

Report

AML Tech Barometer 2023

Financial Crime in a
Borderless World:
Perspectives from Asia



Contents

1. Executive Summary	3
2. Introduction & Methodology	4
3. Current State of Tech Adoption for AML.....	6
4. Interview: Hong Kong Monetary Authority (HKMA) Ms Carmen Chu, Executive Director (Enforcement and AML)	8
5. Use of Advanced Technologies	11
6. Interview: Australian Transaction Reports and Analysis Centre (AUSTRAC) Brad Brown, National Manager Regulatory Operations	14
7. Business and Technology Priorities	17
8. Interview: Financial Services Agency, Japan (FSA) Daisuke Mamba, Director and Head of AML/CFT Policy Office Hiroshi Ozaki, Chief Financial Inspector of AML/CFT	19
9. Frequency of Risk Assessments.....	21
10. Interview: RUSI's Centre for Financial Crime and Security Studies (CFCS) Tom Keatinge, Founding Director	23
11. Transaction Monitoring & Screening	26
12. Trends in Suspicious Transaction Reporting	28
13. Looking Ahead	29

Executive Summary

In the face of enduring global challenges in the past year, including geopolitical and economic instability, we have witnessed ever-increasing efforts by governments, regulators and law enforcement agencies across the globe to disrupt criminal activity, particularly money laundering. As a result, financial firms have continued to prioritise efforts to bolster their financial crime controls and the technology underpinning them.

This AML Tech Barometer report presents findings from the second year of research by NICE Actimize and Regulation Asia to explore how practitioners at Asia Pacific financial institutions (FIs) view their financial crime risk management capabilities and the efforts being made to enhance these capabilities with technology.

The research found that FIs have been increasingly leveraging more advanced technologies in their AML systems, including artificial intelligence and machine learning (AI/ML). According to the respondents, this reflects growing confidence in and increasing maturity of AI/ML, as well as encouragement from regulators to experiment with such technologies. Many FIs that have yet to adopt such approaches indicated that work programmes to do so are either underway or planned.

Following on from the trends identified a year earlier, the research also highlighted a significant increase in the use of more advanced systems to cover transaction monitoring and name screening in 2022 compared to a year earlier, attributed to growing risks in the financial crime landscape including a need to detect and mitigate sanctions-related risks. Transaction monitoring and name screening are also seen as top priorities for 2023, including work to better address high false positive rates generated from such systems.

As we look to the year ahead, Europe is already starting to question the lawfulness of full entity ownership transparency. Closer to home in Asia Pacific, the focus continues to be on data quality, with most FIs looking to prioritise work to streamline the collection and verification of customer information to improve risk detection and obtain more reliable output from analytics. Respondents cited AML analytics as a key technology priority for 2023, reflecting a need for greater efficiency, more productive alerts, and the ability to analyse customer behaviours, relationships and networks.

This report features insights from interviews with the Hong Kong Monetary Authority (HKMA), the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Financial Services Agency of Japan (FSA), and RUSI's Centre for Financial Crime and Security Studies (CFCS).

Introduction & Methodology

In October 2022, INTERPOL [released](#) its first-ever Global Crime Trend report, bringing together data from its 195 member countries alongside information and analysis from its own data holdings and other information sources.

The report said that over 67% of survey respondents from law enforcement agencies around the world ranked money laundering as the number one crime threat, followed by ransomware, phishing and online scams, and financial fraud. In Asia Pacific, although financial fraud was ranked as the number one crime threat, it was closely followed by money laundering.

INTERPOL's report calls for a more concerted approach to combatting financial crime and corruption, particularly money laundering, which "ultimately sustains and empowers organised crime". While urging greater cooperation across countries to improve the tracing, seizure and confiscation of criminal assets, the report also calls for increased efforts, information sharing, and intelligence from private sector actors—the ultimate gatekeepers to the financial system.

The full version of the report, restricted to law enforcement, showed how crime areas converge in complex and mutually reinforcing ways. For instance, cybercriminals rely upon financial fraud to launder their illicit gains. This has given rise to and hastened the emergence of "financial crime-as-a-service", including digital money laundering tools that enable criminals to cash out.

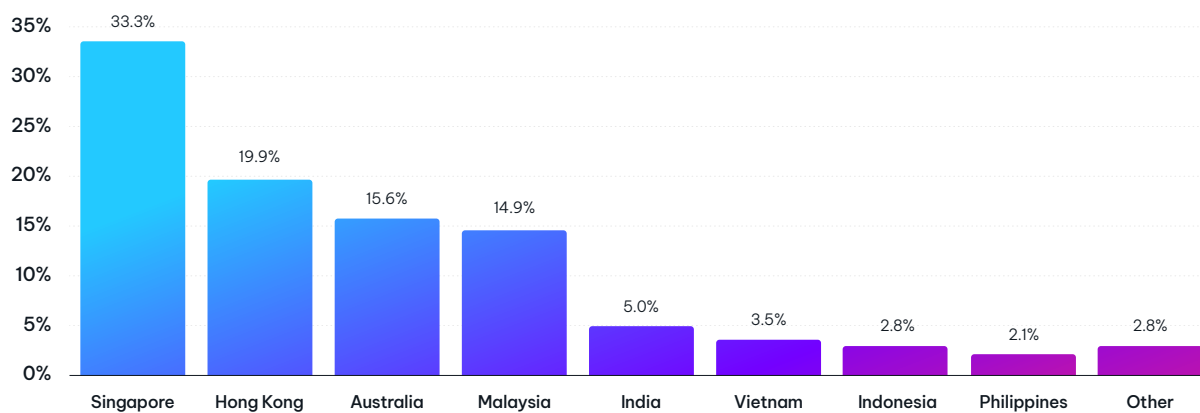
In this paper, the **AML Tech Barometer**, we explore work done by FIs to enhance their financial crime risk management capabilities, based on survey and interview data collected from 289 financial crime and fraud professionals across 12 Asia Pacific jurisdictions. Respondents came from banks, wealth managers, securities brokers, fintech firms, virtual asset service providers (VASPs) and other FI types.

The research explored the current state of technology adoption for AML at FIs in Asia Pacific and the key areas they are prioritising for further development. The paper also considers the challenges experienced in key AML functions and the extent to which FIs are using technology to address them.

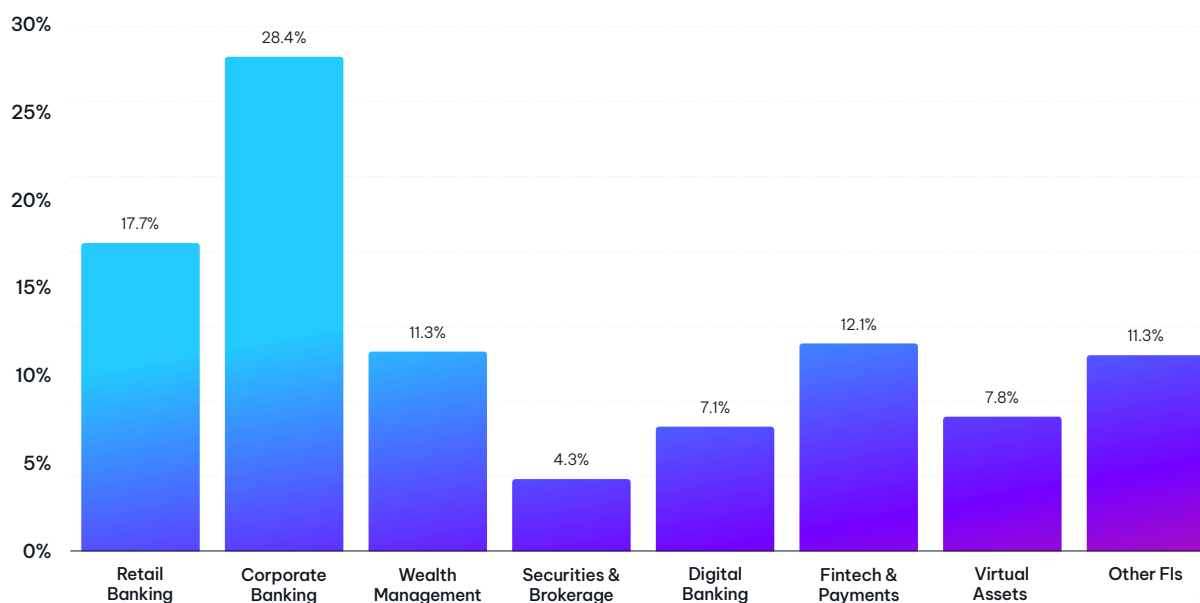
Finally, we look at trends in suspicious transaction/matter reports (STRs/SMRs) to identify key thematic areas of concern for FIs and regulators. The research aimed to establish a benchmark for firms to use to compare themselves against peers and identify gaps for further development.

The AML Tech Barometer 2023 explores work done by FIs to enhance their financial crime risk management capabilities, based on survey and interview data collected from 289 practitioners across 12 Asia Pacific jurisdictions.

Respondents by Jurisdiction



Respondents by Institution Type



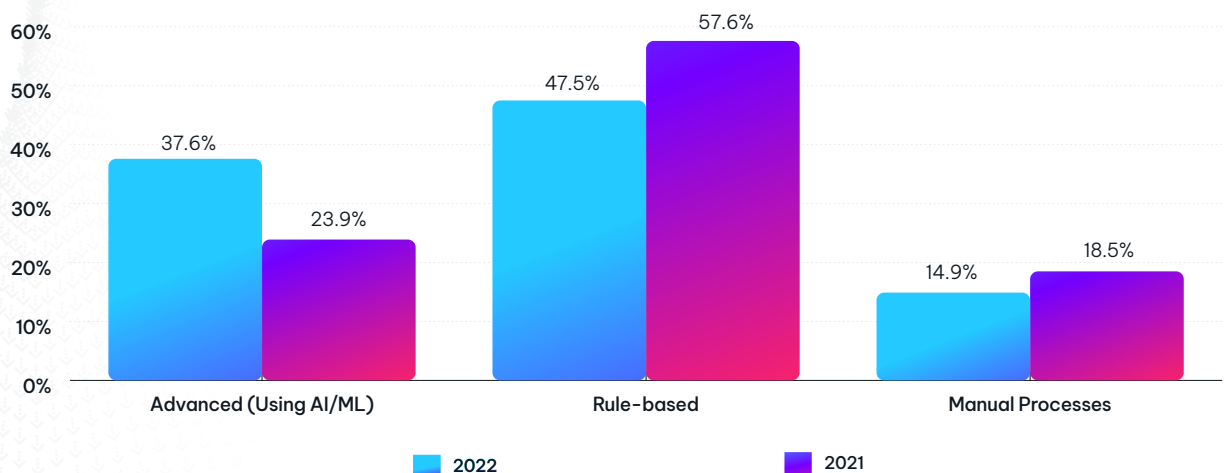
Current State of Tech Adoption for AML

As in [last year's research](#), the survey first sought to benchmark the technological maturity of financial crime risk management systems deployed by FIs in Asia Pacific, asking respondents to describe these systems as mostly 'advanced', 'rule-based', or 'manual'.

Advanced systems were defined as those using business rules as well as AI/ML for advanced analytics or predictive modelling of financial crime risk. Rule-based systems use sets of rules and thresholds to detect financial crime risk. Manual systems are those that would typically rely on less mature solutions such as spreadsheets and human input, with little or no automation.

Notably, the research found that the use of advanced systems is increasing at FIs, with 38% of respondents indicating their use of such systems compared to 24% in 2021. The use of both rule-based and manual AML systems likewise fell in the sample over the same period.

Financial Crime Risk Management System (2022 vs 2021)



The shift towards more advanced systems among FIs points to growing confidence in using AI/ML and increasing maturity of such technologies. According to one respondent, FIs are increasingly applying advanced segmentation and predictive scoring in transaction monitoring, as well as general use of natural language processing (NLP), entity resolution, and network link analysis technologies.

38% of respondents reported using advanced systems that use AI/ML in 2022, compared to 24% in 2021.

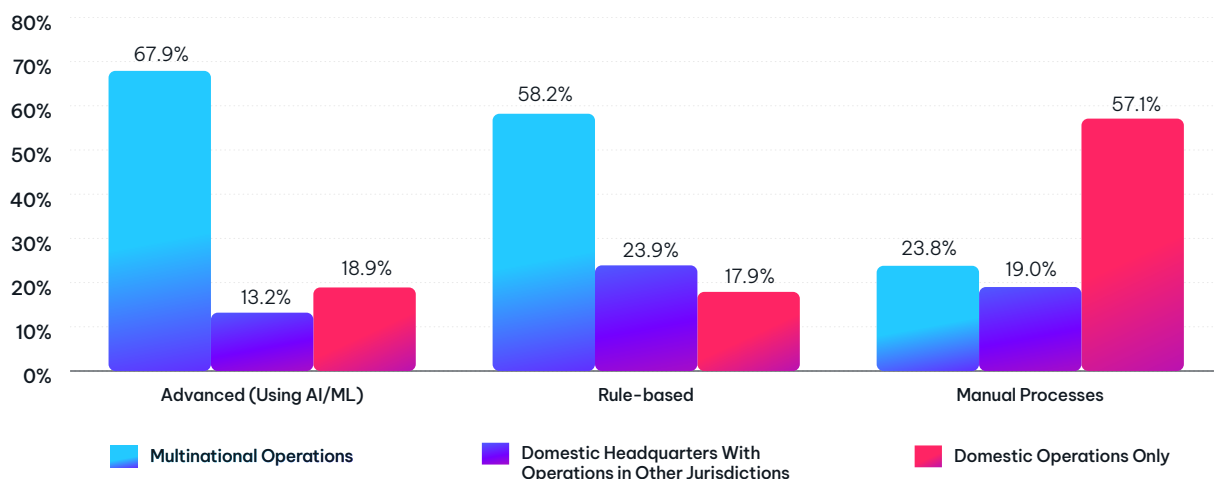
Several respondents noted that regulators have been encouraging the use of such technologies for AML purposes. For instance, the Hong Kong Monetary Authority (HKMA) released a [Regtech Adoption Practice Guide](#) in April 2022 highlighting the benefits of adopting Regtech solutions based on AI. These include more streamlined risk management and compliance processes, reduced manual workloads, and the ability to detect fraud patterns and monitor and analyse large datasets.

Elsewhere in Asia Pacific, the Monetary Authority of Singapore (MAS) has continued to increase its [grant funding](#) for innovative projects, including those involving AI; progressed its [work to assess](#) how FIs are adopting its FEAT Principles (fairness, ethics, accountability and transparency) in their use of AI/ML; and [raised its expectations](#) for banks to use AI/ML to detect suspicious activity connected to scams and frauds.

The research found that the use of advanced and rule-based systems for AML was more prominent among FIs with operations in multiple jurisdictions, reflecting their size and scale, larger volumes of clients and transactions, higher risks associated with cross-border activity, and a need for greater efficiency to maintain regulatory compliance across multiple jurisdictions simultaneously. Likewise, manual systems were most commonly used by FIs with only domestic operations.

According to a respondent from a multinational bank, significant decisions on AML systems “tend to come from the top” (i.e. global headquarters) because “AML issues arising in any branch or subsidiary can have legal and reputational impact at the group level”. Respondents from FIs with domestic-only operations mostly cited a “lack of need” or “constrained budgets” as reasons for not having more automated systems in place.

Use of Financial Risk Management Systems, by Operational Coverage



Interview:

Hong Kong Monetary Authority (HKMA)

Ms Carmen Chu, Executive Director (Enforcement and AML)

Ms Carmen Chu discusses the actions the HKMA is taking to disrupt AML threats to Hong Kong, the impact of increased collaboration across the private and public sectors, and technology initiatives that are making a difference.

What are the biggest AML/CFT threats in Hong Kong and how is the HKMA addressing these challenges?

Carmen Chu: As noted in the Hong Kong Money Laundering and Terrorist Financing Risk Assessment [Report](#), the biggest threats to the banking system continue to be from fraud and mule accounts—driven in part by the rise in online activities—as well as corruption and tax crimes. This is common for international financial centres.

The HKMA has been taking a number of actions to address these challenges, including strengthening collaboration to detect and disrupt fraud and other financial crimes through public-private partnership in the AML ecosystem, keeping our legal and regulatory regime up-to-date and in line with international standards, and encouraging industry adoption of Regtech to help maximise outcomes of AML work.

What impacts have the HKMA's measures to protect banking customers had so far?

Carmen Chu: Fraud and mule accounts remain a key focus for the HKMA's AML efforts. In Hong Kong alone, there were over 19,000 deception cases reported in the first three quarters of 2022, up 40% year-on-year, with losses of around HKD 3.3 billion.

In response to emerging risks, the HKMA and the banking sector have been intensifying AML work and developing innovative approaches to protect the public from losses from fraud and financial crime. We have been achieving good results through our public-private partnership in information sharing and plan to further scale up these efforts in 2023, in terms of both the volume and quality of intelligence as well as the number of participating banks.

Up to Q3 2022, the Fraud and Money Laundering Intelligence Taskforce (FMLIT)—a public-private partnership for information sharing among the Hong Kong Police Force, the HKMA and 23 banks—has identified over 19,000 suspicious accounts

and networks associated with crimes under investigation by the law enforcement agencies, with around HKD 820 million in criminal proceeds restrained or confiscated.

We have also worked with retail banks to develop a 24/7 stop payment service allowing them to offer immediate assistance in intercepting funds whenever a victim reports a fraud to the Police. Most recently, we have worked with the Police, banks and stored value facility licensees on the launch of a search engine called "[Scameter](#)".

This allows members of the public to input information to be checked against databases of information previously linked to scams (including fraudulent websites purported to be hosted by banks) before a transaction is conducted, and is already estimated to have avoided at least HKD 400 million in fraud losses to the public since its launch.

How has the HKMA promoted innovation in the AML space? What progress has been seen so far and what do you see as the next steps?

Carmen Chu: In the face of rising levels of online fraud and financial crime, the HKMA has transformed the way it engages with banks to shape the direction of innovation in AML work; we have been encouraging the wider adoption of technology since the first [AML/CFT Regtech Forum](#) in November 2019.

Our most recent initiative is AMLab, which brings banks and local Regtech firms together in facilitated workshops. The [first AMLab](#) on the use of network analytics to identify fraud mule accounts took place a year ago with five banks, and this theme has just been "encored" in our [third AMLab](#) in November.

Adoption of network analytics by retail banks is progressing well. To date, about 60% of retail banks which are also members of the FMLIT are now deploying network analytics, more than twice as many as three years ago. In the first nine

(Carmen Chu interview continued)

months of 2022, these banks also increased their identification and reporting of suspicious accounts and networks by 127% compared to a year ago, leading to an increase of 166% in the amount of criminal proceeds restrained or confiscated by law enforcement agencies.

My key message is that not only large institutions but also smaller banks can apply AML Regtech techniques and achieve good results, complementing more traditional transaction monitoring systems without incurring high costs or having to recruit large numbers of data scientists.

We will reinforce these messages in the coming months, firstly with a publication specifically focusing on network analytics, including further examples of use cases and guidance on how barriers were overcome, and secondly, with a new initiative to enhance the effectiveness of banks' rule-based transaction monitoring systems which will be rolled out in two phases.

The first phase involves key updates to the HKMA guidance paper on name screening, transaction monitoring and STR reporting to better address recent developments in data and technology. The second phase will cover feedback from thematic reviews we have undertaken together with a leading Regtech firm.

In parallel, the HKMA has also recently started a pilot on the application of data analytics using granular financial crime data across multiple banks for the first time. This will help inform more timely supervisory responses aimed at reducing and preventing serious harm, particularly from mule account networks for fraud and financial crime.

How has work progressed to develop the new bank-to-bank information sharing platform?

Carmen Chu: We are supporting the banking industry in developing a new framework for detecting and sharing early signs of suspicion to complement the existing public-private partnership and public sector initiatives to enhance prevention and detection and, most critically, help stop customers' financial losses from fraud.

Good progress has been made in addressing the legal, cybersecurity and technical challenges of this new bank-to-bank sharing platform, which is targeted to be launched in the coming months.

“In response to emerging risks, the HKMA and the banking sector have been intensifying AML work and developing innovative approaches to protect the public from losses from fraud and financial crime.”

Ms Carmen Chu, HKMA

What new trends can be observed from recent suspicious transaction reports?

Carmen Chu: In line with what we have observed in major international financial centres, the majority (over 80%) of all suspicious transaction reports (STRs) were filed by the banking sector in Hong Kong. The Stored Value Facility sector ranked second, contributing over 8% of total STRs, showing the increasing maturity of controls in the sector.

These STRs continue to provide timely and actionable intelligence for the AML ecosystem, including some previously unknown networks identified using analytical tools. But a big part of the discussion is also about asset recovery, or intercepting fraud related fund flows so we can return them to victims.

The banking sector's ability to intercept fraudulent payments has been enhanced significantly by working with the Anti-Deception Coordination Centre (ADCC) of the Hong Kong Police, which the HKMA has strongly supported. Under the 24/7 stop payment mechanism, the banking industry helped intercept over HKD 2.2 billion in suspected fraudulent payments in 2021.

What should the industry learn from the HKMA's use of its supervisory and enforcement tools?

Carmen Chu: The HKMA deploys a range of supervisory and enforcement tools in a proportionate manner to address concerns identified in our supervisory process. One principal objective is to bring about prompt remedial actions and, where warranted, disciplinary actions will be taken to reinforce the message that banks must have AML/CFT systems that are commensurate with their risks.

(Carmen Chu interview continued)

In recent cases, the lessons highlight the importance of conducting on-going reviews of AML control systems to ensure their design and implementation remain effective. Senior management oversight is also a vital part of an effective ML/TF risk management framework of banks. Proper guidance to staff and clear designation of responsibilities are also crucial.

How does the HKMA view the risk of virtual assets given recent events and what action is being taken to manage these risks?

Carmen Chu: While the HKMA recognises the potential for innovation, the risks associated with virtual assets (VAs) and virtual asset service providers (VASPs) and the need to address them are also becoming better understood. As far as AML is concerned, the Financial Action Task Force (FATF) extended its AML/CFT standards to activities involving VASPs in 2019. Hong Kong, being a FATF member, is currently in the advanced stages of amending its AML/CFT framework to include a [licensing regime](#) for VASPs, which will come into effect in 2023.

The HKMA had responded to VASP sector developments through a [circular](#) in January 2022, addressing both financial crime risks and investor protection, and the approach to be adopted by banks when interfacing with VASPs. In short, the HKMA adopts a risk-based approach to supervising authorised institutions' VA activities in line with applicable international standards and based on the principle of "same risk, same regulation".

"We must have the ambition to deliver our improved processes at a scale and pace which will deliver the right results and a real impact to global financial stability and consumer protection."

Ms Carmen Chu, HKMA

If I were to highlight one area in which the global AML/CFT community is clearly expecting better progress, it would be implementation of the travel rule in accordance with the FATF standards. As risk appetite and the volume of business related to VASPs grows, it will be important to demonstrate full compliance and address challenges regarding interoperability between systems and across jurisdictions. In this regard, the HKMA will continue its active participation in FATF discussions and engagement with the industry and relevant stakeholders.

What should the banking industry understand from the HKMA's AML/CFT initiatives and their impacts to Hong Kong's financial system?

Carmen Chu: We are firmly in a digital era and our financial system, while providing more efficient services, is now more prone to being abused for moving and hiding the proceeds of online fraud and other financial crimes. Everyone—financial institutions, regulators and law enforcement—have to identify and embrace new ways of doing things while closely collaborating with each other.

The most promising areas are data and network analytics, which authorities including the HKMA are applying to AML Suptech. Another is the development of private-private partnerships alongside the existing public-private ones. These initiatives enable banks to collaborate with other stakeholders in the AML ecosystem to spot illicit fund flows more efficiently and share information and intelligence quickly, which leads to more targeted and actionable suspicious transaction reports, and helps to protect the safety and integrity of the financial system and customers from losses.

At a time when the global economy is facing uncertainties and challenges, alongside new developments and opportunities, we must continue to demonstrate the value that banks' AML and financial crime risk management efforts bring to members of the public. And we must have the ambition to deliver our improved processes at a scale and pace which will deliver the right results and a real impact to global financial stability and consumer protection.

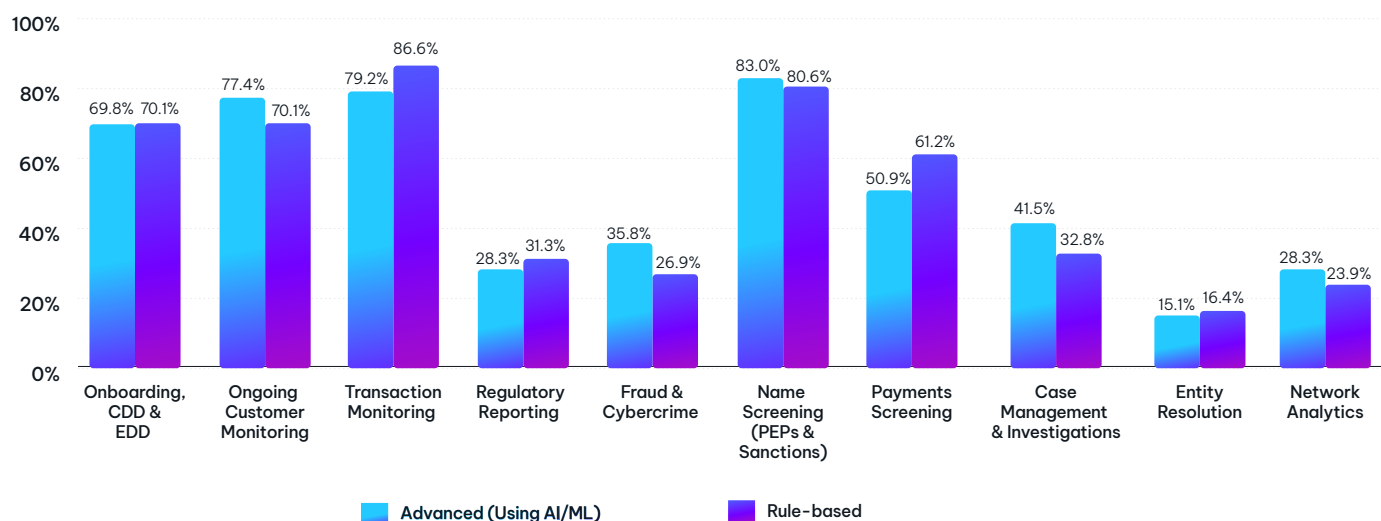
Use of Advanced Technologies

The research highlighted that FIs that have deployed advanced and rule-based systems were most commonly using them to cover transaction monitoring; name screening (PEPs/sanctions); customer monitoring; and onboarding due diligence. In fact, coverage of transaction monitoring and name screening saw a significant increase over the course of 2022.

In 2021, for example, advanced systems covered name screening for just 46% of FIs. The latest data shows that this coverage has increased to 83% in 2022. Respondents suggested that an obvious driver of this has been the wide-ranging sanctions imposed against Russian entities and individuals in response to the war in Ukraine.

“The Russia sanctions came faster and with more complexity than the industry is used to, so many firms were forced to find ways to keep up,” said one respondent from a multinational bank. “Many mid-sized and smaller FIs that didn’t have robust systems to automate screening had to quickly implement external vendor solutions to deal with sanctions risk.”

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



Encouragingly, FIs that had not yet deployed AI/ML as part of their financial crime risk management systems largely indicated that work programmes to do so were either underway or planned. For instance, in transaction monitoring, 44% of respondents indicated they were already using AI/ML; yet 40% more said they had plans to do so. A similar trend was seen in name screening, KYC processes, customer monitoring and other areas.

The research also identified an increase in the use of AI/ML tools for entity resolution and network analytics—two areas more closely studied in this year’s research. For entity resolution, 20% of

The use of advanced and rule-based systems to cover transaction monitoring and name screening saw a significant increase over 2022.

Entity-resolution technology has been helping banks to eliminate duplicate entity records, which provides cleaner and more consolidated records and leads to more accurate and timely risk detection.

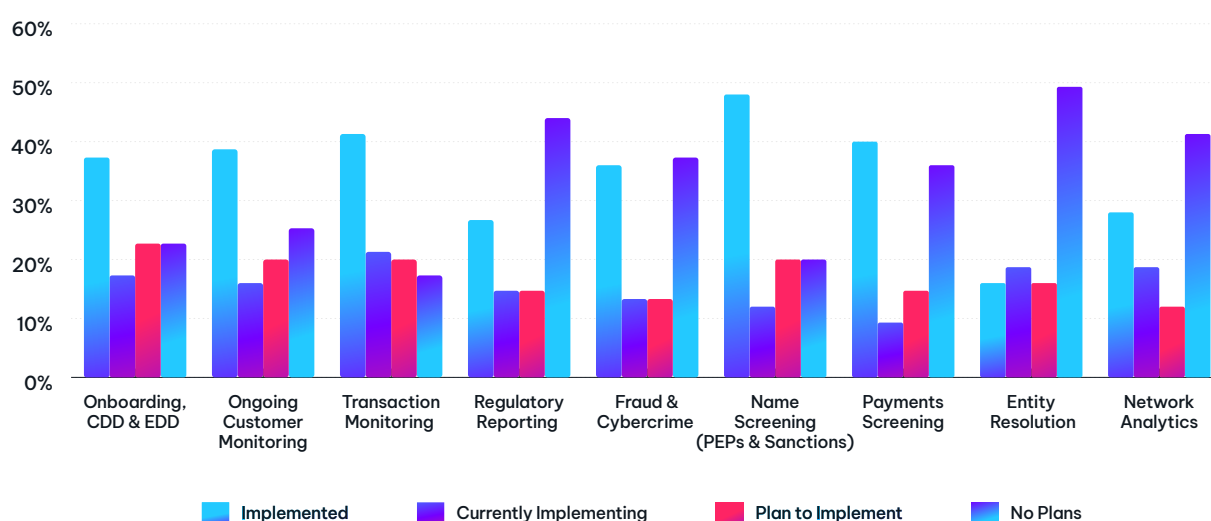
Matthew Field, NICE Actimize

respondents said they have already deployed AI/ML, while 31% indicated their intention to do so. For network analytics, 32% of respondents said they were already using AI/ML, while 31% said they have plans to do so.

Matthew Field, APAC market lead for anti money laundering at NICE Actimize, said entity resolution technology has been helping banking clients “eliminate up to 20 percent of entity records by removing duplicates”, which provides for cleaner and more consolidated records, and leads to more accurate and timely detection of risk in transaction monitoring.

Last year’s AML Tech Barometer report highlighted HKMA initiatives to prioritise the adoption of network analytics capabilities among banks to tackle online fraud and associated mule account networks. This work has since progressed, improving risk identification and reporting of suspicious accounts and networks, and leading to more criminal proceeds being restrained or confiscated. [\[See HKMA interview—page 8\]](#)

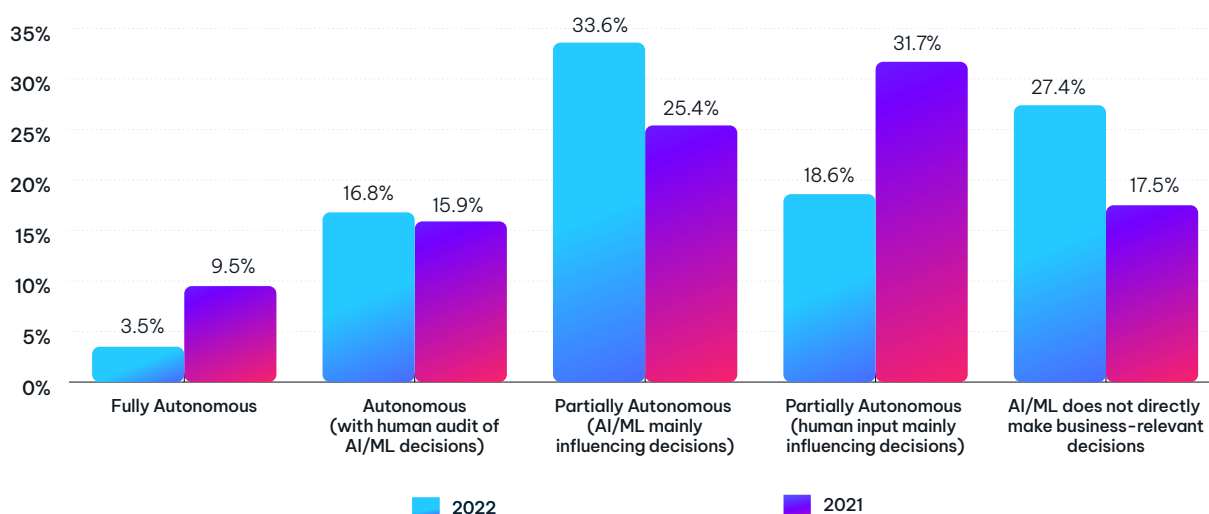
Implementation of AI/ML in Specific AML Functions



The research also revealed a shift in how companies describe their use of AI/ML. Fewer FIs were willing to describe their AI/ML systems as ‘fully autonomous’ compared to a year earlier (10% in 2022 versus 4% in 2021). Respondents preferred instead to describe their AI/ML systems as being only partially autonomous, subject to human audit, or not directly involved in business relevant decision-making.

Some respondents said this suggests some caution in FIs’ use of AI/ML, and highlights a need to ensure that decision-making is subject to stricter governance and oversight. “Our AI system needs oversight and fine-tuning, more so now given how quickly bad actors are changing their methods and techniques. We need to adapt accordingly,” said a Hong Kong bank respondent. “More prudent governance and oversight of AI/ML systems is also what regulators are expecting to see.”

How Autonomous Are Your AI/ML Systems? (2022 vs 2021)



The research also explored the confidence shown by FIs to migrate their AML systems to the cloud. Around a third of respondents said one or more of their key AML processes—such as KYC processes, customer monitoring, transaction monitoring, and name screening—are now in the cloud. In each of these four areas, close to a quarter of other respondents indicated that they were either currently migrating to the cloud or had plans to do so.

“Cloud adoption is an important move because it reduces costs, enables much quicker access to software updates, and removes a lot of the issues that come with managing your own in-house infrastructure setup,” said Adam McLaughlin, the global head of financial crime strategy at NICE Actimize. “It brings an end to 6–12 month implementation timetables, and more importantly reduces the burden of complying with changing regulations on ongoing basis. Cloud deployments also have the added advantage of allowing more efficient information sharing, which enables a federated approach to model development and use.”

“Our AI system needs oversight and fine-tuning, more so now given how quickly bad actors are changing their methods and techniques. We need to adapt accordingly.”

Use of Cloud for Specific AML Functions



Interview:

Australian Transaction Reports and Analysis Centre (AUSTRAC) Brad Brown, National Manager Regulatory Operations

Brad Brown discusses AUSTRAC's continued release of guidance materials, key takeaways from its enforcement actions, the ongoing work to upgrade its reporting system, and efforts to further advance Australia's AML/CTF system.

From an AML/CTF perspective, what risks are AUSTRAC most concerned about and how are they being addressed?

Brad Brown: I would like to suggest there is a more positive outlook, but unfortunately criminals will continue to explore and exploit weaknesses within the financial system to launder their proceeds of crime and in doing so cause harm to the community. We are increasingly vigilant of risks arising from new technologies, new payment methods and new products.

This is why it is so important that businesses take their AML obligations seriously in relation to understanding the risks within their business operations. AUSTRAC continues to provide financial intelligence and expertise to law enforcement and industry to assist in the understanding and efforts to disrupt these risks. Our ongoing positive engagement with domestic and international partners is critical to our success in protecting the community from harm.

Have there been any specific trends that AUSTRAC has observed from SMRs and how are these being addressed?

Brad Brown: Given the broad expanse of businesses that report suspicious activity to AUSTRAC, specific trends are somewhat difficult to call out, however as Australia and other jurisdictions have faced increased cyber-related threats, we have experienced increased reporting of scams and frauds.

AUSTRAC has produced financial crime guides to industry sectors including banking in relation to [preventing the criminal abuse of digital currencies](#), [detecting and stopping ransomware payments](#) and the [misuse of payment fields](#). More recently, AUSTRAC's Fintel Alliance in partnership with the Australian Border Force released a financial crime

guide in relation to [trade based money laundering](#) in Australia.

All of these reports have leveraged law enforcement and industry partners to bring the most contemporary understanding of risks to assist all regulated businesses.

You mention digital currencies, how does AUSTRAC mitigate the financial crime risks commonly associated with these assets?

Brad Brown: AUSTRAC has been quick to work with law enforcement partners and digital currency exchanges to generate information on preventing the criminal abuse of digital currencies. Australia was an early adopter of regulation for digital currency exchanges.

Since April 2018, AUSTRAC has regulated digital currency exchange providers on their compliance with AML/CTF laws. This regulation helps to mitigate the risk of criminals misusing digital currency for money laundering, terrorism financing and cybercrime. AUSTRAC knows that cryptocurrencies have been used in financial and other serious crimes and that global activity and technology continues to rapidly change.

The Australian Government is continuing to explore the wider framework in relation to digital assets and AUSTRAC will provide input to those ongoing efforts.

You've highlighted several new pieces of guidance that AUSTRAC has issued this year. What message would you like this to send to the industry?

Brad Brown: AUSTRAC regulates over 17,000 reporting entities, including banks, credit unions, financial services, gambling, remittance and digital currency exchange service providers and bullion

dealers. The AML/CTF Act requires reporting entities to identify, mitigate and manage the risk that their products and services may be used to facilitate money laundering or other serious and organised crimes.

The overarching messages from our continued release of guidance is firstly for industry to understand and assess the risks they face, not just as a one-off exercise but as a cyclical approach as risks of criminal exploitation are not static. In providing the myriad of financial crime guides and risk assessments arising from AUSTRAC's relationships with law enforcement partners and industry, we see this guidance as a key source of assistance to industry.

Secondly, there are very important AML/CTF obligations relating to understanding the interactions with a customer through the life cycle of that relationship, and it is through good practice application of due diligence and transaction monitoring that industry has the opportunity to protect itself from criminal abuse, protect its customers, and provide significant information to support efforts to disrupt harm in the community.

The intelligence and information shared by the financial services sector is critical in helping AUSTRAC and its partners identify and dismantle criminal networks moving the proceeds of crime through the Australian financial system.

What key lessons should firms be taking away from AUSTRAC's enforcement actions?

Brad Brown: At its most simple, a key takeaway would be that AML/CTF programmes must be a living document, not 'set and forget'. A risk assessment must be alive to new risks arising from products being provided, new customers engaged in those products, and new markets and opportunities the business is engaged in.

“The overarching messages from our continued release of guidance is firstly for industry to understand and assess the risks they face, not just as a one-off exercise but as a cyclical approach as risks of criminal exploitation are not static.”

Brad Brown, AUSTRAC

In circumstances where there are global programmes and operations, risks and obligations specific to Australia need to be documented. Businesses should be actively seeking review, audit and assurance and for that to be more than simply the words on the page but the practices in operation.

AUSTRAC works closely with our reporting entities and expects them all to comply with the AML/CTF legislation. We will take appropriate action where we identify instances of non-compliance which give us concern as to the capability of the business to effectively identify, manage and mitigate its risks, and which therefore exposes the business and the financial system to criminal abuse.

Does AUSTRAC have specific expectations for the industry on technology adoption?

Brad Brown: AUSTRAC expects that when the banking industry is adopting innovative technology and practices that they are acutely aware and have assessed the risks of new platforms and products and that there is strong governance surrounding decisions made as the technology is deployed within the banks AML programme.

Importantly, strong assurance must follow implementation to minimise the risk, and/or identify the risk of unintended consequences, particularly where the technology interfaces with existing legacy technology.

(Brad Brown interview continued)

One of AUSTRAC's own technology initiatives is to upgrade your reporting system. How has this work been progressing?

Brad Brown: AUSTRAC's Reporting Entity System Transformation (REST) programme is well underway and has been providing regular updates through our website on recent activities and upcoming and future areas of focus.

Throughout 2022, there has been significant effort in standardising AUSTRAC international funds transfer instructions (IFTI) reporting schemas to align with the introduction of the ISO 20022 cross-border messaging industry standard which is being rolled out globally from March 2023.

AUSTRAC is very keen to hear from reporting entities wishing to provide feedback on the elements of the programme. Reporting entities can visit our [REST webpage](#), which provides a one stop shop for such feedback.

As part of the REST programme, AUSTRAC is upgrading AUSTRAC Online technology for modern connectivity to allow greater reporting ingestion speed, capacity, and enhanced

user-focused efficiencies and functionality for reporting entities.

New functionality planned within the REST programme includes greater feedback to reporting entities on submitted transaction reports, provision of a secure platform for two-way exchange of information, and delivery of a knowledge base functionality for one stop access to all relevant AUSTRAC information.

Looking ahead, how does AUSTRAC intend to further advance Australia's AML/CTF system?

Brad Brown: AUSTRAC continues to work with the Attorney-General's Department on a range of reforms arising from the Statutory Review of the AML/CTF legislation. In doing so also have regard to changing international standards and the changing criminal threat environment.

We certainly continue to explore options to extend the reach of the AML/CTF regime where appropriate and, following 16 years of the legislative regime, identify legislative provisions that can be streamlined and clarified in order to provide certainty for business and reduce undue impact whilst responding more effectively to new risks, new technologies and new practices.

Just as we do not expect industry to rest on its laurels, the same is true of AUSTRAC. We are continually looking across our regulatory and intelligence operations to ensure we maximise the information made available to us for its value to disrupt money laundering, terrorism financing and serious crime, and its value in supporting how we apply our regulatory tools to assist businesses to comply and act swiftly on areas of non-compliance.

As mentioned earlier we have a substantial programme of transformation to assist in the future reporting and engagement between AUSTRAC and industry.

“AML/CTF programmes must be a living document, not ‘set and forget’. A risk assessment must be alive to new risks arising from products being provided, new customers engaged in those products, and new markets and opportunities the business is engaged in.”

Brad Brown, AUSTRAC

Business and Technology Priorities

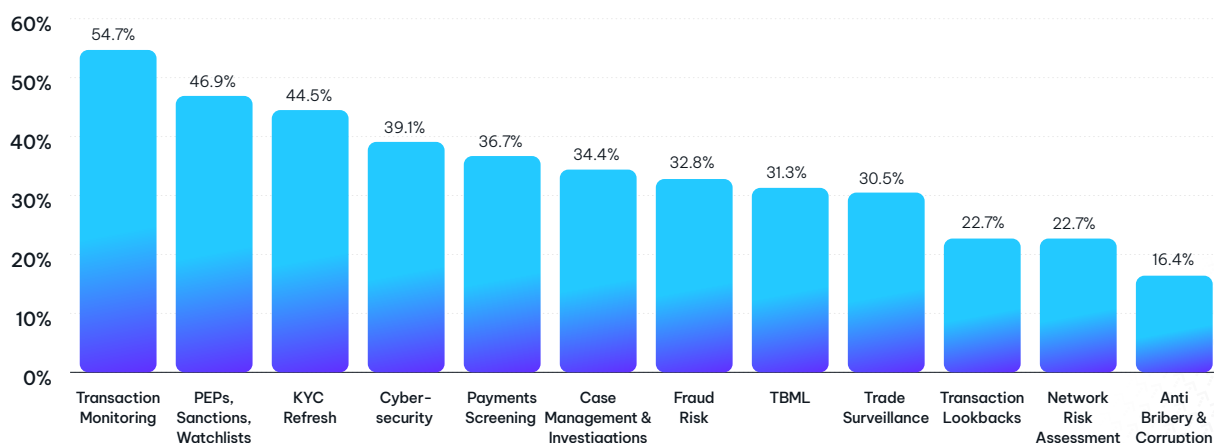
The research sought to understand the key financial crime priorities for Asia Pacific FIs in the next 12 months. The priority areas most frequently cited by respondents for 2023 were transaction monitoring, PEPs and sanctions, KYC data refresh, and cybersecurity—the same top four as in last year's report. For the fifth highest priority, payments screening replaced TBML in this year's report.

PEPs and sanctions appeared to be less of a priority area compared to a year earlier (62% versus 48%), which may not have been expected given the wide-ranging Russia-related sanctions that have been imposed to date.

“Sanctions risk is certainly still a priority, but there is greater certainty on the risk now than earlier in 2022, because FIs have largely already put in place robust processes for screening counterparties and blocking transactions,” one respondent at a Singapore bank explained. “That said, we are increasing our focus on being able to better understand beneficial ownership and counterparty networks to detect sanctions risk as well as money laundering risk, and also trying to improve our handling of alerts.”

The survey indeed found that network risk assessments (25% in 2022 versus 13% in 2021) and case management and investigations (37% in 2022 versus 23% in 2021) were two areas that were considered higher priorities than a year earlier.

Financial Crime Business Priorities for 2023



“Sanctions risk is certainly still a priority, but there is greater certainty on the risk now than earlier in 2022, because FIs have largely already put in place robust processes for screening counterparties and blocking transactions.”

Data management “underpins every good KYC process and is necessary for any reliable analytics.”

As in last year’s report, KYC and onboarding systems were ranked as the top technology priority area for 2023, with respondents citing a need for more streamlined orchestration of the initial collection and verification of a new customer’s information, through to ensuring internal records are “continuously up-to-date, accurate and complete”.

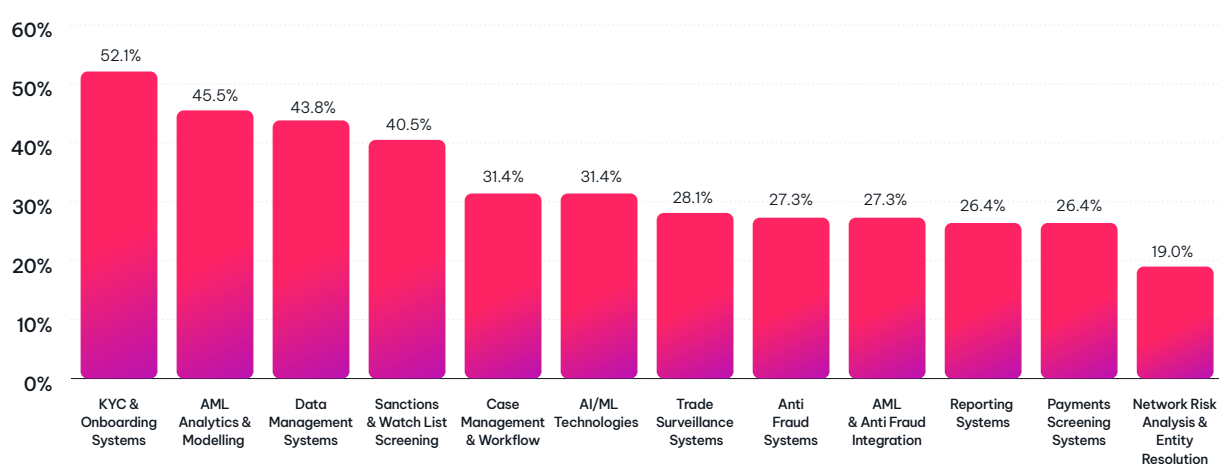
“There are always ways for FIs to improve their onboarding systems and KYC—these are key parts of any financial crime risk management programme,” one respondent said in a follow-up interview. “These improvements can involve integrating fraud detection components such as behavioural and device

intelligence in the onboarding process or subscribing to new external data sources that can automatically flag when a change to a customer’s information has occurred.”

Also like last year, AML analytics was cited as the second highest technology priority for the year ahead, reflecting a need for greater efficiency, more productive alerts, and the ability to analyse customer behaviours, relationships and networks. Data management systems replaced anti-fraud systems as the third highest priority in this year’s research, with one respondent noting “data underpins every good KYC process and is necessary for any reliable analytics.”

Japan’s Financial Services Agency (FSA) has emphasised the need for quality data to support AML processes. The “freshness and accuracy” of customer data is important for detecting suspicious transaction patterns and improving the quality of STRs, the regulator says, adding that enforcement agencies, supervisors and regulators rely on FIs to collect and keep good data. **[See JFSA Interview—[page 19](#)]**

Financial Crime Technology Priorities for 2023



Interview:

Financial Services Agency, Japan (FSA)

Daisuke Mamba, Director and Head of AML/CFT Policy Office

Hiroshi Ozaki, Chief Financial Inspector of AML/CFT

Daisuke Mamba and Hiroshi Ozaki discuss the FSA's approach to its AML/CFT inspections, its expectations on the adoption of technology, and the need for solid risk awareness and good quality data for the risk-based approach to work.

What have been some key observations from suspicious transaction reports (STRs) submitted by Japanese FIs?

Japan's STRs submitted by all obliged entities was more than 530,000 in 2021. It's a vast number, and around 80% come from banks. We have also noticed an increase in STRs coming from Crypto-asset Exchange Service Providers (CESPs) each year since they became obliged entities in 2017. Also, money lending businesses and credit card issuers respectively submitted 6-7% of total STRs.

Another observation is that many STRs are also coming due to increased credit card transactions and cybercrimes. Credit card issuers submitted around 6% of total STRs. In 2021, the damage caused by fraudulent use of credit cards reached JPY 33 billion (USD 242 million) for the year, the largest full-year amount ever. The damage in the first half of 2022 reached over JPY 20 billion, the most ever.

One of the main reasons is the increasing popularity of e-commerce transactions following the COVID-19 pandemic. Cyber-enabled financial crime has increased precipitously in recent years, notably throughout the pandemic. Phishing is prevalent among bad actors, and credit card information is often the target.

What is the FSA's approach to inspections of FIs? What are you looking for when conducting an inspection?

Since last year, FSA started targeted AML/CFT inspections with the Local Finance Bureaus, using a hybrid of on-site and off-site due to the COVID-19 pandemic. We are mainly conducting on-site inspections these days because the Government

loosened movement restrictions. These targeted AML/CFT inspections are the focus from 2021 to 2023 because we've set a deadline that requires FIs to satisfy all the requirements of our AML/CFT guidelines by the end of March 2024.

In the inspections, we are checking on the progress achieved by FIs and to what extent they have filled in remaining gaps between the AML/CFT guidelines and their current practices. So, these are more 'guidance-style' inspections, which are intensive but also friendly and involving a lot of dialogue. We work closely with our Local Finance Bureaus on these targeted inspections at regional financial institutions, other midsize and smaller banks, money remittance businesses, and some CESPs.

The inspections ensure FIs take a risk-based approach in their AML/CFT controls and cover risk identification and assessment, transaction monitoring, and ongoing customer due diligence (CDD). We are also checking on internal control issues, AML/CFT programme governance, PDCA reviews, staffing, and documents against our AML/CFT Guidelines and FAQs. It's very comprehensive.

What are your expectations when it comes to technology adoption for AML/CFT purposes?

Technology is the key to detecting suspicious transactions from flows of data and transactions. Just an eyeball check cannot make this happen. So the technology system is essential, but the investment is also required. Simply implementing a set of scenarios and rules with a solutions vendor doesn't work and produces many false positives. Many FIs face high false-positive rates of over 90 percent from legacy transaction monitoring systems, not just in Japan but across the Asia Pacific. This false-positive issue is a common pain point with legacy transaction monitoring systems.

(FSA interview continued)

In 2020, the Japanese Bankers Association (JBA) conducted a proof of concept (POC) project hosted by the New Energy and Industrial Technology Development Organization (NEDO). JBA aims to develop shared AML systems, including transaction monitoring and screening, using machine learning technology to increase efficiency and effectiveness. Currently, JBA is undertaking a full-scale study for practical application and intends to start a shared AML system around the spring of 2024.

Also, FIs have to combine transaction monitoring and better ongoing CDD of the entire customer list. The freshness and accuracy of that data are vital to check for suspicious transaction patterns. Opening cases for investigation with good data also makes the body of STRs better.

So, ongoing CDD with accurate information and transaction monitoring are the two sides of the coin. So that's why we're asking FIs for ongoing CDD, to have better risk assessments of the client and more effective transaction monitoring.

How will the shared AML transaction monitoring system work for participating FIs?

There might be two options. One option is for a bank to submit the output of its legacy transaction monitoring system, which includes the transaction

data, to the shared platform. The other option is for a bank to submit the transaction data in raw form. In either case, the shared platform will output a score based on the likelihood of the transaction requiring an STR submission with narrative explanations. These options are still under consideration, but the system takes care of detection and triage, and the bank will have to decide whether to submit the STR.

Altogether this will help streamline triage and judgment processes, reducing manual work. When many FIs use the shared platform, it ultimately helps improve transaction monitoring across the industry, and that's what we aim for as a goal.

Given your participation in the work of the Financial Action Task Force (FATF), what key messages would you like to convey to the industry?

The FATF has been putting more weight on law enforcement and its role in asset forfeiture, seizure, and asset recovery. Strengthening asset recovery will be one of the highest priorities for the FATF in the coming two years under the Singapore Presidency, as well as countering illicit finance of cyber-enabled crime. STRs are a vital part of investigations, so we must seek more STRs and more information with better quality.

We'd also like to ask FIs to improve their risk awareness and understanding, whatever the risk. And the point is that FIs are in a dynamic world, not static, and the risk is constantly changing. There are always new typologies, as bad actors constantly change their techniques. But risk awareness is the key. With risk awareness, the risk-based approach can work properly.

Another key message is on data quality. Whatever methodology, technology, or system you use, garbage data produces garbage output. We need good-quality data, and only FIs can collect this data. As enforcement agencies, supervisors, and regulators, we must collect information from FIs; they are the ones facing their customers, so they are the entities that should know the risk and keep good information and data.

“FIs have to combine transaction monitoring and better ongoing CDD of the entire customer list. The freshness and accuracy of that data are vital to check for suspicious transaction patterns.”

Daisuke Mamba and Hiroshi Ozaki, JFSA

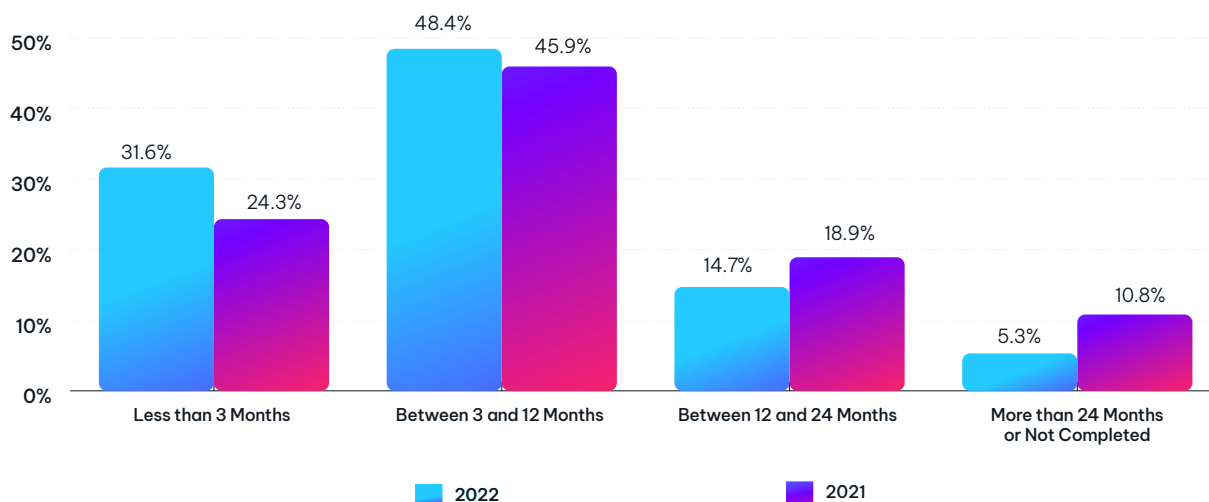
Frequency of Risk Assessments

The AML Tech Barometer survey also identified that some Asia Pacific FIs now carry out enterprise-wide AML risk assessments more frequently. This reflects an increased aversion to risk, a fast-changing financial crime landscape, and pressure from regulators, said one Singapore respondent. “This regulatory expectation may be less emphasised for newer firms like fintech firms and crypto exchanges, and in smaller markets, but overall we are trying to increase the frequency of our risk assessments.”

The survey found that 32% of respondents had conducted their latest AML risk assessment within the previous three months, compared to 24% in the 2021 survey. Over 48% of respondents said their latest assessment was completed within the previous 12 months, compared to 46% a year earlier. Fewer respondents had outdated or uncompleted risk assessments.

“The trend towards more frequent risk assessments is good for the industry as a whole. It means that the risks associated with financial products, services and customers are identified earlier and can be handled before they become bigger issues,” said Adam McLaughlin at NICE Actimize. “It’s worth remembering the importance of data access when it comes to enterprise-wide risk assessments. You cannot have data siloed off. Customer data, fraud risk data, AML data, and increasingly ESG data—this all needs to be accessible for your risk assessments to be effective.”

When Was Your Last Enterprise Wide Risk Assessment for AML? (2022 vs 2021)



“The trend towards more frequent risk assessments is good for the industry as a whole. It means that the risks associated with financial products, services and customers are identified earlier and can be handled before they become bigger issues.”

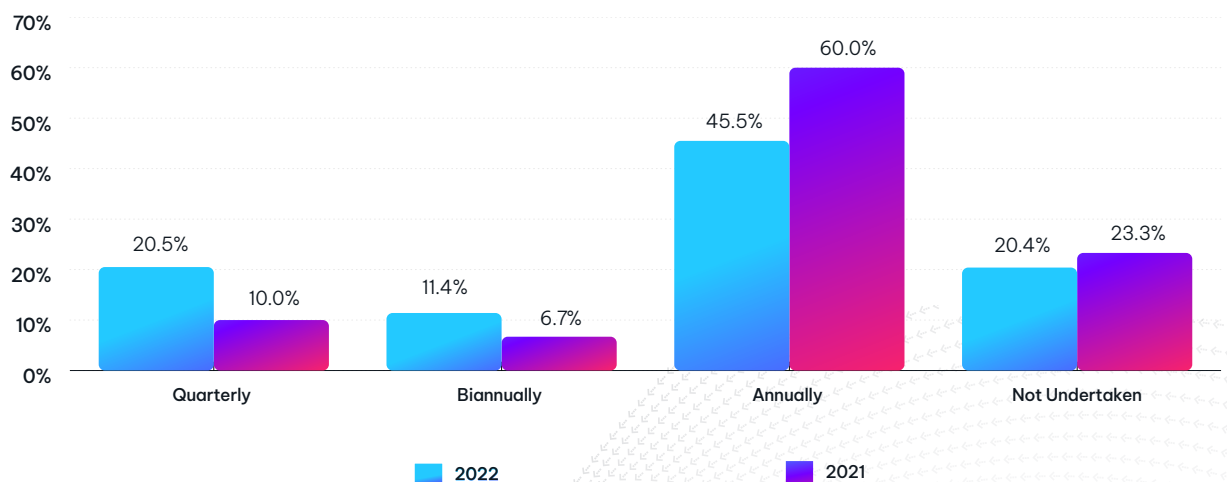
Adam McLaughlin, NICE Actimize

‘29% of respondents indicated that they had noticed either a ‘moderate’ or ‘significant’ increase in TBML-related activities in the previous 12 months.’

Notably, risk assessments of FI’s trade finance businesses are also being carried out more frequently. Of the respondent FIs with active trade finance businesses, 21% carry out risk assessments quarterly, compared to just 10% a year earlier. Around 11% do so biannually, compared to 7% a year earlier.

The results reflected an increased perception of risk in the trade space. Indeed, 29% of respondents indicated that they had observed either a ‘moderate’ or ‘significant’ increase in TBML-related activities in the previous 12 months. According to the respondents, the biggest challenges facing trade finance businesses were related to paper-based documentation, difficulties detecting trade misinvoicing, and dealing with hidden relationships between trade counterparties.

Risk Assessment Frequency, Trade Finance Activities



Interview:

RUSI's Centre for Financial Crime and Security Studies (CFCS) Tom Keatinge, Founding Director

Tom Keatinge discusses the continuing focus on fraud and scams in Asia, work underway to improve global asset recovery mechanisms, the alignment of jurisdictions to Western sanctions, and efforts to target different types of environmental crime.

If you had to pick one financial crime theme as the focus of your work for the next 12 months, what would it be?

Tom Keatinge: I've been really struck in my recent conversations in Asia—including Singapore, Hong Kong, Taiwan, Malaysia—by the extent to which the financial crime dialogue has been completely suffocated by scams and frauds. This is similar to what we see Europe and the UK.

We started looking at fraud more closely in 2019. In January 2021, we published a paper, "[The Silent Threat](#)", about the way in which fraud had gone from being a petty crime to being a serious organised crime. It has clearly become industrialised, and it's become a social issue.

And the challenge with scams and fraud is that it happens at speed—money moves from bank to bank to bank and then out of the country very quickly. On top of that, technology allows fraud to occur at an industrial scale. So, if I were to pick one topic to focus on for the next 12 months, it would be fraud.

How are the private and public sectors responding to the fraud threat? And what can be done to better protect financial consumers?

Tom Keatinge: Banks are responding by merging their fraud and AML departments, so you start hearing about so-called 'FRAML' departments. The thing about fraud is that there's no question of suspicion when a fraud occurs. And a lot of the barriers that would typically limit the ability to pool information between different organisations don't exist.

For example, in the U.K., there's a fraud prevention service called [Cifas](#), which works as an aggregation mechanism for fraud cases. It's meant to try and have an 'all seeing eye' about the types of fraud that are emerging, so it can then alert its member banks, other private sector entities, and some government agencies.

I do think there is more that we can get out of technology in this area, such as solutions that can overlay payments data with analytics to identify suspected mule accounts and map the movement of stolen funds. There's definitely a role for technology. Frauds and scams use technology against their victims, so we ultimately need to use technology against the fraudsters.

We also need much more recognition of and engagement with the problem from the technology companies, such as internet search providers, social media platforms, web domain companies and telecom network providers. What are these companies doing to try and reduce the extent to which individuals are exposed to potential scams such as through advertising? They are often the conduit for scams, so the focus cannot just be on banks to step up from the private sector.

There's a lot more we can do to strengthen the perimeter, but there will inevitably be frauds that are successful. So then you need to focus on the second line, which is investigating, tracing the funds, and recovering the stolen assets—often from other jurisdictions. That's the responsibility of governments.

"The tooling around asset recovery in most parts of the world is probably a decade out of date. Often, they don't recognise the role technology plays today, or the way in which financial payments have changed."

Tom Keatinge, RUSI

(RUSI interview continued)

What mechanisms are in place to facilitate asset recovery when funds are stolen by fraudsters and other bad actors? And what more needs to be done in this area?

Tom Keatinge: One of the focuses of the Singapore FATF presidency for the next two years is asset recovery. This includes trying to reboot Carin [[Camden Asset Recovery Inter-agency Network](#)]. In various regions of the world, there are Carin hubs, which are meant to try and coordinate asset recovery in their region and then coordinate between each other. For example, if there is a scam in Asia that is coming out of Africa, then those two hubs would work together to try and coordinate a response around asset recovery.

Unfortunately, the tooling around asset recovery in most parts of the world is probably a decade out of date. Often, they don't recognise the role technology plays today, or the way in which financial payments have changed. So, there's a lot to be done on asset recovery, such as updating legislation and response mechanisms, and especially promoting better international cooperations and information sharing.

The majority of cases will involve trying to recover assets from other jurisdictions, so countries need to have good mutual legal assistance treaties in place which enable them to trust each other, share information, and be willing to collaborate to respond to another country's challenges.

“Banks in the West are asking whether they should be putting in place extra controls to check if their clients are counterparties in jurisdictions that have chosen not to align with Western sanctions on Russia.”

Tom Keatinge, RUSI

This year we've seen significant international cooperation on sanctions. Where do you see sanctions risk intersecting with AML?

Tom Keatinge: When it comes to sanctions, some countries have chosen to align themselves with Western sanctions regimes in a way they hadn't done before—Singapore being the example everyone points to. But others have not. This is interesting because the U.N. process for designations appears to be broken at the moment, so countries are left to operate autonomously or create alliances.

From a European perspective, it was interesting to see the Russian superyacht, Nord, in Hong Kong in October. That's an asset that should be frozen, but Hong Kong [allowed](#) it to come and go; what does this attitude to sanctions implementation say to Western financial institutions operating in Hong Kong that have a global sanctions policy in place?

This is a question that is coming up increasingly in Western countries: how to respond to jurisdictions that are not aligned with the sanctions on Russia? Financial institutions in the West will become increasingly concerned that the banks and trading companies they're dealing with in Hong Kong could also be handling Russian money or serving as fronts for Russian trade.

From an AML perspective, banks in the West are asking whether they should be putting in place extra controls to check if their clients are counterparties in jurisdictions that have chosen not to align with Western sanctions on Russia, and whether they could be exposed to sanctions evasion as a result.

What other financial crime challenges are you seeing regulators and policymakers trying to address? And in what areas should they be doing more?

Tom Keatinge: The big focus in recent years has been on non-state based threats. But increasingly you see states using financial measures as ways of either gaining legitimate influence or trying to exert malign influence. Over the last year we've been looking at how Western governments should be

considering financial flows coming from places like Russia, which are not necessarily the proceeds of crime, but they may have a malign intent.

The reason why this is interesting is that the existing AML system is almost entirely set up to identify the proceeds of crime (the exception being some forms of terrorist financing), and money that comes to exert state influence is not obviously the proceeds of crime. So for banks, this is not typically the way in which their financial crime units work. Our research in Europe shows that banks are finding it quite difficult to figure out how to get their arms around this challenge.

One topic that appears to have vanished from the priority list is terrorist financing. Fortunately, terrorist attacks in Europe have dropped dramatically in the past two to three years. But with that, the focus on terrorist financing has gone from being a key part of the counterterrorism response to a technical matter pursued to get past FATF evaluations. In a recent [article](#), I argue that policymakers and political leaders need to continuously be assessing ways to strengthen defences against terrorist financing.

Another observation I would make is that the pandemic impact on public-private partnerships in Asia has been more meaningful than in the West, because of the more cautious approach taken in the region. This matters because Asian financial hubs are key conduits facilitating the flow of global illicit finance. For example, Malaysia's MyFINet [Malaysia Financial Intelligence Network] launched in late 2019, but collaborative work has inevitably suffered over the last couple of years. This is an area where we need a post-pandemic reboot.

What are your views on efforts made to combat the various types of environmental crime and how could they be improved?

Tom Keatinge: Environmental crime and wildlife trafficking are areas where the public sector needs to do more. There's a lot of effort and energy in the private sector, but I'm not sure it is being matched by the public sector authorities such as FIUs and financial investigators. Banks can't arrest people or gather evidence

“The private sector may have more luck identifying environmental crime in areas where there are corporate structures behind the illicit activities—for example illegal fishing or timber trafficking and deforestation”

Tom Keatinge, RUSI

for prosecutions. So for countries that are destination or transit countries like Hong Kong or Malaysia—I would ask whether our energies are being focused in the right areas.

In my view, the private sector may have more luck identifying environmental crime in areas where there are corporate structures behind the illicit activities—for example illegal fishing or timber trafficking and deforestation—rather than the singular focus on the illegal wildlife trade. Furniture manufacturers and construction companies are using timber, so they need to be checking where their timber is coming from, and banks facilitating the payments need to be doing the same.

Another area we are focused on is Illegal, unreported and unregulated fishing (IUU), which was also a key focus of the APG's [annual topologies report](#) issued in August. At CFCS, we have likewise been [expressing concerns](#) that the FATF has not placed more emphasis on IUU fishing as part of their environmental crime focus. Vessel ownership information, bank due diligence—these are parts of the AML system that are already set up to deal with these kinds of corporate level environmental crimes.

We've also recently published an [article](#) about the corruption risks related to the transition to net zero, which is where you're likely to see a connection between AML and ESG. Currently there is a big focus at the G20 on trying to ensure there isn't corruption in, for example, green energy projects that rely on partnerships between the public and private sector. We hope political leaders prioritise these types of risks.

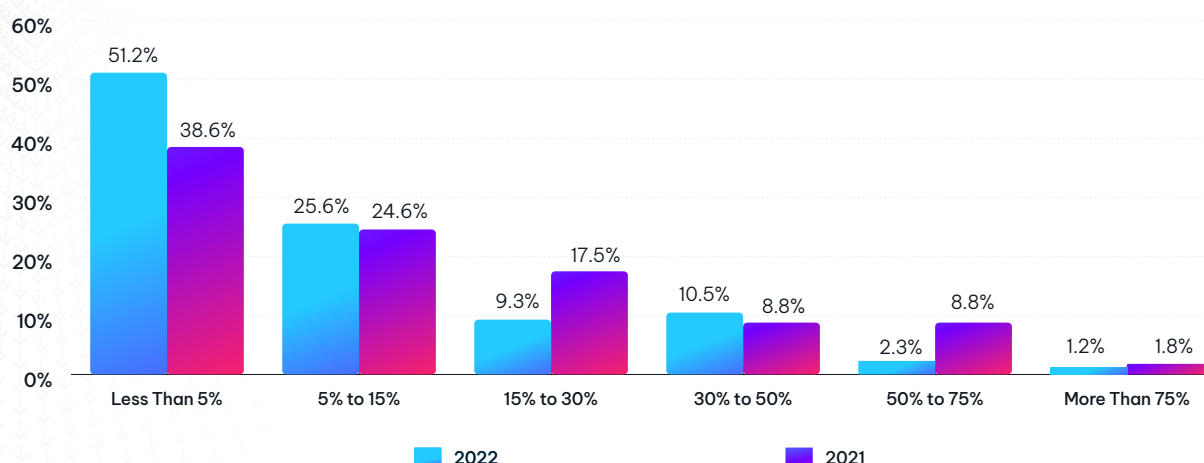
Transaction Monitoring & Screening

The research identified high false positive rates in transaction monitoring and screening systems as a continuing issue, to an even greater degree of severity than in the previous report. This was attributed by some respondents to larger transaction volumes in an increasingly digital environment, and a need to set tighter thresholds given the fast-changing risk landscape, which “throws up more red flags”.

Participants were asked to estimate the percentage of alerts that are ultimately escalated. The alert-to-case ratio was reported to be lower than 15 percent for 77% of respondents, compared to 63% a year earlier. Just 9% of respondents reported ratios between 15–30 percent, compared to 18% a year earlier. The results show that the proportion of alerts generated in 2022 that were not eventually converted to investigations or STRs/SMRs was higher than in 2021.

“We can escalate fewer alerts because we have been casting a wider net in our monitoring, in recognition that in the current environment there are always new risks we have to take into account as criminal actors evolve their techniques,” explained one respondent at a regional bank. “Naturally, this leads to more alert volumes, and many of these don’t result in any escalation.”

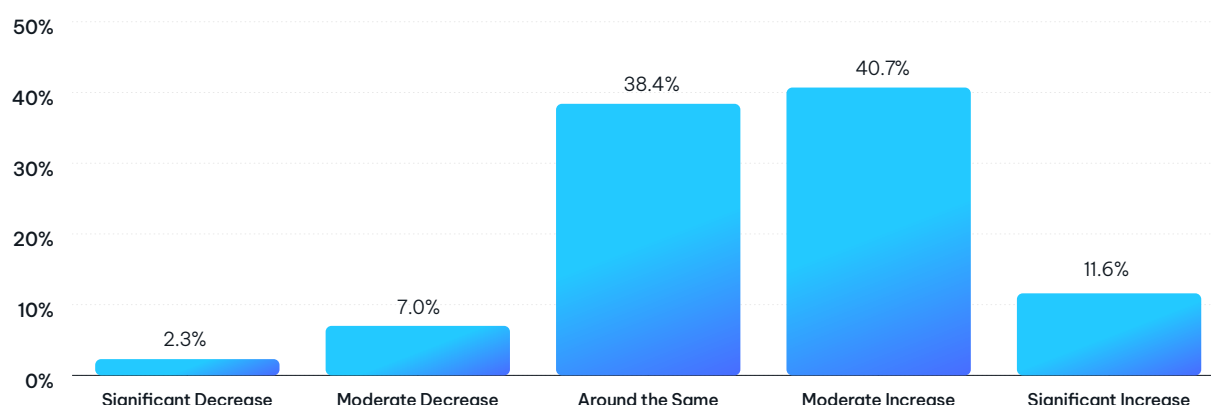
Alert-to-Case Ratios, 2022 vs 2021



Indeed, more than 52% of respondents said their transaction monitoring alerts increased over the previous 12 months, compared to just 9% who said their alerts decreased. The rest of the respondents said their alert levels remained about the same. Several respondents commented that they expect alert volumes to continue to increase in the coming year. “The continuing challenge moving forward will be on remediating false positives and improving the quality of our alerts,” said one respondent from a retail bank.

“We can escalate fewer alerts because we have been casting a wider net in our monitoring, in recognition that in the current environment there are always new risks”

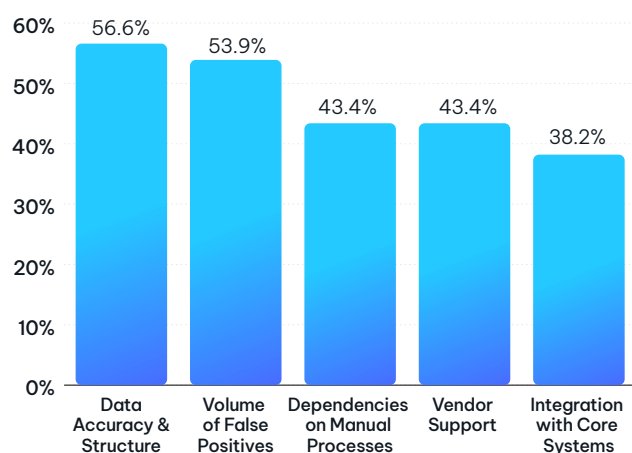
Change in Transaction Monitoring Alerts (Past 12 Months)



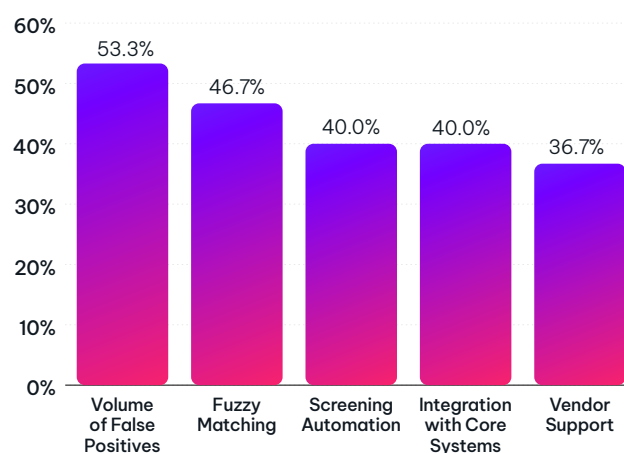
Moreover, high false positive rates were cited as a top factor—and to a greater degree than a year earlier—influencing confidence in transaction monitoring (54% in 2022 versus 39% in 2021) and screening (53% in 2022 versus 43% in 2021) systems. Other important factors impacting how confident respondents were in their transaction monitoring and screening systems were related to automation capabilities, vendor support, and their ability to integrate with core systems.

“Firms should be careful not to try to boil the ocean across all aspects of their AML process, but instead adopt an [‘Entity Centric’ approach to AML](#),” says NICE Actimize’s Matthew Field. “This means addressing each building block of your AML programme in a systematic manner, with a focus on ensuring each entity is fully understood and monitored for the right money laundering risks all the time. This helps to boost alert accuracy, cut down on false positives, and ultimately identify truly suspicious events earlier and with greater precision.”

Factors Influencing Confidence in Transaction Monitoring Systems



Factors Influencing Confidence in Screening Systems



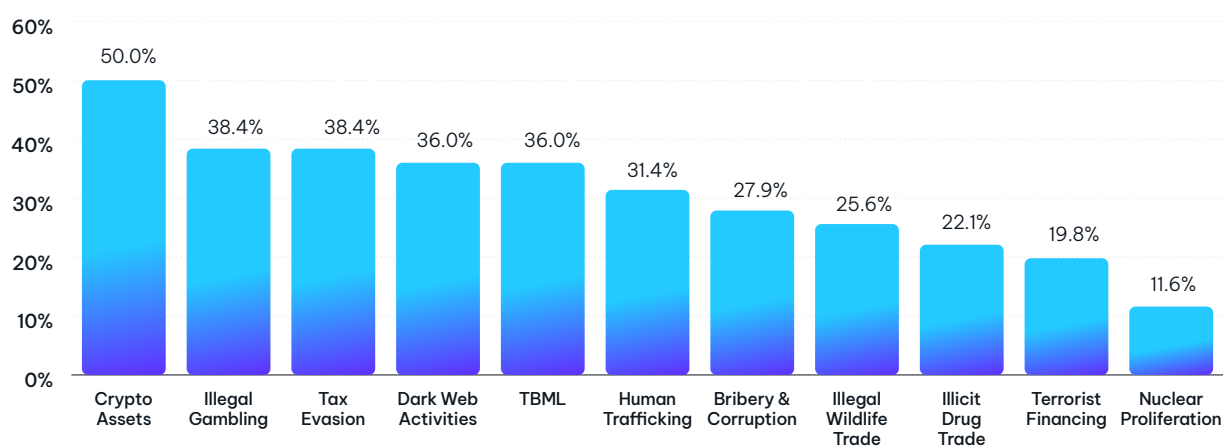
Trends in Suspicious Transaction Reporting

The research also sought to identify the areas where FIs were seeing increased focus and subsequent reporting of suspicious activity and transactions. Cryptocurrency-related activity was the top trend in STRs/SMRs for 2022, cited by around half of the respondents as an area of increasing activity. Other notable areas that led to increases in STRs/SMRs during 2022 were tax evasion, illegal gambling, dark web activities, and TBML—areas which were also among the most active areas cited by respondents a year earlier.

Concerning crypto, almost 25% of respondents said they have already adapted their systems to detect crypto-specific behaviours and typologies and perform related analytics on such activities. More than 35% of respondents said they were considering doing the same.

“You don’t know what you don’t know, so the detection of high risk crypto-related behavioural activity continues to be important to all firms,” said Matthew Field at NICE Actimize. “Even firms with no direct crypto activities are increasingly needing to become experts in both on- and off-chain monitoring and due diligence.”

Areas of Increased Activity in Suspicious Activity Reporting



In April 2022, AUSTRAC published a financial crime guide providing behavioural and financial indicators to help regulated entities recognise and report illicit transactions involving digital currencies. Since April 2018, digital currency exchange providers in Australia have been required to comply with the country’s AML/CTF laws, which AUSTRAC says has helped to mitigate the risk of digital currency misuse. [\[See AUSTRAC interview—page 14\]](#)

Looking Ahead

As we look to the year ahead and a looming global recession, the focus on the linkages between fraud, cybercrime and money laundering are likely to increase. Moreover, regulators will continue to target perceived weak links in the risk coverage of AML/CTF programmes and encourage the use of innovative technologies to enhance risk detection efficiency and effectiveness.

With a focus on geopolitical tensions and economic instability, the past year was not considered a standout year for AML enforcement activity, especially compared to 2020, which saw large penalties issued in Australia and Malaysia. Rather, in a trend expected to continue, Asia Pacific regulators are intensifying their AML supervision and inspection work, adopting a more collaborative approach that focuses on outcomes rather than outright punitive action.

We have seen a number of regulators, including the HKMA, AUSTRAC and FSA, focus their efforts on providing guidance and recommendations to the industry to facilitate AML compliance, establish best practices and promote scalable compliance frameworks that can capture new risks as and when they emerge, rather than engage in headline-grabbing enforcement actions to punish non-compliance.

In line with this approach, FIs that cooperate with their supervisors and are willing to invest in improving their systems and governance will be best placed to avoid large penalties for deficiencies in their AML programmes. That said, FIs will need to brace for the repercussions of sanctions non-compliance. Complicated by a rapidly evolving geopolitical landscape, the fallout—which includes reputational damage, financial losses, and potentially large fines—will be a key catalyst of change for the next several years.

Other themes likely to resurface in the coming year include a refocusing by regulators and law enforcement on areas such as terrorist financing, transnational organised crime, human trafficking and wildlife trade. The proliferation of frauds and scams, and the money mules that enable them, will also continue to be a major focus for most Asia Pacific jurisdictions, as will crypto-related crime.

In the past year across Asia Pacific, information sharing and public-private partnerships continued to strengthen. The same was true for Europe, however [recent developments](#) have shifted the focus for the coming year to finding a balance between public access to beneficial ownership information and the right to privacy enshrined in EU law.

Meanwhile, with ESG issues continuing to dominate policy and industry discussions, the expectation for the year ahead is for environmental crime to be brought into greater focus in AML programmes. Financial crime typologies, adverse media, and other AML data will increasingly be duct-taped together and repurposed to detect ESG-related risks.

Considerable progress has already been made in this regard, with FIs already accounting for ESG issues in their AML risk assessments. This is expected to become further entrenched in the year ahead, with an increased focus on customer supply chains and corruption risks associated with green projects. **[See Interview Box 4: RUSI—page 23]**

We live in an age of continuous and rapid evolution of the financial crime risk landscape. Bad actors have become quicker than ever before, including in how they innovate new techniques and tools to exploit weaknesses in the financial system. As an industry, we must continue to be vigilant of emerging risks.

As this research shows, FIs across Asia Pacific have continued to demonstrate their resolve to innovate and use advanced technologies to detect financial crime and prevent bad actors from exploiting their services. While technology is not a panacea, we can be certain that innovation in the AML space will continue to be one of the best strategies we have in the ongoing battle against financial crime.

We are also encouraged by increasing public-private collaboration and information sharing to identify and disrupt financial crime threats. While much of this collaboration occurs behind the scenes, there are obvious signs of progress, which will ultimately lead to a safer, more resilient, and robust financial ecosystem.

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 financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumer and investor 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 concerns such as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

Find us at www.niceactimize.com  [@NICE_Actimize](https://twitter.com/NICE_Actimize)


Get in touch

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

Adam McLaughlin
Global Head of Financial Crime Strategy
NICE Actimize
Adam.McLaughlin@niceactimize.com

About Regulation Asia

Regulation Asia is the leading source for actionable regulatory intelligence for APAC markets. Through our news, events, and research, we serve over 30,000 financial services professionals from more than 1,000 financial institutions, as well as regulatory bodies, exchanges, technology firms and other service providers.

www.regulationasia.com  [@RegulationAsia](https://twitter.com/RegulationAsia)