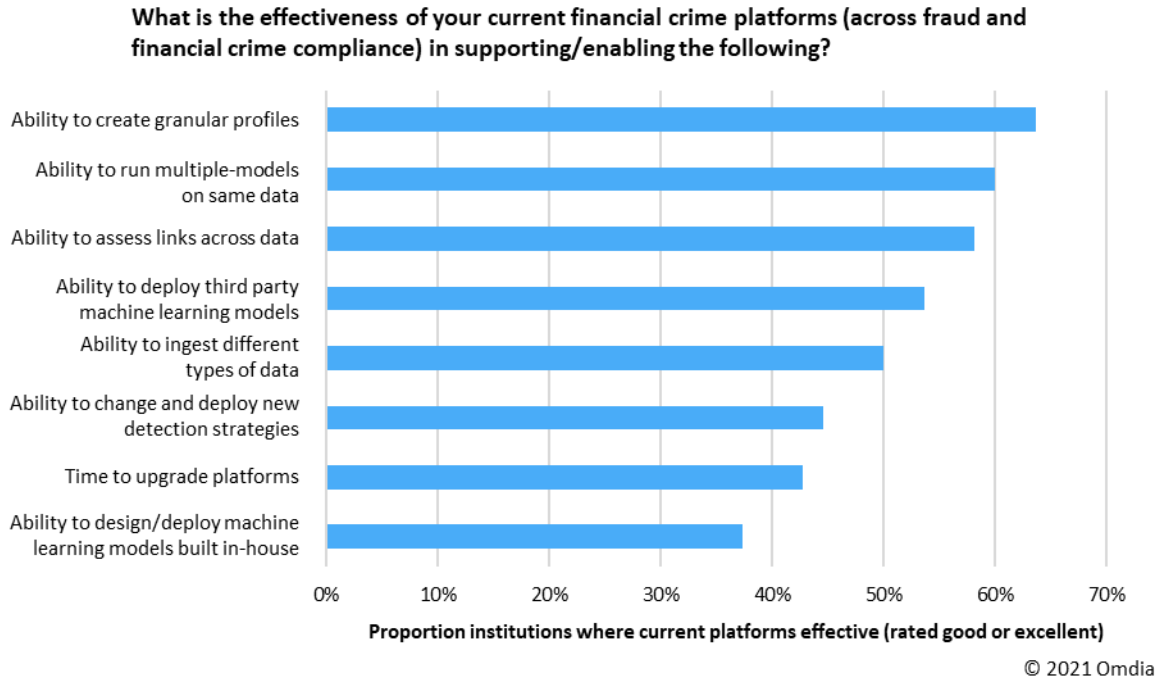
Interestingly, in addition to detection and coverage benefits, executives also see fairly strong benefits from AI and ML in the ability to adapt to emerging threats, cost reduction, and reduction of false positives, with average ratings of 2.92 for adaptability and 2.85 for the latter two close to the 3.0 benchmark. Cost reduction benefits were seen more stronger by fraud and compliance executives, in contrast to technology executives, suggest it is providing operational cost benefits, albeit driving higher costs on the technology side.

Regionally, institutions rate benefits very much in line with each other, with the main difference in benefits seen by tier. Larger institutions see stronger benefits from artificial intelligence and machine learning overall, led by high ratings for more complete detection and fuller coverage of risks, but also in the ability to reduce false positives and adapt rapidly (all average benefits ratings here for large institutions were above 3.0).

Existing platforms are generally strong in creating granular profiles and leveraging data across models, but struggle to incorporate and support machine learning

While AI and ML appear to be showing strong promise, the challenge for most institutions is that existing platforms are often not very effective in supporting this. Figure 13 looks at the effectiveness of current platforms in supporting financial crime management across a number of technology and data-related dimensions. As with Figure 11, institutions were asked to rate effectiveness of their existing platforms on a 1 to 5 scale, with 4 being good and 5 excellent. The chart shows the proportion of institutions where current platforms are considered at least good in supporting that area, indicating that executive do consider their platforms effective in meeting requirements.

Figure 13: Effectiveness of current financial crime platforms



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

As Figure 13 shows, platforms are widely effective in many aspects, with institutions generally able to support use and creation of granular profiles, as well in the ability to collate and run multiple models on the same data, (although security and technology executives gave much weaker assessments here. Similarly, the ability to assess links across data is generally strong, although interestingly rated significantly weaker by fraud executives in contrast to high ratings from the compliance side.

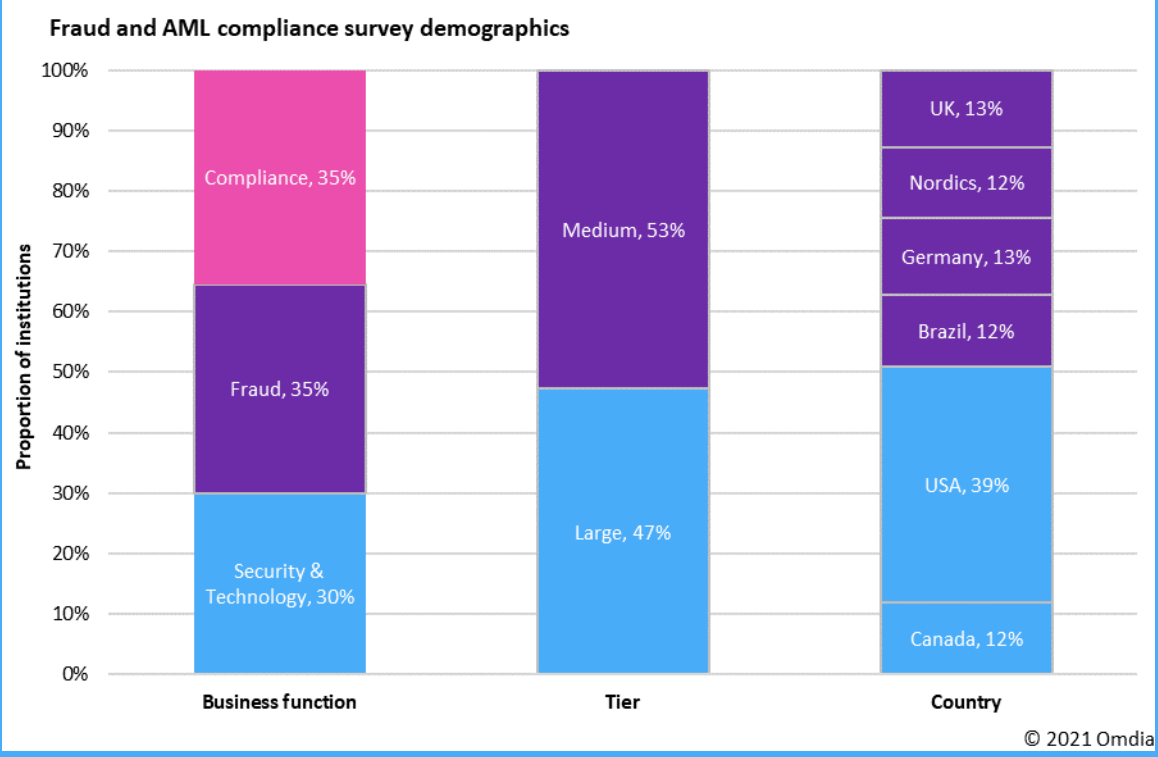
Where platforms seem to be generally weak from a technology perspective is in their adaptability, both in deploying new or change strategies and time requirements for upgrades, and in supporting machine learning. The ability to deploy third party ML models is stronger, likely driven by third-party vendors being better able to deploy their platforms, however, the ability to support in-house development and deployment of ML models is particularly weak. This was rated weakest by fraud executives, with only 29% rating their platforms as good or excellent in this respective.

Given that AI and ML is producing significant benefits for institutions in tackling financial crime from a detection and adaptability perspective, as well as operational benefits in cost reduction and reducing false positives, this platform gap is likely to be increasing problematic for institutions unless addressed.

Appendix

Methodology

The primary research program involved interviews with 110 retail banks carried out over Novemebr and December 2020. 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.



Source: Omdia Fraud and AML Compliance Banking Survey 4Q20

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-sized 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, with medium-sized banks including banks with customer bases from this respective minimum to 5 million.

Author

Daniel Mayo
Chief Analyst, Financial Services Technology
daniel.mayo@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia 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 global base of analysts, 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 profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms 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, Omdia's consulting team may be able to help your company identify future trends and opportunities.

How FICO Helps

FICO® Falcon® X helps you take an integrated approach to fraud and AML compliance leveraging centralized intelligence. FICO Falcon X helps you strengthen customer loyalty with a unified fraud and financial crime prevention environment that puts you in control. It's designed to deliver more efficient operations by utilizing:

- Unified Operations: Design fraud and compliance strategies in a single environment with centralized case management across all investigations
- X-Dimensional Profiling: Deliver nano-profiling and historical context across all dimensions of behavior with real-time aggregations and variable calculations
- Open Machine Learning: Deploy proven FICO models, in-house models, and third-party models. FICO® Falcon® X supports transparency throughout the machine learning lifecycle
- Data Freedom: Ingest, wrangle, and blend any data, from any source, and deliver it to any fraud or compliance workflow for real-time financial crime detection

Thousands of institutions around the globe rely on FICO to help detect fraud and financial crimes. With FICO Falcon X you can benefit from this deep domain knowledge and proven AI expertise within a new, extensible architecture. This allows you to author and manage a wide range of machine learning models, simulate outcomes, and measure results while maintaining the radical flexibility needed to delight consumers, today and in the future. This versatile engine helps you power incredibly accurate and effective strategies, so you can support all banking interactions, stop crimes faster, and solidify banking relationships.

Copyright notice and disclaimer

without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.