NICE ACTIMIZE

Report

AML Tech Barometer: Perspectives from Asia

Regulation Asia

Executive Summary

Although definitive statistics on the true value of financial crime have not been possible to date, it is clear that criminals are generating more illicit funds than at any other time in history. Recent estimates have been as high as 6.7 percent of global GDP. Yet, only a fraction of this activity is actually detected and recovered.

Financial institutions have been working to enhance their ability to detect and prevent financial crime, seeking to strike a balance between efficiency and effectiveness. In research conducted in collaboration with NICE Actimize, *Regulation Asia* explored how APAC financial institutions are progressing with these enhancements, leveraging survey data and interviews with regulators and practitioners.

This publication – the **AML Tech Barometer** – presents the research findings, shedding light on the current levels of technology adoption in financial crime risk management functions in APAC. The research found that financial institutions have been prioritising work in areas where the appetite for risk is low, such as KYC, customer due diligence, screening, and transaction monitoring.

From a technology perspective, respondents described name screening and transaction monitoring in particular as the "lowest-hanging fruit" when it comes to the adoption of artificial intelligence and machine learning-based approaches. In this regard, the ability to create, deploy and adjust rules and thresholds was highlighted as a key factor in the use of technology, particularly as a mechanism to address high false positives.

The research also highlighted the lack of beneficial ownership transparency as a consistent pain point across all types of institutions, in all jurisdictions, and regardless of the operational focus of respondents. However, respondents were encouraged by the work the Financial Action Task Force (FATF) is doing in this area, as well as in areas such as environmental crime, illegal wildlife trade and proliferation financing.

A key finding of the research was that global, regional and local financial institutions alike are increasingly willing to invest in technology to bolster their AML capabilities. Some institutions are undergoing complex transformation programmes or overhauling entire technology stacks, while others are targeting their investments in specific risk areas. Most respondents expect these trends to continue in 2022 and beyond.

The report includes insights from the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Hong Kong Monetary Authority (HKMA), the Monetary Authority of Singapore (MAS), and participating financial industry practitioners.

Contents

Introduction

The most recent global estimate of total illicit financial flows was published in June 2020 by Financial Crime News, leveraging information from international agencies, governments, non-governmental bodies, law enforcement, and other experts. The report valued the business of financial crime at USD 5.8 trillion for 2018, or 6.7 percent of global GDP. This was nearly three times the USD 2.1 trillion figure estimated for 2009 (3.6 percent of GDP), as published by the UN Office on Drugs and Crime (UNODC) in October 2011.

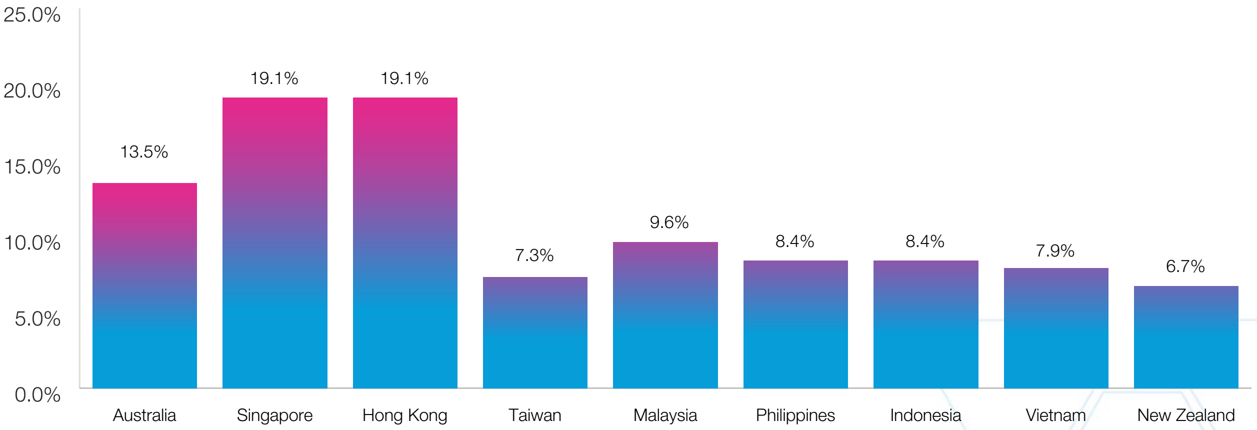
Prior to the UNODC report, the most widely quoted estimate of global money laundering was 2-5 percent of global GDP, a ‘consensus range’ that dates back to an International Monetary Fund (IMF) working paper published in 1996. While definitive statistics on the true value of financial crime have not been possible to date, it is clear that criminals are generating more illicit funds than at any other time in history. Yet, only a fraction of this activity is actually detected and recovered.

Amid the global pandemic, new financial crime typologies emerged as bad actors rapidly adapted to the new environment. From trade-based money laundering (TBML) involving medical goods, to new digital forms of money muling, criminals have continued to demonstrate an ability to innovate.

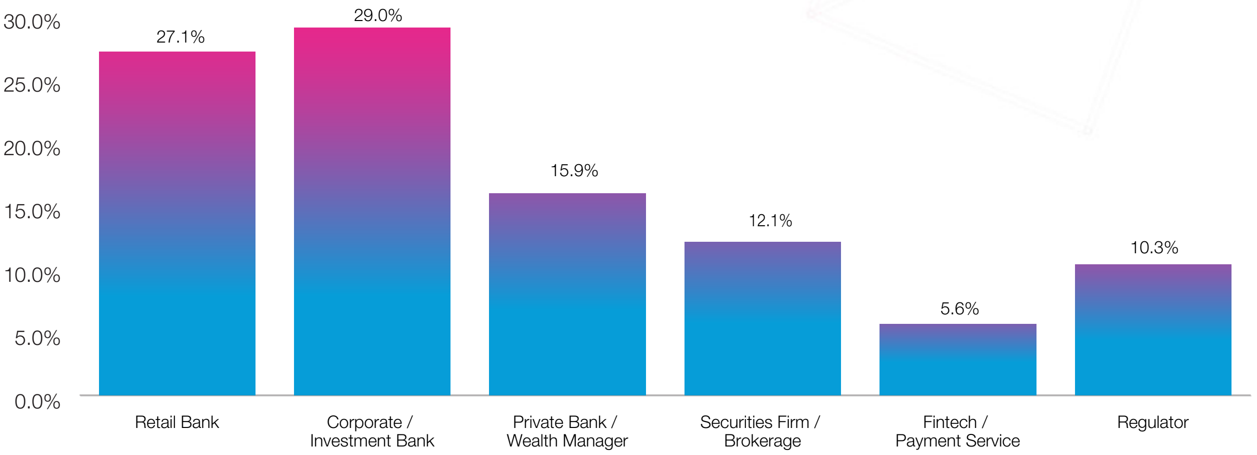
Meanwhile, the financial services industry has accelerated its shift to digital, in some cases creating new opportunities for the very same bad actors. Still, scores of enforcement actions and billion-dollar penalties continue to be levied against financial institutions (FIs), with some firms being dealt severe reputational blows, or enduring years-long battles in court, while others have lost operating licences.

In 2020, APAC overtook the US in terms of the value of enforcement actions for the first time since 2015, with regulators imposing almost USD 5.2 billion in fines for anti-money laundering (AML) violations during the year. While this was largely the result of out-sized enforcement actions in Malaysia and Australia, the trend towards more frequent and bigger-ticket AML penalties is only expected to continue as global bodies such as the Financial Action Task Force (FATF) and national governments and regulators ramp up efforts to stem the flow of illicit funds.

APAC Jurisdictions Covered in Research



Types of Institutions Covered in Research



FIs have been working to enhance their financial crime risk management capabilities, seeking to strike a balance between efficiency and effectiveness. Specifically, work is underway to improve business processes and operational workflows, through the use of technology, in key areas such as KYC, customer due diligence (CDD), screening, transaction monitoring, case management and investigations.

This paper presents the **AML Tech Barometer**, a longitudinal study that aims to track over time how FIs in APAC are integrating technology into their AML programmes. The research was conducted by *Regulation Asia*, in collaboration with NICE Actimize, between August and November 2021.

The researchers analysed survey data collected from 216 financial crime and fraud professionals across nine APAC jurisdictions. Practitioners from retail banks, corporate banks, private banks, wealth managers, securities brokers, and fintech and payment services providers participated in the study. The data was collected through an online survey, with a mix of global (38.7%), regional (27.4%) and local institutions (34.0%) covered in the sample.

> **“There is a broad recognition by the industry that data and technology, including the interface and controls between systems, are absolutely critical to get right, because this feeds into a bank’s downstream activities.”**
>
> Siddhant Sahai, Asia Pacific Director, Anti-financial Crime Testing & Quality Assurance, Deutsche Bank

Supplemented by interviews with practitioners and regulators, the research also explored the key areas firms are prioritising from both a business and technology perspective, the challenges they face in technology adoption, and their outlook for 2022. The aim of the research was to establish maturity levels at FIs for peer comparison and identify areas in financial crime risk management for further development.

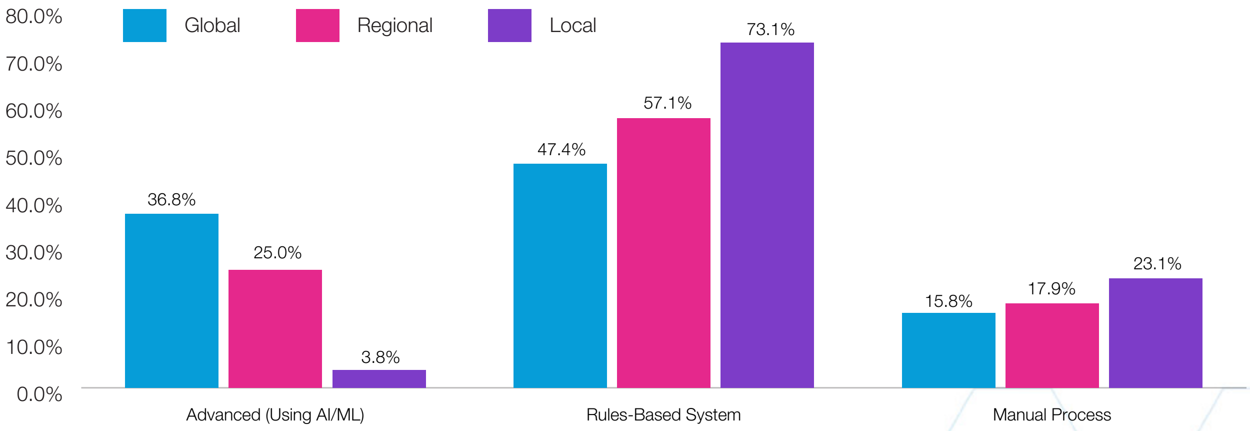
Current State of Technology Adoption

The research sought to benchmark the types of systems used across FIs, asking respondents to describe their systems as 'advanced', 'rules-based', or 'manual'. 'Advanced' systems use artificial intelligence/machine learning (AI/ML) for advanced analytics or predictive modelling. 'Rules-based' systems use sets of rules and thresholds to analyse data and detect financial crime risk. 'Manual' systems are those that would typically rely on spreadsheets and human input.

Almost a quarter (23.9%) of respondents – mostly global and regional institutions – described their financial crime risk management systems as advanced, while more than half (57.6%) described them as mainly rules-based. About 17% of respondents reported using mostly manual systems, though this was more prominent among smaller FIs with less regional or global activity.

The research revealed differences in how advanced AI/ML is defined, as well as wide variations in how autonomous advanced systems are in practice. Of the respondents who reported the use of advanced systems, a higher than expected 9.5% said their AI/ML capabilities were 'fully autonomous', meaning

Financial Crime Risk Management Systems Used by Respondents



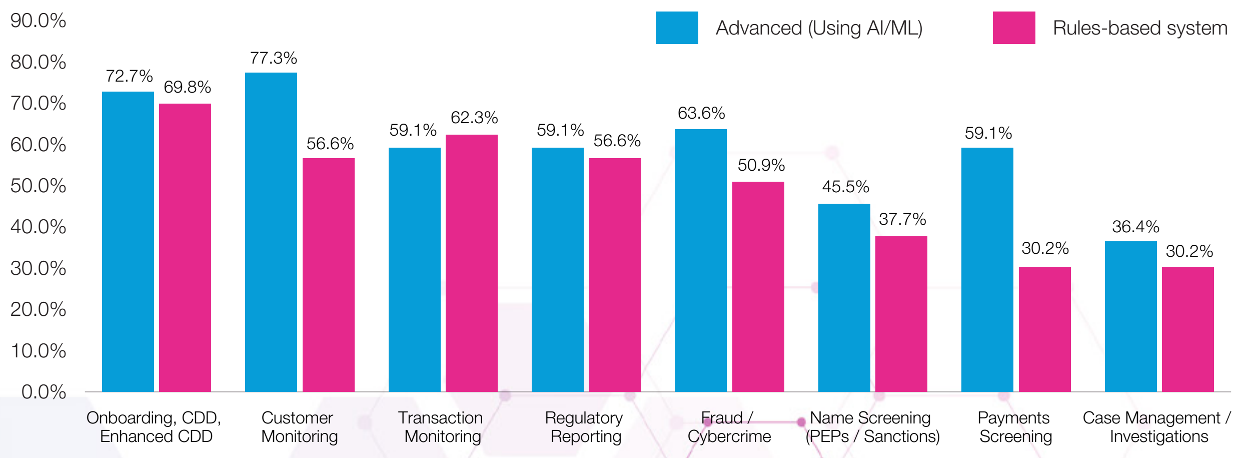
systems entirely govern or control themselves rather than rely on human input.

Other respondents said they were utilising a hybrid model, which entails the use of AI/ML with varying degrees of human input in decision-making. For the time being, the adoption of AI/ML in the sample of respondents remains nascent and its use for complicated scenarios remains limited.

The research found that the vast majority of global institutions have deployed AI/ML or rules-based systems in transaction monitoring (92.6%), screening (88.9%), customer monitoring (77.8%) and onboarding due diligence (74.1%) – reflecting their larger volumes of clients and transactions, greater exposure to risk through cross-border transactions, and a need to maintain regulatory compliance across multiple jurisdictions simultaneously.

Several respondents from global institutions cited the rapidly changing global AML and sanctions regulatory landscape, as well as the high potential cost of any non-compliance, as reasons for automating AML functions such as transaction monitoring, screening, and KYC. "These are the most fundamental areas of AML compliance and

Use of Advanced Systems vs. Rules-based Systems in Specific AML Functions



> **“Respondents from global institutions cited the rapidly changing global AML and sanctions regulatory landscape, as well as the high potential cost of any non-compliance, as reasons for automating AML functions…”**

also the most labour-intensive without appropriate technology in place,” one respondent said.

For regionally-focused FIs, the research found strong adoption of advanced AI/ML or rules-based systems for name screening (71.4%), however the use of such technology was less prevalent in transaction monitoring (57.1%) and customer monitoring (61.9%). Less than half (42.9%) of respondents from regional FIs indicated they had deployed technology for payments screening, which was below expectations given their potential exposures to financial crime hotspots in the region through cross-border payments.

Respondents from local institutions reported high adoption of technology in transaction monitoring (84%) and, to a lesser extent, customer monitoring (63.2%). Technology was less widely adopted among these respondents for name screening (47.4%) and payments screening (42.1%), reflecting their lower transaction volumes and lower exposure to risk from international payments.

On a country level, Singapore and Australia respondents in particular highlighted a strong focus on customer risk from national regulators, which have promoted a more proactive approach to ensuring customer information is complete, accurate and kept up-to-date. This was reflected in the use of technology for customer monitoring in Singapore (70%) and Australia (77.8%).

In an interview, AUSTRAC’s National Manager of Regulatory Operations, Nathan Newman, indicated that customer risk should be an FI’s “first point of call”. He highlighted that effective customer risk assessments rely on good quality data and a good understanding of data lineage, which can also help to manage flow-on risks to other AML functions such as transaction monitoring. *[See Interview Box 1: AUSTRAC – page 9]*

Respondents from Australia also revealed widespread adoption of technology in transaction monitoring (100%), payments screening (77.8%), and fraud and cybercrime (77.8%). Several respondents said this reflected increased regulatory expectations in these areas, as well as a need to better protect customers, shareholders and the broader financial system after heavy AML penalties and years of scrutiny following the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry (2017–2019).

> **“In the latest financial year 2020-2021, we received 309,772 SMRs – a 380 percent increase over the past four years.”**
>
> Nathan Newman, National Manager of Regulatory Operations, AUSTRAC

Australian Transaction Reports and Analysis Centre (AUSTRAC)

Nathan Newman, National Manager, Regulatory Operations

Nathan Newman, National Manager of Regulatory Operations at AUSTRAC, discussed financial crime risks and priorities, focusing on industry efforts to uplift Australia’s AML capabilities through technology transformation and the need to advance industry collaboration..

How have you seen the financial crime landscape change over the past 12 to 18 months? What key lessons can you highlight from these changes?

Nathan Newman: The pandemic created opportunities for criminals to move into new ways of doing their business. One key example of that, which we saw in Australia and globally, was the exploitation of government stimulus programmes.

We worked with the industry very rapidly to identify this and other trends in criminal activity that were emerging during the pandemic. Through our public private partnership – Fintel Alliance – we drew from the industry and our own data and intelligence to share typologies, which reporting entities were then able to apply to their transaction monitoring and customer risk assessments.

This highlighted the importance of industry, the FIU and the regulator continuing to work collaboratively to identify trends and share knowledge, to ensure reporting entities can put controls and risk mitigation measures in place.

Have you noticed an increase in suspicious matter reports (SMRs)?

Nathan Newman: In the latest financial year 2020-2021, we received 309,772 SMRs – a 380 percent increase over the past four years. That said, we have systems to help us triage and automate analysis of the information coming in, so we are less concerned about the volume and more about the quality of information. We try to make sure reporting entities are submitting high-quality SMRs to us.

In the past 12 months, we have provided updated guidance to entities on what a good SMR looks like. SMRs should contain detail about the suspicious activity or the nature of specific activity networks and whether there are connections to individuals. Other data such as telephone numbers and IP addresses are also very helpful.

These are all bits of the puzzle that we can use to connect intelligence and find patterns. The richer the information in an SMR is, the better it is for us to interrogate that information.

What have been the key trends you have noticed in SMRs in the last 12-18 months? What are your expectations moving forward?

Nathan Newman: Tax evasion is always a common trend. But given the increasing reliance on online and digital technology, we have also seen an uptick in scams, frauds, cyber-related crime, and the use of digital currencies to facilitate criminal activity.

The pandemic forced businesses to shift their operating models online, so looking ahead we may see a continuation of that not only within industries, but also in the criminal sector. In addition, as global economies and borders reopen, we are likely to see criminals again readjust to that operating environment, and we may see more movements of illicit goods or cash like we’ve seen in the past.

From an AUSTRAC lens, when new trends emerge, reporting suspicious matters to relevant authorities becomes especially important so that we, along with our

AUSTRAC (continued)

law enforcement partners, can get on top of those trends early and head them off quickly.

What are the key priorities for reporting entities in Australia when it comes to financial crime risk mitigation?

Nathan Newman: Based on the lessons from our enforcement actions and compliance work in the last few years, I would say customer risk is an important theme. This includes customer source of funds, whether they are PEPs, and so on. If you understand the customer risks, you can then mitigate and manage any flow-on risks, so this should be your first point of call.

Capacity is another area. Having capacity and the resources to be able to deliver on your AML obligations is important. You can't uplift on an oily rag so you have to make sure that you're investing. And we have seen a lot of uplift and transformation in the AML space – both domestically and globally.

We also emphasise governance, i.e. making sure controls are in place, and there is adequate senior management and board oversight and involvement. Businesses need to understand the importance of AML, why it is necessary, have accountability, and make sure roles, responsibilities, and decision-making are properly understood.

The other area we highlight is assurance, which links together all this work and investment that's taking place to uplift AML capabilities in Australia. We've seen situations where businesses have broken things or introduced coding errors as part of their uplift efforts, which they then have to remediate. We've then tested that remediation, and discovered in some cases that the issue hasn't been resolved. This is usually because appropriate assurance hasn't been applied.

When it comes to technology, what should be the key priorities for reporting entities? What are your expectations on the use of technology?

Nathan Newman: We've learned from some of our enforcement actions that AML investment in Australia was under done for a number of years. So part of the expenditure in uplift now is to catch up rather than to go above and beyond.

While some entities are investing in key uplifts in certain areas such as KYC systems, we're seeing a greater focus on more holistic transformation programmes. Some complex banks for example have programmes underway for changing their entire technology stacks. Meanwhile, smaller entities are also relying more on third-party vendors to provide transaction monitoring and other capabilities.

A common theme among reporting entities is data lineage, which starts from an understanding of the data being collected at onboarding and how this information feeds into customer risk assessments and other AML functions such as transaction monitoring. We see entities trying to improve their data, particularly to enhance their understanding of customer risk.

Without being prescriptive on the use of technology, we expect that it must be fit for purpose. Businesses have to understand how a piece of technology will address their AML risks and interact with their control environment. They should also know they can adjust and tailor the technology solution as the risk environment evolves.

What are the key areas of focus to uplift AUSTRAC's own technology capabilities?

Nathan Newman: Our 'REST' programme – or Reporting Entity System Transformation programme – is a big body of work to replace our existing reporting system, AUSTRAC Online, with a more modern and user-friendly technology environment for our reporting entities.

The new system design and user experience will make it easier for entities to report suspicious matters to us. We plan to provide APIs that businesses can use to integrate the reporting process within their systems, including to leverage the data contained in ISO 20022 payment messages. Guidance and support will also be available from within the platform so that entities can quickly access and draw on these resources.

We are over a year into this body of work so there's still a ways to go, but this is the number one technology priority at AUSTRAC. Besides this, we are also continuing work to improve our data and intelligence tools, so we can continue to interrogate the important data that the industry provides us, translate it, and then share it back to the industry in the form of typologies.

Business and Technology Priorities

The research also sought to understand the key priority areas for APAC FIs in the next 12 months from both a business and technology perspective. Mismatches between business and technology priorities were identified; however, respondents noted that some business priorities were related to planned enhancements to processes, procedures and internal control, rather than additional technology adoption.

From a business perspective, respondents highlighted transaction monitoring and name screening as their highest priorities, followed by KYC/CDD refresh. Given this, it is unsurprising that respondents reported broad adoption of technologies in these areas, as noted in the previous section.

One respondent noted that the first priorities will always be to comply with fundamental regulatory requirements, which are more costly for firms that get it wrong. “This is why you see many banks using technology or updating their systems in areas such as transaction monitoring, sanctions screening, KYC compliance – areas where the appetite for risk is zero,” he said. *[See Interview Box 2: Deutsche Bank – page 14]*

Cybersecurity and TBML were also highlighted by respondents as key business priorities, particularly for global and regional institutions. There were suggestions from respondents that firms will be increasingly looking to deploy new technology tools in these areas in the years to come.

“TBML has been an even bigger focus than in previous years due to increased trade between countries, as well as bad actors taking advantage of the pandemic,” said a Singapore respondent at a global bank. “Even with technology solutions in place to manage large volumes of transactions, TBML is difficult to detect as it relies on specialised expertise and manpower to check documentation and perform due diligence.”

One respondent highlighted observations that FIs are increasingly moving from having AML compliance professionals with generalist roles to having more functional specialists across different AML risk types, such as bribery, corruption, fraud and sanctions. Another respondent noted that specialists are needed in areas like illegal wildlife trade and human trafficking for document analysis and investigations. Looking ahead, coverage of all risk types, typologies and scenarios within AML teams is expected to continue to be a major challenge.

The research found network risk assessment to be a relatively low priority, despite its proven effectiveness in uncovering hidden connections between bad actors and potential criminal networks. This may change over time, however, as some regulators such as the Hong Kong Monetary Authority (HKMA) have made it a key priority to promote network analytics capabilities to tackle online fraud and associated mule account networks. *[See Interview Box 3: HKMA – page 17]*

From a technology perspective, KYC/CDD was cited as the main priority area for the year ahead. Participants in the research highlighted a need for technology-driven approaches to collect, verify and update customer information due to increased digitalisation in the financial services industry, accelerated by the pandemic.

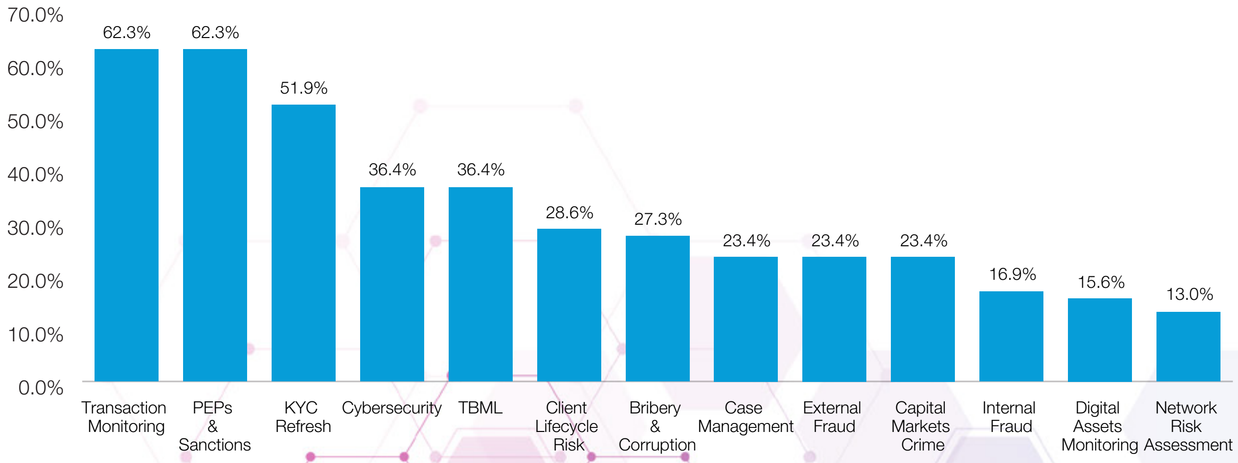
AML analytics was another key technology priority for the year ahead, though a lesser focus for local FIs. This reflects the need for increased efficiency and effectiveness to detect financial crime, explained one respondent. "The industry needs more productive alerts, and to be able to analyse customer behaviour and relationships between customers to identify patterns."

The Monetary Authority of Singapore (MAS) has been consistently encouraging FIs to explore the use of data analytics to strengthen their AML capabilities, producing guidance and collaborating with the industry through its public–private partnership. MAS says a number of Singapore FIs have already deployed data analytics tools in areas such as transaction monitoring, name screening and network analysis. *[See Interview Box 4: MAS – page 21]*

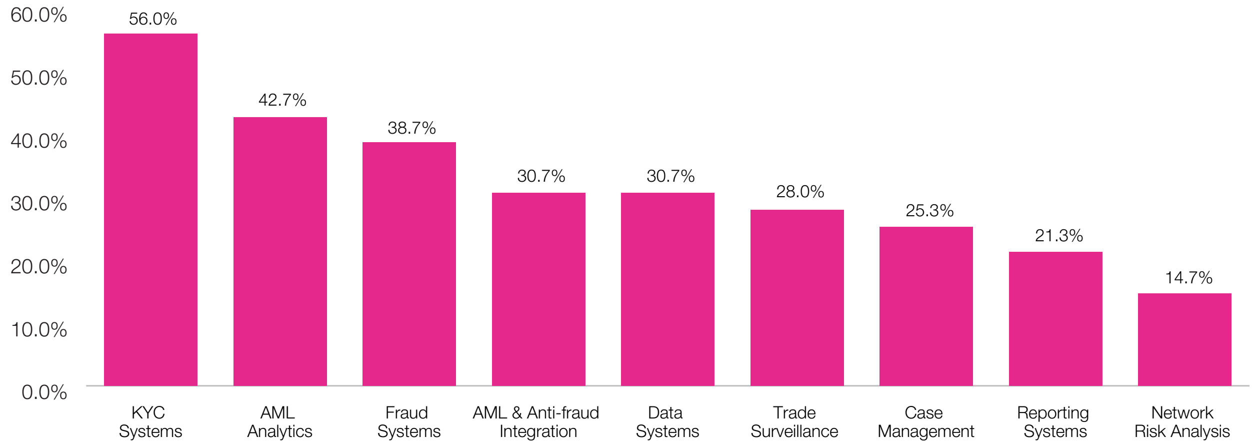
The research also identified fraud monitoring and detection systems as a key technology priority for FIs. Given a natural cross-over between AML and fraud systems, respondents indicated that achieving greater integration across these systems will be a bigger priority moving forward for the industry as a whole.

"A key trend we are seeing is increased collaboration between the AML and fraud functions," said one respondent. "Full convergence is probably not likely because these teams require a slightly different skill set, but there

Financial Crime Business Priorities Selected by Respondents



Financial Crime Technology Priorities Selected by Respondents

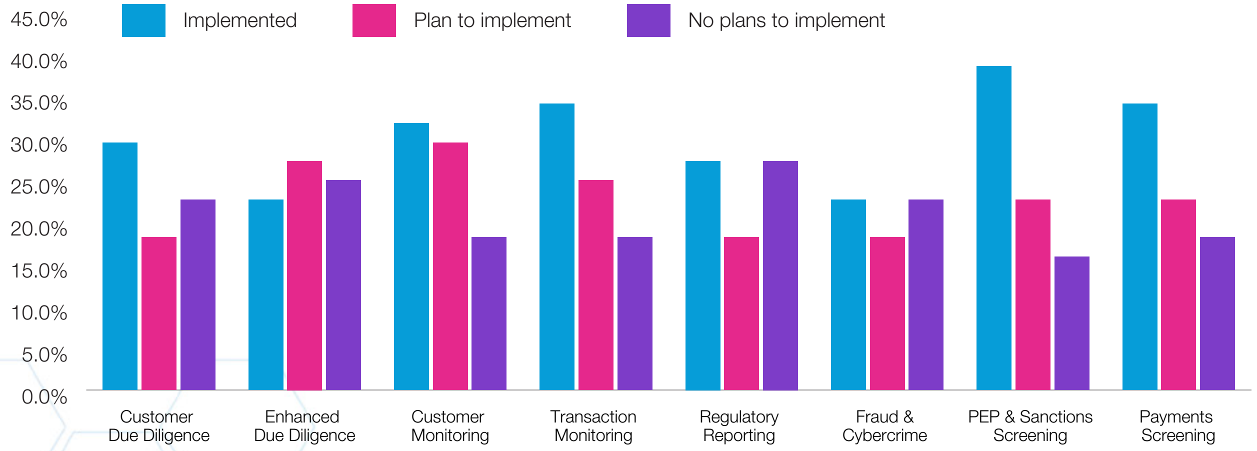


is an increased recognition that they cannot exist completely independently of one another."

Among the key technology priorities identified in the research, respondents from global institutions in particular reported data quality and management as high on the list, citing a need to standardise practices across the different jurisdictions in which they operate. Some respondents noted that data localisation and privacy regimes in some APAC jurisdictions were creating fragmentation in their own operations and systems deployments, requiring manual workarounds, or for data repositories and infrastructure to be duplicated across jurisdictions.

The research also sought to identify the systems in which FIs are planning to enhance or augment with AI/ML solutions. The top areas where respondents said AI/ML tools have already been deployed, or where there were plans in place to do so, were customer monitoring, screening and transaction monitoring.

Use of AI/Machine Learning in AML Systems



Some respondents described name screening and transaction monitoring in particular as the "lowest-hanging fruit" in their own advanced AI/ML adoption journey. "Generally speaking, these high volume, low value areas are more conducive to such technologies, and also much needed to address the issue of false positives that we see with more traditional rules-based systems," said one respondent.

More than a quarter of respondents (27.3%) indicated plans to adopt AI/ML for enhanced due diligence of high risk customers, an area where there are generally lower levels of automation across the industry. In interviews, respondents highlighted a need for better education on the benefits of using advanced AI/ML for different use cases.

Deutsche Bank

Siddhant Sahai, Asia Pacific Director, Anti-financial Crime Testing & Quality Assurance

Siddhant Sahai, Asia Pacific Director for Anti Financial Crime (AFC) Testing and Quality Assurance at Deutsche Bank, discussed financial crime risks and priorities, highlighting the need for greater collaboration and technology interventions to address the financial crime threat.

How have you seen the financial crime landscape change in the last 18 months as the world has increasingly gone digital?

Siddhant Sahai: In the last 18 months, the rapid adoption of technology by banks to go digital in everything that we do has challenged the traditional way in which we look at financial crime. In particular, the use of data analytics and other technologies in financial crime risk management has been on the rise and this will likely expand further in 2022.

For example, trade-based money laundering (TBML) is prone to fraud and money laundering and naturally a key area of concern for regulators, particularly given the increase in global trade volumes. The ability to use technologies such as blockchain to address some of the challenges with trade-related transactions changes the game.

Then there are areas like KYC, which has progressed to e-KYC with increasing use of digital IDs. In a remote working environment, banks must evolve their processes to ensure there are no fake IDs, there is no element of fraud, and that they are collecting the necessary information from clients and performing the right level of due diligence.

Is fraud an area that you are concerned with?

Siddhant Sahai: Fraud is omnipresent. It may be a risk type within financial crime or within operational risk at some banks, but the fact is that it cuts across everything. We're increasingly seeing the fraud function converge with areas like cyber risk and AML as there are overlaps.

In each of our reviews – whether it's transaction monitoring, sanctions screening, or bribery and corruption – the fact is that fraud risk is present across all these areas. So, we spend a lot of time testing against various fraud scenarios to make sure we provide assurance on areas where frauds could occur, and that anti-fraud controls can be put in place.

What are the key challenges the industry faces when it comes to customer due diligence?

Siddhant Sahai: In today's competitive environment with neo-banks, fintechs, etc. you must perform KYC faster to serve clients and remain competitive. At the same time, you often need some confirmation from the first line or more time to reach a certain depth of detail in your customer due diligence. This conflict can make it difficult to always obtain a full view of a client.

When it comes to due diligence, especially when it comes to the wealth management/high net-worth segment, one of the biggest problems is in identifying beneficial ownership. Some of the corporate structures in place are specifically designed to hide the ownership. And frankly speaking, action around this globally across the industry needs to improve substantially.

Even in places where you are able to obtain data from a registry, often that information is limited or of low quality. Some jurisdictions are also planning to impose stricter restrictions on the data that can be accessed, in the name of privacy, which is contrary to the whole idea of transparency.

Deutsche Bank (continued)

We need to have beneficial ownership registries that are open and transparent. But I think this will take some time to resolve, because jurisdictions are varying in their approaches and there is strong resistance in some countries.

What do you see as the main business and technology priority areas for banks when it comes to addressing financial crime risks. How will this evolve in the years to come?

Siddhant Sahai: Naturally the first priorities for banks will be to comply with regulatory requirements. This is why you see many banks using technology or updating their systems in areas such as transaction monitoring, sanctions screening, KYC compliance – areas where the appetite for risk is zero. For example, you can't have a sanctions impact, otherwise your bank will be in the news and the organisation's reputation and business can be badly affected.

Besides the regulatory requirements, these are also high cost areas for banks. For example, transaction monitoring comes with a lot of false positives which are a huge manpower cost to remediate. So for example, there is a lot of investment in technology projects around the use of machine learning to try to reduce false positives.

That said, this doesn't necessarily mean you're always able to prevent financial crime, even as one is adhering to laws, and applicable regulatory requirements. Areas like cyber, trade, external fraud, anti-bribery, virtual assets – these are areas where I expect the focus to be in the years to come to truly address financial crime risks.

What would you like to see from the industry to – as you put it – truly address financial crime risks?

Siddhant Sahai: I feel there is not enough focus on inter-bank relationship monitoring. Even if you detect certain risks and you offboard a customer, they could go to another bank or non-banking institution and find other ways around the system.

As we know, bad actors can be very creative and are only getting more innovative. Through the pandemic we've seen an increase in wildlife trafficking, drug trafficking, fake charities, investment scams – this is all happening through online mechanisms. And as more people adopt digital technology the risks increase.

We need to ensure that the collaboration between governments, FIUs, banks – and countries between themselves – have open, transparent and timely sharing of information in order to genuinely be able to prevent crime. This is an area where I think technology systems designed specifically for collaboration need to come in.

Where do you see the industry heading from a technology perspective? Where are banks investing?

Siddhant Sahai: Most banks start off using Robotics Process Automation (RPA), such as for KYC. This is the lowest hanging fruit. The more complex would be technologies like network and graph analytics, where you start identifying patterns between customers and transactions and making use of scenarios for analysis.

Somewhere in the middle is the use of AI and machine learning – this is where I see most banks investing, particularly for transaction monitoring and screening, to reduce the number of false positives that have to be manually remediated. Banks want to use machines to handle low value alerts, so that humans with more specialist expertise are free to handle high value alerts.

Ultimately this helps banks get faster and better focus on the quality of intelligence, which can lead to more worthwhile investigations and higher quality SARs [suspicious activity reports] – which is a key factor for regulators and law enforcement to be able to criminally prosecute bad actors.

A point worth mentioning is that a lot of these technology interventions rely on the bank's quality of data, and the flow of data from disparate systems – because if your data is not correct, then your monitoring will be flawed. Data management continues to be a top risk for any bank, that's why you see these massive projects around data across the industry.

That said, I think there is a broad recognition by the industry that data and technology, including the interface and controls between systems, are absolutely critical to get right, because this feeds into a bank's downstream activities. These kinds of changes are already underway, and in this regard the industry seems to be heading in the right direction.

Customer Due Diligence Challenges

The research sought to understand the primary challenges FIs face when it comes to CDD, by asking respondents to rank these challenges. About 60% of respondents said complex corporate structures were their top CDD challenge, reflecting a continued lack of beneficial ownership transparency across jurisdictions, which has been a key area of focus for the Financial Action Task Force (FATF).

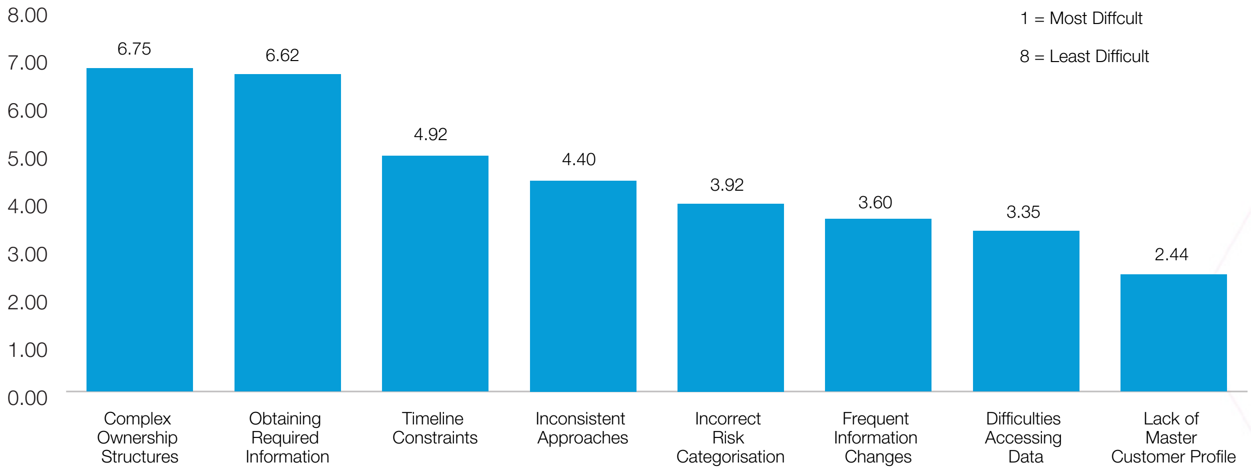
Following its October Plenary, the FATF released a statement directly addressing the Pandora Papers leak and highlighting the urgent need to put an end to the use of networks of anonymous shell companies and legal arrangements to obscure beneficial ownership and hide illicit profits. Out of more than 100 mutual evaluations, only 10 percent of countries were found to be taking effective measures to ensure the transparency of company and trust ownership, the FATF said.

The FATF has proposed amendments to its standards on transparency and beneficial ownership of legal persons to ensure jurisdictions make adequate beneficial ownership information available and keep it up to date. Once finalised, the amendments will require FATF member jurisdictions to designate a public authority or body to hold beneficial ownership information (e.g. companies registry, beneficial ownership registry), or otherwise provide for an alternative mechanism that can serve the same function.

In the research, the lack of beneficial ownership transparency appeared to be a consistent pain point across all types of institutions, in all jurisdictions, and regardless of the operational focus of respondents. This was perceived as a greater challenge for firms that predominantly use rules-based systems, compared to those using advanced or manual systems.

Respondents said the burden on FIs to identify beneficial ownership forces them to use alternative approaches and data sources, which is often manual. “Even in places where corporate

The Challenges in CDD (Rank-based Scores)



> **“Part of the HKMA’s “Fintech 2025” vision is to see Regtech being extensively adopted by the banking sector, particularly where financial crime risk management is concerned.”**
>
> Hong Kong Monetary Authority

registries are established, there are persistent and ongoing data quality issues that need to be addressed, maybe through intervention by the FATF”, one respondent said.

According to some respondents, a key factor that makes this area so challenging is the tendency for bad actors to frequently change the ownership structures and actual owners of offshore and shell companies to evade detection. This is an issue that has also been highlighted by MAS, which said criminals will often switch out company directors, signatories or other key personnel after opening an account in order to engage in money laundering or other financial crimes. *[See Interview Box 4: MAS – page 21]*

“FIs would typically not identify such changes until they perform a periodic review,” said one bank respondent. “There is a increasing need for technology solutions that automate the collection and aggregation of beneficial ownership information from disparate and fragmented data sources on an ongoing basis.”

Among their key CDD challenges, respondents also cited difficulties obtaining the information they need, meeting timeline constraints, and accessing the relevant data. These are likely to also be related to the lack of beneficial ownership transparency in many jurisdictions.

“Ensuring a greater understanding of customers, their relationships, and their associated risks has been an ongoing challenge for many organisations,” said Adam McLaughlin, Global Head of Financial Crime Strategy at NICE Actimize. “Taking an entity-centric approach is a way to overcome these challenges.”

“This approach involves aggregating data, and centralising the assessment against a consolidated customer profile. It includes automated assessments of customers’ corporate networks and ultimate owners and controllers, and continual monitoring of data. Continuous assessment means moving CDD programmes from a periodic risk assessment process to a trigger based process. This ensures firms always have an accurate picture of customer risk.”

Hong Kong Monetary Authority

As part of the research project, the Hong Kong Monetary Authority (HKMA) submitted written comments highlighting its observations on the use of technology in the AML space, and key initiatives to facilitate greater adoption moving forward.

What should be a FI’s key priorities when it comes to ML risk management?

HKMA: KYC/CDD, onboarding, transaction monitoring and screening are all important processes and systems when it comes to ML risk management. What we see as a priority area for banks in particular is to make these control systems more effective and efficient, while minimising as far as possible any additional touch points for customers. Implementation of these processes and systems represents significant investments of cost, staff resources and effort, thus it is highly desirable to maximise returns and value.

And it does not have to mean investing large sums in entirely new systems. In recent years, new methods have emerged that offer real opportunities to get more out of

Hong Kong Monetary Authority (continued)

existing systems. For example, some banks have been able to demonstrate the value of machine learning to significantly lower the levels of false hits in transaction monitoring systems, freeing human analysts to focus on higher-value work requiring professional judgement.

We have also seen rapid growth in remote customer on-boarding, in part as a result of social distancing requirements under Covid-19, although the trend had already started developing before the pandemic. The launch of eight virtual banks in Hong Kong has also been a big factor. This is good for customers, who can access services more easily, and provides banks with additional channels to engage customers.

Of course, there is no one-size-fits-all solution and each institution needs to identify the approach that best suits its own circumstances and business focuses.

What are the priority areas where technology can enhance ML risk management?

HKMA: The HKMA is prioritising the promotion of Regtech adoption because we fully believe Regtech has the potential to bring massive benefits; to banks, to customers and to regulators, including the HKMA.

At the sectoral level, the key priority is to further enhance the effectiveness of the AML/CFT regime through greater use of data and technology, and to augment the positive impact of information and intelligence sharing in preventing criminal abuse of the banking system and protecting customer accounts.

We also understand the priorities for banks at the institutional level, as we are enhancing our ecosystem surveillance and engagement, periodically collecting data and meeting banks on a variety of platforms including the HKMA Fintech Supervisory Chatroom. As a general observation, there are two key priorities for Regtech adoption from banks' perspectives: first, to improve the end-to-end customer experience (e.g. remote customer on-boarding and account maintenance); and secondly, to develop a more holistic strategy around data.

In terms of specific technology applications, while the priorities will differ depending on a FI's individual business models and customer base, transaction monitoring and screening are areas regarded as offering some of the best potential for effectiveness and efficiency gains.

What are the HKMA's expectations on the adoption of technology for AML?

HKMA: In our engagement, we have put forward clear evidence that Regtech can benefit different stakeholders in the AML ecosystem. At the same time, we also work closely with banks in addressing the challenges associated with Regtech adoption.

Part of the HKMA's "Fintech 2025" vision is to see Regtech being extensively adopted by the banking sector, particularly where financial crime risk management is concerned. To facilitate this, we have been sharing success stories of Regtech implementation – how others overcame the challenges and providing practical guidance to banks, such as in the "AML/CFT Regtech: Case Studies and Insights" report issued in January 2021.

What are some of the key HKMA initiatives aimed at promoting technology adoption for AML purposes?

HKMA: The HKMA launched on 5 November 2021 the first AMLab, in collaboration with Cyberport and supported by Deloitte, to further encourage the use of Regtech under the "Fintech 2025" strategy. The AMLab series will strengthen banks' capabilities to protect customers from fraud and financial crime losses, reduce risk displacement across the banking sector and raise the overall effectiveness of the AML ecosystem.

The first AMLab focuses on using network analytics to target the risks of fraud mule-account networks, enhancing data and information sharing through public-private partnership efforts in AML. Future AMLabs are being planned which will look at other areas where Regtech can support banks' gatekeeper role in the AML ecosystem and help safeguard customer accounts.

Indeed, AMLab is another initiative the HKMA is taking as part of the broader "Fintech 2025" strategy to advance banks' positive and responsible use of new technologies for AML/CFT. In September, the HKMA also hosted an AML webinar with speakers from law enforcement agencies and industry to share experience and success stories of banks and Stored Value Facility (SVF) licensees.

The agenda focused on how the industry is combatting online fraud and money laundering networks using technology and data, underpinned by increasing public-private collaboration. Events like this, where industry practitioners share their experience, are an important way of encouraging learning and collaboration.

Transaction Monitoring & Screening Confidence

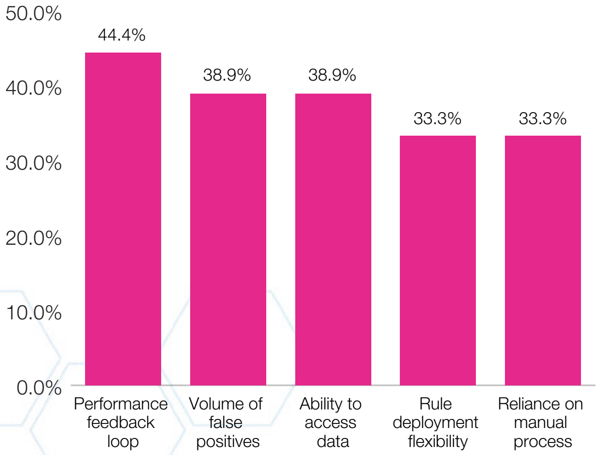
Through the research, transaction monitoring and screening were identified as the areas where the use of technology for automation is most widespread across the industry. Most FIs are either relatively advanced in or have work programmes underway to enhance their transaction monitoring and screening systems. In light of this, the research sought to identify the key factors that influence confidence in these systems.

For transaction monitoring, the biggest confidence influencer was the ability to understand the performance of rules and thresholds. Most FIs adjust these rules and thresholds based on key AML risk areas, red flags and their organisational risk tolerance. "Within the industry, depending on your vendor, it is often a challenge to measure and assess the impact of rule changes, which is key to finding the right balance between efficiency and effectiveness," one respondent said.

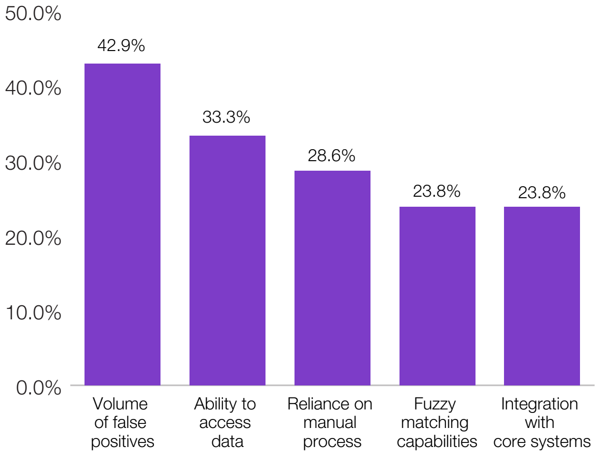
The ability to create, deploy and adjust rules and thresholds was also highlighted in the research as a key factor influencing confidence in transaction monitoring systems. Some respondents noted that certain vendors do not provide flexibility to allow FIs to make changes to rules and thresholds using in-house teams. "Having to go back to the vendor to make a change each time hinders a bank's ability to fine-tune its systems in a timely and cost-effective manner," said one participant in the research.

The need for rule deployment and adjustment flexibility is further underscored by another factor: the volume of false positives, which was identified as a top issue for both transaction monitoring and screening systems. Highlighting the high manpower and time costs associated with resolving these alerts, several respondents noted that the ability to flexibly adjust rules and thresholds, and understand the impact of

Factors that Influence Confidence in Transaction Monitoring Systems



Factors that Influence Confidence in Screening Systems



such changes, is an important mechanism for addressing high false positives.

For both transaction monitoring and screening, the ability to access up-to-date and relevant data was also cited as a major factor influencing confidence in these systems. In transaction monitoring, the focus was on the ability to access data from disparate systems, including customer entity information and transaction data, to enhance the quality of the detection rules. Several respondents said such information should be incorporated in all alert generation.

The research highlighted a strong aversion to manual processing of alerts generated from transaction monitoring and screening systems. This reflects earlier findings that both areas are key business priorities for most FIs in the year ahead, as firms seek to enhance processes and procedures for dealing with high alert volumes.

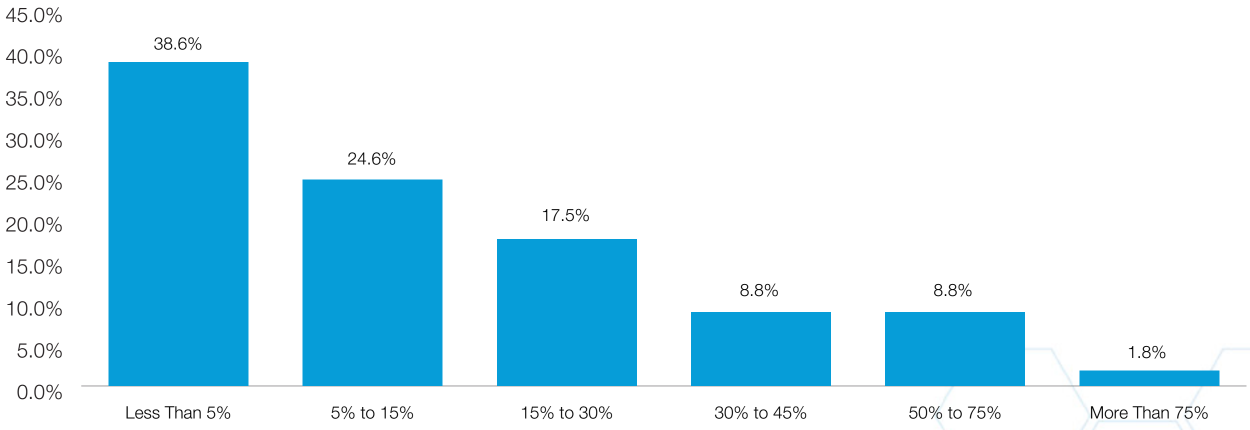
The research further explored high false-positive rates reported in the industry by asking respondents to estimate the percentage of alerts that are ultimately escalated to suspicious transaction/matter reports (STRs/SMRs). The alert-to-case ratio was reported to be lower than 15 percent for 63.2% of respondents. However, 17.5% of respondents reported ratios between 15-30 percent, and 19.3% reported ratios over 30 percent – which were outside expectations.

More granular analysis of the data revealed that respondents reporting the higher ratios were clustered around retail banks and firms using rules-based systems. Advanced systems that use AI/ML or other data analytics techniques are widely seen as being more effective at resolving alerts in a timely manner. In follow-up interviews with some respondents, there were indications of insufficient ability to generate quality alerts, a lack of skilled or experienced investigators, or a low regulatory risk appetite.

For some FIs, cases were being escalated more quickly to ensure that STRs/SMRs were filed quickly, commonly known as 'defensive reporting', which has long been a challenge for regulators, FIUs and law enforcement agencies. Large volumes of STRs can often hinder investigations and prosecutions, particularly when the information submitted is of low quality or contains limited useful intelligence.

FIUs such as AUSTRAC have systems in place to triage incoming SMRs and automate analysis of the information, making high volumes less of an issue. Still, AUSTRAC emphasises that the quality of information submitted by FIs is of particular importance for the information to be useful in investigations. *[See Interview Box 1: AUSTRAC – page 9]*

Average Alert-to-Case Ratio of Respondent Institutions



“MAS has consistently encouraged FIs to explore how they can use data analytics and digital processes to strengthen their AML/CFT capabilities.”

Monetary Authority of Singapore

Monetary Authority of Singapore

As part of the research project, the Monetary Authority of Singapore (MAS) submitted written comments highlighting its expectations on the use of technology in AML risk management and its approach to industry engagement.

What should be a FI’s key priorities when it comes to AML?

MAS: An effective ML/TF risk management framework requires robust controls at all stages of the customer relationship, as criminals can take advantage of the weakest link in the chain.

For instance, MAS and the Commercial Affairs Department (CAD) have warned the industry of typologies where criminals employ front men when opening a corporate account, but then switch the company’s directors, signatories or other key personnel thereafter to engage in money laundering or other financial crimes.

The banks involved were able to detect the changes in ownership to higher-risk individuals based overseas, as well as suspicious transactions that did not fit the customer’s profile at onboarding.

What are MAS’ expectations on the use of technology for AML?

MAS: MAS has consistently encouraged FIs to explore how they can use data analytics and digital processes to strengthen their AML/CFT capabilities. This should be anchored by a robust governance framework that ensures high-quality data inputs, identifies clear objectives and desired outcomes, and systematically measures the effectiveness of these tools.

Through our AML/CFT Industry Partnership (ACIP), we have worked with the industry to highlight successful use cases, address operational challenges, and outline good governance principles.

For example, ACIP’s 2018 report highlighted areas where data analytics can help to improve the effectiveness of FIs’ AML/CFT measures, such as to address high false positive rates in screening and transaction monitoring. In 2019, ACIP also published key takeaways from a workshop with FIs on the adoption of data analytics to enhance AML effectiveness, focusing on explainability and governance.

Since then, a number of FIs have deployed data analytics tools in areas such as name screening and the use of network linked analysis to uncover potential criminal networks.

While FIs have made significant progress in strengthening their AML/CFT effectiveness, including through the use of data analytics tools, a major remaining challenge is that they are unable to warn each other about unusual activity in customers’ accounts. The Collaborative Sharing of ML/

> **“There is uniformed recognition from FATF members including Singapore that criminals are exploiting the crisis to commit scams, fraud and cybercrime.”**
>
> Monetary Authority of Singapore

Monetary Authority of Singapore (continued)

TF Information & Cases platform, or COSMIC, will address this gap by letting FIs more quickly detect and put a stop to serious criminal behaviours.

How have MAS and ACIP helped to ensure FIs are able to adapt to new financial crime typologies?

MAS: MAS identifies emerging concerns through our surveillance and close supervisory engagements with FIs, as well as partnerships such as ACIP. MAS then warns the industry of such new risks by issuing confidential alerts or working with ACIP on advisories, and following up with the affected FIs.

For major and systemic concerns, MAS may conduct thematic inspections and publish guidance papers to ensure that the industry's defences are attuned to the threat. ACIP may also set out industry best practices for dealing with such risks.

What is MAS' approach to suspicious transaction reporting? Have you seen any trends emerge in the past 12-18 months?

MAS: MAS monitors FIs' STR filing trends in collaboration with the Suspicious Transaction Reporting Office (STRO) which is Singapore's financial intelligence unit (FIU). Where necessary, MAS engages FIs to clarify situations where STR filing is required and tighten their approach to doing so.

On 8 October 2021, the CAD released its annual report for 2020, which includes details of STRO's work such as the annual statistics and other information relating to Singapore's STR regime. It also includes high level comments on the financial crime landscape that are relevant.

The FATF also published a paper last year on “Covid-19 related Money Laundering and Terrorist Financing Risks and Policy Response”. This is a compilation of FATF members' observations as the pandemic unfolded. There is uniformed recognition from FATF members including Singapore that criminals are exploiting the crisis to commit scams, fraud and cybercrime.

Trends in Suspicious Transaction Reporting

The research also sought to identify areas where respondents saw an increased focus in STR/SMR filings, with a view to offering a point of comparison against future editions of the AML Tech Barometer.

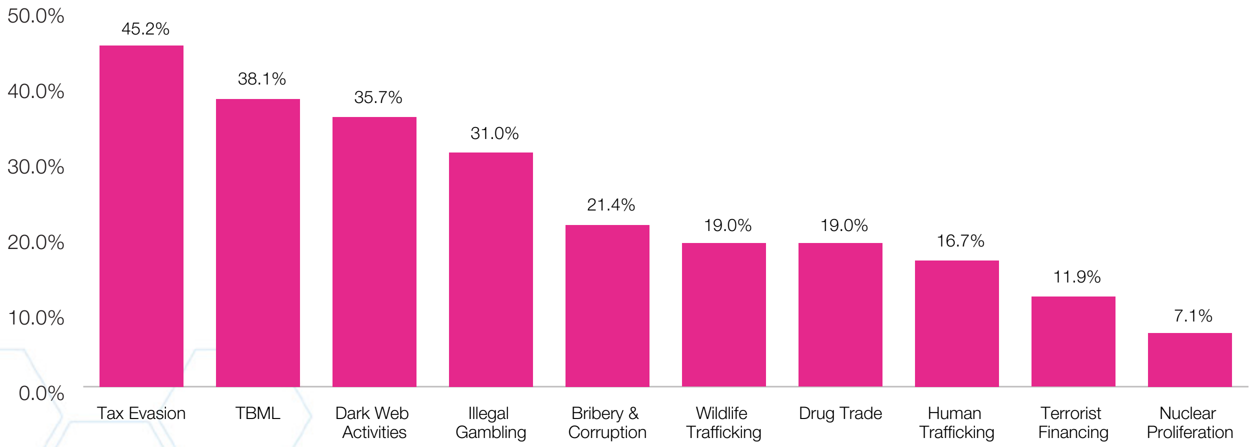
According to the respondents, tax evasion was the top area of activity in filings. As one participant noted, it is common for tax evasion to be the top reason for filing an STR/SMR, but it is often only after a full investigation that it would be revealed that a different predicate crime might be involved.

TBML was found to be the second-most prominent area of activity in filings, according to respondents, reflecting a major pain point for APAC FIs. Emerging dark web activities, being the third most active area in filings, reflects a heightened awareness of risks relating to cybercrime, ransomware attacks and cryptocurrency-related crimes.

Areas such as illegal wildlife trade and human trafficking crimes were not considered high focus areas, though respondents suggested that this would change over time as typologies and detection capabilities for these offences improve, and governments, regulators and law enforcement agencies ramp up pressure on criminal networks engaged in these activities.

The research showed that nuclear proliferation is not yet a major area of focus in filings. However given that this activity is increasingly being prioritised by the FATF, individual jurisdictions are expected to follow suit. Nuclear proliferation is expected to become a greater focus in STR/SMR filings in the years ahead, some respondents said.

Areas of Increased Activity in STRs/SMRs



Looking Ahead

The inaugural **AML Tech Barometer** and the research that went into it provided an opportunity to better understand the technology adoption journey at individual FIs, and how they are prioritising resources to enhance their AML effectiveness. For the most part, FIs are largely focused on advancing the most fundamental areas of their AML systems, in order to meet regulatory requirements, first and foremost.

However, this doesn't necessarily mean an FI is preventing financial crime, said one respondent. “You're doing a check-the-box exercise because that's what the regulations require. You have to do transaction monitoring, sanctions screening, KYC – this is not new. To target meaningful financial crime prevention, we have to invest more in areas like fraud, anti-bribery and corruption, and cyber.”

The findings indeed showed that FIs are increasingly looking for opportunities to increase convergence between their AML, fraud, and cybersecurity functions, recognising that the existing distinctions between these systems are the result of self-made organisational silos, rather than a compliance necessity, and that no such boundaries exist for bad actors.

The research also shows that local institutions are doing more to enhance their AML systems than they are often given credit for. Locally-focused institutions are often perceived as laggards, due to their conservative nature, reliance on manual processes, and resource constraints. Rather, the research shows that many local FIs, which are often smaller and easier to manoeuvre, are leveraging technology at a rapid pace to leapfrog their larger, slower-moving peers.

In the course of the research, a number of respondents applauded the FATF's efforts in recent years, targeting what some industry practitioners think should be “the biggest areas of concern for the industry and the world” – such as environmental crime, illegal wildlife trade and proliferation financing, among other areas. Some respondents said the FATF standards are increasingly helping to promote regulatory harmonisation and an enterprise-wide focus on financial crime at FIs.

Beyond its standards, the FATF has also been encouraging innovation and the use of technology to improve the efficiency and effectiveness of AML processes. This encouragement has been a

> **“Criminals are continually adapting and enhancing their tools to counter our defences. The only way we are going to win is by fighting back…”**
>
> Adam McLaughlin, Global Head of Financial Crime Strategy, NICE Actimize

crucial factor driving engagement on technology issues at the local level, one participant said from a bank in Hong Kong.

“The work the FATF is doing to promote internationally consistent AML compliance and governance standards has been both important and impactful,” the banker said. “There is still more work to be done, but we are seeing that regulatory harmonisation is achievable in the long-run, and that innovation will increasingly help us to stamp out bad actors.”

The efforts by the FATF, regulatory bodies and the regulated sector to drive greater effectiveness has been encouraging, said Matthew Field, APAC Market Lead for Anti Money Laundering at NICE Actimize. “We are all working towards the same goal, which is to identify criminal behaviour and report this behaviour to regulators and law enforcement.”

“Criminals are continually adapting and enhancing their tools to counter our defences. The only way we are going to win is by fighting back, and that means greater adoption of new, advanced technologies. It also means we all need to work together and share critical information about suspicious entities, new and evolving typologies, and suspicious activity.”

As the research showed, there is indeed a strong push to deploy advanced AI/ML tools in areas like transaction monitoring and screening. Meanwhile, data analytics techniques are increasingly being used to better understand customer risk, detect patterns, and identify network risks. Such tools enable FIs to generate more productive alerts, so that AML practitioners with specialist expertise are free to handle higher value alerts.

Looking ahead through 2022 and beyond, banks will continue to evolve their processes to adapt to new digital norms, in the process making the use of technology for AML even more widespread, and information sharing all the more necessary.

This paper was published by Regulation Asia in collaboration with NICE Actimize.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global FIs, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance.

The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Find us at www.niceactimize.com @NICE_Actimize

Get in Touch

Matthew Field
APAC Market Lead for Anti Money Laundering
NICE Actimize
Matthew.Field@niceactimize.com

About Regulation Asia

Regulation Asia is the leading source for actionable regulatory intelligence for APAC markets. Since 2013, our audience and subscription base have grown to include regulatory bodies, exchanges, banks, asset managers and service providers, allowing us to play a key role in the regulatory agenda.

www.regulationasia.com