Plenitude
Inspiring confidence, delivering excellence

RegIntel: 2024 Recap and 2025 Outlook Report

Executive Summary

In this year's edition of Plenitude's RegIntel report, our Regulatory Intelligence team provides an in-depth review of financial crime regulatory developments throughout 2024 and anticipates potential changes on the horizon for 2025. This paper covers critical regulatory advancements across four leading global financial jurisdictions: the United Kingdom, European Union, Hong Kong, and Singapore.

The report explores significant legislative, regulatory, and industry updates across the core anti financial crime areas such as, anti-money laundering (AML), counter-terrorist financing (CTF), counter-proliferation financing (CPF), fraud prevention, sanctions compliance, and enforcement actions from regulators.

This report is designed to assist financial crime compliance (FCC) teams in navigating the ever-evolving regulatory landscape, staying informed of new and amended requirements, and adopting best practices aligned with industry standards.

With the election of the Labour Party in early July, the United Kingdom's regulatory focus transitioned from the Conservative government's anti-fraud blueprint—addressing payment fraud, corporate criminal liability, and fraud prevention, outlined within their Second Economic Crime Plan 2023–2026—to Labour's redoubled efforts against corruption and money laundering. Despite the change in political hue, both parties have remained resolute in their shared commitment to address fraud, both domestically and internationally, reflecting a consistent cross-party resolve.

The European Union has made notable progress in strengthening its regulatory framework, setting a global benchmark in key areas of governance. With the European AI Act now in force, the EU has set a new global standard for artificial intelligence, striking a delicate balance between fostering innovation and safeguarding societal values. In tandem, France also reinforced its financial crime prevention framework, tightening transparency requirements under the Monetary and Financial Code. Additionally, the EU's comprehensive anti-money laundering and counter-terrorist financing reforms—embodied in the Sixth Anti-Money Laundering Directive, the 'Single Rulebook', and the AMLA Regulation—have fortified the Union's commitment to tackling financial crime with a unified and robust approach across member states.

In 2024, Hong Kong spearheaded regulatory innovation, exemplified by initiatives such as the AML/CTF Surveillance Capability Enhancement Project (AMLS) and the HKMA's public consultation on information sharing —both of which reflect a decisive commitment to strengthening regulatory frameworks and leveraging RegTech solutions.

spearheaded regulatory innovation, exemplified by initiatives such as the AML/CTF Surveillance Capability Enhancement Project (AMLS) and the HKMA's public consultation on information sharing —both of which reflect a decisive commitment to strengthening regulatory frameworks and leveraging RegTech solutions.

Similarly, throughout 2024, Singapore further cemented its position as a global financial hub with the introduction of key legislation, and initiatives aimed at bolstering its anti-money laundering (AML) and financial crime frameworks. Notably, the Anti-Money Laundering and Other Matters Bill expanded regulatory requirements for financial institutions, enhancing due diligence and reporting obligations to better combat money laundering and terrorism financing Similarly, throughout 2024, Singapore further cemented its position as a global financial hub with the introduction of key legislation, and initiatives aimed at bolstering its anti-money laundering (AML) and financial crime frameworks. Notably, the Anti-Money Laundering and Other Matters Bill expanded regulatory requirements for financial institutions, enhancing due diligence and reporting obligations to better combat money laundering and terrorism financing.

Both Hong Kong and Singapore placed a premium on cross-sector cooperation and the integration of advanced technologies to address emerging threats, such as cyber fraud and vulnerabilities arising from digital assets. As we look to 2025, the emphasis in Asia's key financial hubs will undoubtedly pivot towards aligning cutting-edge technological advancements with robust regulatory frameworks, ensuring that firms are not only prepared to meet heightened regulatory scrutiny but also equipped to adapt to the evolving complexities of operational demands.

This report foresees continued regulatory evolution, particularly in relation to emerging technologies and the growing risks of international financial crime. As such, firms must stay vigilant and agile, ensuring their compliance frameworks are adaptable to the shifting global landscape. Providing critical insights into the regulatory developments of 2024, this RegIntel report also offers strategic foresight into the trends and challenges expected to shape 2025. Financial institutions must take proactive measures to adjust to these changes, positioning themselves to navigate an increasingly complex and interconnected financial system.

Throughout 2024, regulatory scrutiny on financial crime prevention has intensified, imposing stricter compliance requirements on firms across key jurisdictions. As we move into 2025, the regulatory landscape will be defined by a heightened commitment to accountability and corporate responsibility, notably through the introduction of the Failure to Prevent Fraud (FTPF) offence in the UK, compelling firms to adopt stronger internal controls. Simultaneously, the full implementation of the Markets in Crypto-Assets (MiCA) Regulation will solidify a comprehensive framework for digital asset oversight across Europe, reinforcing transparency and compliance. As regulatory bodies intensify their focus on emerging technologies like AI, 2025 will usher in an era of greater integration, collaboration, and sophistication in the global fight against financial crime.

> **Financial crime, including fraud and money laundering, does enormous damage. It harms consumers and businesses, and undermines trust in our financial system.**
>
> Emily Shepperd, FCA COO

1 Introduction

As we approach the close of 2024 and look towards the regulatory horizon of 2025, the financial crime prevention and compliance domain finds itself amidst a period of profound transformation. This evolution is, in large part, driven by rapid advancements in technology, particularly in the realms of artificial intelligence and machine learning, which—similar to the emergence and proliferation of cryptocurrency and digital assets—are transforming the design, implementation, and enforcement of regulatory frameworks, thereby necessitating new approaches to governance, security, and compliance.

This report provides a comprehensive overview of the key regulatory developments that influenced international regulations across the United Kingdom, the European Union, France, Hong Kong, and Singapore. These changes, while diverse in their geographic scope, reflect a converging trend towards heightened accountability, technological integration, and an ever-expanding global regulatory framework targeting financial crime in its many forms.

In the United Kingdom, 2024 was marked by a series of pivotal reforms aimed at fortifying anti-money laundering, counter-terrorist financing, and counter-proliferation financing (AML/CTF/CPF) measures. These changes were driven by an ever-evolving landscape of global risks, from the relentless rise of cybercrime and the transformative threats posed by artificial intelligence and machine learning, to the increasingly volatile geopolitical environment, marked by escalating tensions in the Middle East and Russia's persistent defiance of NATO. In this context, the UK renewed its commitment to the Financial Action Task Force (FATF) standards, with an enhanced focus on high-risk jurisdictions and Politically Exposed Persons (PEPs).

At the same time, the Financial Conduct Authority (FCA) continued to refine its supervisory approach, spotlighting common control failings while introducing new obligations under Consumer Duty. As enforcement ramps up, the FCA has levied significant penalties for financial crime non-compliance, reinforcing the importance of a robust regulatory framework.

Fraud, and in particular Authorised Push Payment (APP) scams, has emerged as a key focus of regulatory reform within the United Kingdom. The recent introduction of the APP Reimbursement Rule represents a pivotal development in consumer protection, requiring firms to reimburse victims within five working days, with a cap of £85,000 per claim. This regulatory shift forms part of a wider initiative to strengthen the UK's fraud prevention framework. It is further highlighted by the upcoming introduction of the Failure to Prevent Fraud (FTPF) offence, set to take effect in 2025. This legislation will place a firm legal obligation on organisations to implement stronger internal controls to identify and prevent fraud. By doing so, it reflects the growing emphasis on corporate accountability in combating financial crime and the rising expectation for firms to adopt a proactive approach to managing these risks.

The regulatory landscape across Europe has been equally dynamic. The European Union introduced a new AML/CTF package, alongside the rollout of the EU Artificial Intelligence (AI) Act, designed to balance innovation with improved risk management. In 2024, significant progress was made in digital asset regulation, with the phased implementation of the Markets in Crypto-Assets (MiCA) Regulation. While certain MiCA provisions took effect incrementally during 2024, its full impact is anticipated in 2025.

Meanwhile, individual member states, such as France, have taken notable steps to strengthen financial crime regulations, focusing on greater transparency and enhanced oversight of PEPs.

In Asia, Hong Kong and Singapore rolled out significant measures, showcasing their leadership in financial innovation and commitment to global standards. Hong Kong focused on modernising AML/CTF surveillance and improving cross-institutional information sharing, setting a strong precedent. Singapore introduced strict legislative reforms to combat proliferation financing and strengthen its anti-money laundering framework. These steps align with global trends, as regulators adopt international standards like the FATF Travel Rule, particularly in managing digital assets.

Three clear priorities emerge from these regulatory developments: stricter compliance requirements across industries, the dual role of technology in creating risks and offering solutions, and a stronger focus on transparency and accountability. These changes reflect a global push for a more coordinated and technology-driven fight against financial crime.

By 2025, these trends will gain momentum. The UK plans to introduce the FTPF offence, Europe is advancing digital asset regulation, and cross-border collaboration is becoming more critical. Together, these developments will drive a more integrated global approach to safeguarding financial systems.

This paper is organised by jurisdiction, covering the UK, EU and France, alongside Hong Kong and Singapore, with each section following a consistent structure. Each jurisdiction begins by setting the scene with a recap of significant legislative and regulatory developments in 2024, highlighting key trends and enforcement actions. The sections then transition to focus on forward-looking themes, including anticipated regulatory changes and emerging priorities for 2025.

2 United Kingdom

In 2024, the UK significantly strengthened its approach to tackling financial crime, marked by new government and regulatory measures aimed at bolstering the nation's defences against fraud and money laundering. With an estimated **£100 billion laundered annually** the urgency of these reforms is clear and emphasises the critical need for effective preventative action.

In the first half of the year, the Conservative Government advanced their Second Economic Crime Plan for 2023–2026, prioritising payment fraud, corporate criminal liability, and fraud prevention. In the latter half, the new Labour Government shifted attention towards anti-corruption and money laundering, employing targeted sanctions and strengthening law enforcement. Despite these shifts, tackling both internal and external fraud remains a bipartisan priority.

This year, the UK has prioritised tackling financial crime through collaboration across government, regulators, public organisations, and the private sector. The National Crime Agency (NCA), in its annual report, highlighted that most crime now occurs online. The accessibility of online tools for financial criminals underscores the need for a collaborative approach to combat these threats. In September, the FCA emphasised its role within a 'whole system response,' reinforcing the critical contribution of the private sector to government and regulatory efforts.

Throughout 2024, the UK Government amended the Money Laundering Regulations (MLRs), reflecting an ongoing refinement of its regulatory framework. Schedule 3ZA, the list of high-risk third countries, with a requirement for firms to monitor jurisdictions identified by the FATF as either High-Risk Jurisdictions subject to a Call for Action or Jurisdictions under Increased Monitoring. This necessitates continuous updates to risk assessments and customer due diligence (CDD) procedures in response to FATF's periodic reviews, with enhanced vigilance required for clients linked to high-risk nations. In parallel, the treatment of Politically Exposed Persons (PEPs) was further refined, distinguishing between domestic and foreign PEPs.

In 2024, the UK government also utilised sanctions as a key tool in its financial crime strategy. February saw the Conservative administration unveil a sanctions framework designed to align with foreign policy goals and bolster national security. This approach aimed to strengthen international alliances and private sector collaboration, while enhancing cross-government enforcement. The Labour government, building on this foundation, integrated sanctions enforcement within broader financial crime typologies, focusing particularly on kleptocracy.

Notable enforcement actions included the Office of Financial Sanctions Implementation (OFSI) imposing its first penalty for breaches of Russian sanctions. In October, the Office of Trade Sanctions Implementation (OTSI) was established to enforce trade sanctions, wielding significant penalties and enhanced reporting powers. Sanctions on regimes such as Russia, Iran, and North Korea underscored the UK's commitment to curbing illicit activities and human rights violations. The regulatory framework is set to strengthen further in 2025, with increased enforcement at the firm level.

Simultaneously, fraud prevention became a central focus, with the government responding to the £341 million lost to APP scams in 2023. The Payment Systems Regulator (PSR) introduced a mandatory reimbursement rule, mandating firms to reimburse victims within five days, with a revised cap of £85,000 per claim. The Financial Conduct Authority (FCA)

reinforced this by issuing guidance to payment service providers, urging them to enhance fraud prevention systems. The introduction of the Failure to Prevent Fraud (FTPF) offence, effective in September 2025, signals a shift towards corporate accountability for fraud.

The rise of emerging technologies, particularly AI and machine learning, has prompted regulators to address their potential misuse in fraud. Both the Public Sector Fraud Authority (PSFA) and the UK Financial Intelligence Unit (UKFIU) have raised alarms about AI-enabled fraud, encouraging businesses to adopt advanced AI enabled technologies to stay ahead of increasingly sophisticated threats. As the UK moves into 2025, the regulatory landscape will continue to evolve, with a sharper focus on technological integration, rigorous enforcement, and sustained collaboration between regulators, government, and the private sector.

> **The tide is turning. The golden age of money laundering is over.**
>
> David Lammy, Foreign Secretary

2.1 AML/CTF/CPF

UPDATED: The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs)

Politically Exposed Persons
A key regulatory focus, first raised by the FCA in September 2023 concerning access to and closure of UK payment accounts, continued into 2024, centring on the treatment of PEPs. On 10th January 2024, the UK government amended the MLRs to differentiate between the treatment of domestic and foreign PEPs. The amendment outlined how financial institutions should handle customers or potential customers who are domestic PEPs, or a relative or close associate (RCA), when no heightened risk factors are present. In such cases, the level of EDD required for domestic PEPs should be less stringent than that applied to non-domestic PEPs, if there are no high-risk indicators to suggest otherwise.

Institutions should identify and address gaps in their policies and controls, adopting a risk-based approach to manage false positives in PEP and RCA screening. Effective risk assessment methodologies, screening, and CDD processes continues to be essential in producing proportionate and accurate customer classifications.

High Risk Third Countries
On 24th January, the list of high-risk third countries under Schedule 3ZA were removed, with regulation 33(3)(a) requiring firms to now review countries named as either a high-risk jurisdiction subject to a call to action or under increased monitoring by the FATF. Firms must monitor and respond to ongoing changes to the lists, in turn updating risk assessments and customer due diligence (CDD) / enhanced due diligence (EDD) processes as needed. This shift necessitates robust systems to ensure timely adjustments in response to FATF's periodic updates, with heightened monitoring requirements for clients linked to high-risk jurisdictions.

UPDATED: Financial Crime Guide

In April, the FCA opened a consultation on proposed changes to the Financial Crime Guide (FCG) aiming to clarify its expectations, assist firms in evaluating the effectiveness of their financial crime systems and controls, and address any weaknesses within the FCG. The consultation concluded in June, and in November the FCA published a finalised Policy Statement. The Policy Statement considered the feedback garnered during the consultation period, thereby paving the way for the release of a refined final draft of the FCG.

Notably, the FCA has strengthened the sanctions chapter of the FCG, in response to evolving global and domestic financial crime challenges. The amendments draw from a

comprehensive assessment of firms' sanctions systems and controls conducted in the wake of Russia's invasion of Ukraine. The revised chapter integrated key lessons learned, ensuring that firms remain vigilant and compliant with an increasingly stringent sanctions framework.

A significant update included increased explicit coverage of PF throughout the FCG, underscoring the 2022 amendment to the MLRs which mandated firms to conduct PF risk assessments. The shift highlights the growing recognition of PF as a critical financial crime risk, and highlights that although related to financial sanctions, PF presents its own risks and threats. The FCA also provided enhanced guidance on the implementation and maintenance of automated and manual transaction monitoring systems, endorsing responsible innovation and the adoption of emerging technologies. Self-assessment questions for crypto asset firms registered under the MLRs used for evaluating the effectiveness of their financial crime systems and controls were also updated. Furthermore, additional wording was inserted to reflect the requirement for firms to ensure their systems and controls align with the Consumer Duty, which necessitates treating customers fairly while preventing financial crime. The update also omitted outdated references to EU rules, post-Brexit, and incorporated refreshed case studies based on recent FCA enforcement notices, thereby ensuring the FCG reflects current enforcement processes.

In light of these updates, firms are urged to carefully assess their systems and controls against the updated FCG, adjusting internal policies, monitoring mechanisms, training programmes, and governance structures as required to comply with the new amendments to the FCG.

UPDATED: **The Economic Crime and Corporate Transparency Act (ECCTA) 2023**

Throughout 2024, new provisions of the landmark ECCTA which seeks to bridge the nexus between corporate transparency and tackling financial crime entered into force. In January, the pre-investigation powers of the Serious Fraud Office (SFO) were expanded under the Act. Previously limited to international bribery and corruption, these powers now extend to all SFO cases, including fraud and domestic bribery, through which companies may be required to provide information.

In March, provisions made by the ECCTA came into force amending the Companies Act 2006. The scope of registrable beneficial owners for the Register of Overseas Entities and mandated additional information for Companies House was broadened, with Companies House also afforded new enforcement powers including fines and prosecution. The ECCTA empowered UK authorities to investigate, freeze, seize, and recover crypto assets in April. The confiscation and civil recovery regime under the Proceeds of Crime Act 2002 (POCA) was extended to crypto assets, designed to expedite law enforcement processes involving the seizure, freezing, and recovery of crypto assets connected to illicit or criminal activity.

NEW: **Dear CEO Letter on Action Needed in Response to Common Control Failings Identified in Anti-Money Laundering Frameworks**

In March, the FCA issued a Dear CEO letter to financial institutions (FIs) (Annex 1 firms), highlighting commonly identified control failings in assessed firms' AML frameworks. The letter highlighted discrepancies between registered and actual business activities, with financial crime controls failing to align with business growth.

Where we assess a firm's actions in response to this letter to be inadequate, we will consider appropriate regulatory intervention to manage the Financial Crime risk posed

Dear CEO letter, Pg 3

It called for improvements in business-wide and customer risk assessments to better identify and mitigate vulnerabilities, and raised concerns over insufficiently detailed policies, which left staff unclear on some compliance requirements under the MLRs. To strengthen governance, the FCA urged firms to allocate adequate resources, enhance staff training, and maintain clear audit trails for decision-making. The FCA expected FIs to have completed a gap analysis against each of the common weaknesses within six months of receipt of the letter.

NEW: **Payment Account Access and Closure Report**

In September, the FCA released a follow-up review on payment account access and closures, prompted by concerns over accounts being closed due to customers' political beliefs or lawful expressions. The FCA identified common reasons for account denials or terminations, including non-specific financial crime concerns, reputational risks, challenges faced by vulnerable customers, and difficulties meeting due diligence requirements due to unclear or burdensome information requests.

NEW: **Consumer Duty Feedback to CP21/36 and Final Rules**

The FCA reminded firms of their Consumer Duty obligations, in force for open products and services since July 2023, and for closed products and services from July 2024, to ensure fair outcomes for customers. It emphasised the importance of proportionate financial crime controls tailored to identified risks, avoiding generic approaches, and providing appropriate support for vulnerable customers in line with FCA guidance. As was seen in 2023, the FCA does not view financial crime compliance and consumer duty compliance as siloed processes. Firms should continue to review customer outcomes whilst discharging their wider compliance requirements.

2025 Outlook

HMT Consultation on improving the effectiveness of the Money Laundering Regulations

The **Economic Crime Plan 2023-26** included commitments from His Majesty's Treasury (HMT) to consult on changes to the MLRs as part of a broader initiative to reduce money laundering. In March 2024, HMT launched its consultation to enhance the effectiveness of the MLRs. The consultation requested feedback on how the MLRs can make CDD more proportionate and effective, strengthen system coordination, provide clarity on the scope of the MLRs, and reform registration requirements for the Trust Registration Service. While the exact date for the publication of the consultation's conclusions remains unknown, firms may look to the responses from industry bodies and stakeholders for insight and direction including the **Wolfsberg Group**, Crypto.UK, and UK Finance for insights into perspectives the Government will consider. In its response, UK Finance identified specific areas where the MLRs could be construed to allow tick-box compliance, diverting resources to low-impact activities that do little to detect or prevent economic crime, with the group highlighting that an effective risk-based approach offers flexibility to focus efforts on customer-specific risks and priority areas with high financial crime vulnerabilities.

NEW: Guidance on the Treatment of PEPs: Proposed Changes

In July, the FCA published its eagerly awaited multi-firm review assessing the treatment of PEPs. The review concluded that firms including banks and payment firms should do more to ensure parliamentarians, senior public servants, and their families are not treated unfairly purely due to their political status and affiliations. The FCA highlighted several issues with financial institutions' treatment of PEPs including overly broad definitions, ineffective classification of former PEPs, weak risk assessments, and unclear justifications for customer risk ratings – all of which had been found on some occasions to result in disproportionate risk ratings and subsequent treatments. Additionally, shortcomings were identified across firms involving communication with PEPs and RCAs, insufficient staff training, and outdated policies that failed to reflect new requirements under the MLRs to treat domestic PEPs and RCAs as lower risk unless high-risk indicators are present to suggest otherwise.

Coupled with the report, the FCA launched a consultation proposing amendments to its guidance on the treatment of PEPs, focusing on three key changes. First, Non-executive Board Members (NEBMs) of UK government departments would under the proposal not be classified as PEPs, as they offer external advice without executive authority. Second, all PEP relationships would be required to have formal sign off from senior management, with amendments seeking to preserve money laundering reporting officer (MLRO) oversight while also permitting alternative approval methods. Lastly, in line with amendments made to the MLRs, the FCA proposed to amend guidance to emphasise how firms should tailor their treatment of domestic PEPs as lower risk, unless other risk factors are identified.

Key Regulatory Strategies 2024-25

Economic Crime Plan 2023-2026	• Reducing money laundering and recovering more criminal assets • Combatting kleptocracy and driving down sanction evasion • Cutting fraud
NCA Strategic 5 Year Plan	• Reduce fraud and combat corrupt elites, state threats, cybercrime, money laundering and other economic crime • Play a full role in delivering the Government's objectives to reduce and prevent crime and respond to national security threats
FCA Strategy 2022-2025	The FCA pledges to deliver on its 13 public commitments focusing on: • Reducing and preventing financial crime • Putting consumers' needs first
UK Government Counter Fraud Functional Strategy 2024-2027	• Support and develop people and awareness • Harness data and technology more effectively • Embed prevention • Drive a targeted, proportionate response against fraudsters • Secure cross-system cultural change
UK Government Sanctions Strategy 2024	• Undermine Russia's ability to fund and wage its war against Ukraine, including by cracking down on efforts to get around sanctions • Address threats and malign activity through geographic and thematic sanctions regimes • Build international coalitions and take co-ordinated action with allies and partners to maximise the impact of our sanctions while deepening engagement with business, financial institutions and other stakeholders • Reinforce sanctions implementation and enforcement, including by helping UK businesses to understand and comply with sanctions and by taking robust action on non-compliance
SFO Strategic Objectives 2024-2029	• Enhancing operational resilience • Developing core skills within the organisation

UK AML Key Actions

1 Strengthen Risk Assessments

- **Boards and CEOs**: Ensure the organisation's risk assessment framework is robust and resourced to address FATF updates and regulatory expectations.
- **MLROs and Compliance Teams:** Continuously update CDD/EDD processes to monitor high-risk jurisdictions and adapt to evolving threats.

2 Enhance PEP Screening

- **Boards and CEOs:** Oversee policy updates to ensure PEP screening aligns with amended MLRs and supports fair treatment.
- **MLROs and Compliance Teams:** Apply risk-based approaches to differentiate domestic and foreign PEPs, ensuring proportionate handling while reducing false positives.

3 Prepare for Regulatory Changes

- **Boards and CEOs:** Lead readiness efforts for the FTPF offence and other 2024-25 regulatory changes, ensuring accountability across teams.
- **MLROs and Compliance Teams:** Conduct gap analyses to address weaknesses and align processes with upcoming legislation.

4 Leverage Technology for Compliance

- **Operations and Technology Teams:** Invest in AI-enabled systems to strengthen transaction monitoring and fraud prevention.
- **MLROs and Compliance Teams:** Collaborate with tech teams to ensure tools are optimised for AML/CTF effectiveness.

5 Foster Cross-Functional Collaboration

- **Boards and CEOs:** Champion collaboration across compliance, operations, and technology teams to build a cohesive AML/CTF strategy.
- **MLROs and Compliance Teams:** Engage with internal and external stakeholders to address emerging risks and regulatory priorities effectively.

2.2 Fraud

If 2023 was a year of fraud policy formation, 2024 was the year of implementation. With **£341m** lost to Authorised Push Payment (APP) scams in 2023, preventing and tackling both internal and external fraud remains a key cross-party legislative agenda item in the UK. Complex cases of fraud mean that a one-size-fits all approach to preventing and tackling it isn't effective, as fraud does not impact all industries the same way. True resilience will come from understanding the problem and operationalising a proportionate response.

The UK's fraud landscape in 2024 was marked by several landmark rule implementations and announcements. The Payment Systems Regulator (PSR) introduced new APP reimbursement rules for banks and other in-scope payment firms, and the eagerly anticipated guidance on the forthcoming failure to prevent fraud offence was issued, with the offence in place from 1st September 2025. Developments during 2024 highlighted the importance of implementing robust fraud prevention frameworks which promote frictionless customer experiences. As 2025 approaches, financial institutions must continue to adapt to the evolving threat landscape by leveraging technology, strengthening their fraud prevention frameworks, and fostering ongoing collaboration with regulatory bodies.

> **Fraud continues to pose a major threat in this country with over £570 million stolen through payment fraud in the first half of the year.**
>
> Ben Donaldson, UK Finance Economic Crime MD

NEW: APP Fraud Reimbursement Requirement

In May 2022, the Treasury announced its plan to introduce legislation enabling the PSR to mandate victim reimbursement for APP scams, enacted in June 2023 via the Financial Services and Markets Act. In December 2023 the PSR **finalised its policy statement** outlining its position on the reimbursement requirement for APP scams. Fast forward to 7th October 2024, and the APP Reimbursement Rule is now in force, requiring in scope firms to reimburse victims within five working days of their claim, with an optional excess that firms can apply of £100 and a maximum reimbursement amount set at £85,000 per claim.

The rule was subject to consultation, debate and change throughout 2024, including a change in the maximum reimbursement rate from the initially set value of £415,000. The change followed an industry-wide **consultation** and regulator-industry engagement sessions which concluded that the lower rate aligns with the fact that the majority of high-value Faster Payments APP scam cases scams often consisted of multiple low value payments. On the horizon, the reimbursement rule could extend to banks and other payment firms participating in Clearing House Automated Payment System (CHAPS), following consultation in May, as to reflect the reality that criminals operate across multiple payment systems in conducting fraud.

For in-scope firms, prompt action and a strategic plan are key to ensuring fraud risk management remains resilient, minimises losses, and costs, and meets the PSR's expectations and requirements. Robust fraud detection, mitigation and prevention processes are key to reducing instances of APP fraud for customers, in turn reducing reimbursement claims.

Aligning with the introduction of the new APP Reimbursement requirements in October, the FCA published two 'Dear CEO' letters to **PSPs and EMIs**, as well as to **banks and building societies**, stating their expectations of all in-scope firms to be reducing APP fraud by enhancing their anti-fraud systems and controls.

In the letters, the FCA reinforced its expectation that firms establish adequate oversight, systems, and controls to meet these requirements. Steps to proactively prevent scams and protect customers are critical, as failures can lead to consumer harm, reputational damage, and long-term business risks. The FCA and PSR will collaborate to monitor firms' compliance, using data to track prudential issues, conduct breaches, and inadequate systems and controls, ensuring they effectively protect consumers from APP fraud.

In September, the FCA consulted on drafted amendments to the Payment Services Regulations (PSRs) which would enable payment service providers (PSPs) to delay making a payment or transaction where they have reasonable grounds to suspect fraud or dishonesty. Coined the 'payment delays legislation', the amendment would impact the payment processing systems of PSPs and electronic money institutions (EMIs). In the consultation, the FCA acknowledged industry concerns surrounding the current 'D+1' requirement mandating the process of outbound transactions by the end of the next business day following receipt of a payment order; a timeframe which reduces the time firms have to investigate potentially fraudulent activity, In response, new legislation would extend this timeframe to 4 business days, providing firms with greater time and in turn flexibility to conduct thorough assessments, including by communicating with relevant parties, such as law enforcement or the payee's PSP. As can be expected, the onus remains on PSPs and EMIs to demonstrate that they have taken reasonable steps to review the legitimacy of transactions for anti-fraud purposes.

Artificial Intelligence and Fraud

Given the sheer volume of transactions and data, it is unsurprising that financial crime and fraud prevention are complex, particularly when coupled with a common reliance across firms of all scales and scopes on manual processes. These processes are often time-consuming, error-prone, costly, and inefficient, potentially hindering compliance with regulatory obligations. As a result, AI has become a strategic priority for firms looking to streamline their fraud detection and prevention processes, driven largely by the transformative opportunities unlocked by generative AI (GenAI) and the Large Language Models (LLMs) underpinning it, as well as by Machine Learning, of which the operational and compliance benefits are continually being explored.

While the potential of AI continues to be explored by the government, regulators, and firms alike, there was a marked increase in AI risk evaluations and explorations in 2024. The Public Sector Fraud Authority (PSFA) and the UK Financial Intelligence Unit (UKFIU) highlighted the increasing threat of AI-enabled fraud. AI tools like deepfakes and LLMs do have the dual propensity to be exploited to perpetrate scams, making it harder for victims to identify fraudulent activities. Both organisations have emphasised the importance of understanding and addressing these emerging risks to effectively combat fraud. New and emerging technologies and their capabilities will pose risks, but it is their mitigation which will remain key, particularly if tools including AI and Machine Learning are to be leveraged to enhance fraud detection and prevention efforts. Centralising fraud tools and standardising metrics has the potential to improve efficiency and accountability, whilst investing in advanced technologies like real-time transaction monitoring can help firms identify and block suspicious activities before the fraud has occurred. For firms, remaining cognisant of the developing role of new technologies in fraud regulation and compliance will remain key. In November, the Alan Turing Institute, Plenitude Consulting, Napier AI, and the FCA launched a project aimed at enhancing money laundering detection. The initiative focused on creating a synthetic dataset by combining anonymised financial transactions from high street banks with diverse money laundering typologies. The project aimed to address the FCA's findings that the lack of realistic data was a significant barrier to developing innovative detection methods beyond traditional "rules-based" approaches. The synthetic dataset, accessible through the FCA's digital sandbox, would allow firms to test and refine new algorithms in a controlled environment.

This collaboration is part of the FCA's broader effort to leverage data and analytics to combat financial crime. It aligns with the UK's Second Economic Crime Plan and the FCA's Business Plan, aiming to foster a more dynamic market for money laundering detection solutions and enhance the ability of retail banks to prevent illicit activities. By providing firms with a realistic testing environment, the project will help them develop more effective detection technologies, ultimately strengthening the financial sector's efforts to combat money laundering.

2025 Outlook

NEW: Failure to Prevent Fraud Offence

In November, the UK Government published the widely anticipated guidance on the new Failure to Prevent Fraud (FTPF) offence, introduced by the ECCTA. In force from 1st September 2025, firms should use the coming months to revise and enhance policies and procedures concerning both internal and external fraud to prepare for forthcoming requirements.

The criminal offence is designed to hold large accountable for failing to prevent fraud committed by employees, agents, or other associated persons acting on their behalf, where the fraud benefits the organisation or its clients. The guidance outlined key principles for support firms' fraud prevention framework, including ensuring senior management commitment, conducting a risk assessment of fraud exposure, implementing proportionate and practical fraud prevention procedures, applying due diligence when engaging associated persons, and establishing robust communication, training, and whistleblowing mechanisms internally. In addition to guiding businesses, the FTPF offence is instrumental of the government focus on corporate criminal liability for financial crime, designed to reduce fraud by strengthening corporate governance and transparency. Even mature organisations continue to lack insight and oversight, making it vital for firms to review and implement controls in response to the offence.

75% of firms are already using AI, with a further 10% planning to use AI over the next three years

Bank of England / FCA joint survey on AI

UK Fraud Key Actions

1 Enhance Fraud Prevention Frameworks

- **Boards and CEOs**: Oversee the integration of fraud prevention strategies, ensuring alignment with APP reimbursement rules and the forthcoming Failure to Prevent Fraud (FTPF) offence.
- **Fraud and Compliance Teams:** Conduct comprehensive fraud risk assessments and revise policies to address internal and external fraud risks effectively.

2 Leverage Advanced Technology

- **Operational and Technology Teams:** Invest in AI-driven tools for real-time transaction monitoring and fraud detection to enhance efficiency and accuracy.
- **Fraud Teams:** Explore the use of synthetic datasets and machine learning models for refining detection capabilities and improving response times.

3 Prepare for the FTPF Offence

- **Boards and CEOs:** Ensure senior management commitment to compliance, embedding robust fraud prevention measures across the organisation.
- **Fraud and Legal Teams:** Establish clear procedures for due diligence, staff training, and whistleblowing to mitigate the risk of corporate liability under FTPF.

4 Optimise APP Fraud Mitigation

- **Compliance Teams:** Strengthen controls to prevent APP fraud, reducing reimbursement claims and aligning with FCA and PSR expectations.
- **Customer Operations Teams:** Improve fraud communication and support mechanisms to protect customers and enhance trust.

5 Foster Collaboration and Knowledge Sharing

- **All Stakeholders:** Participate in industry initiatives, like FCA's digital sandbox projects, to leverage shared insights and develop innovative detection methodologies.
- **Fraud Teams:** Work with law enforcement, regulators, and other financial institutions to address fraud threats collaboratively.

2.3 Sanctions

In February 2024, the Conservative government unveiled its **sanctions strategy**, outlining its approach to addressing global threats, upholding international norms, and safeguarding national security. The strategy focused on aligning sanctions with UK foreign policy priorities, strengthening international partnerships, collaborating with the private sector and civil society, and fostering an integrated approach to implementation and enforcement across government. The Labour government has since focused on positioning sanctions enforcement at the nexus point of broader financial crime typologies through a crackdown on kleptocracy and its wider links to crimes including corruption and money laundering.

The UK government doubled down on the enforcement of sanctions this year, with the Office of Financial Sanctions Implementation (OFSI) issuing its first monetary penalty against a firm for breaching Russian sanctions requirements. The new Office of Trade Sanctions Implementation (OTSI), launched in October, will now enforce trade sanctions, imposing significant financial penalties on violators, and introduce robust reporting and information request powers, placing further onus on firms to implement robust trade finance processes and controls to comply with these regulations.

Extensive sanctions, from asset freezes to trade restrictions, were issued and enforced by the UK government in 2024, illustrating the cross-party commitment to using restrictive measures to target individuals and entities involved in illicit activities and human rights abuses. Designations on individuals and groups operating in and with regimes including Russia, Iran and North Korea were imposed, whilst the Oil Price Cap, a product of a continuing global coalition, continues to be in force on Russian oil to reduce Russian revenue from oil exports. Sanctions will undoubtedly remain a primary weapon in the UK government's arsenal in 2025, and agencies will continue to double down on their enforcement at firm level.

NEW: The Sanctions (EU Exit) (Miscellaneous Amendments) (No.2) Regulations 2024

In November, a myriad of general and regime-specific sanctions amendments was introduced in Parliament, aimed at improving compliance and enforcement and impacting a wide range of sectors. From the 5th of December, all UK persons holding assets of designated persons (DPs) are now required to provide annual reports to OFSI detailing these assets, as to enhance ownership transparency and oversight. Amendments to licensing and exceptions provisions including the introduction of a new insolvency licensing purpose and required payments exception also came into force, as well as changes to Russian sanctions surrounding the use of trusts, reporting requirements and new civil monetary penalty powers for specific breaches. On 14th May 2025, reporting obligations will extend to high-value dealers, art market participants, letting agencies, and insolvency practitioners, with these sectors advised to already begin reviewing and uplifting reporting processes and policies.

> **"This new government is resolutely committed to strengthening our sanctions regime, with robust enforcement and penalties for those who fail to comply. From Moscow to Tehran, kleptocrats, aggressors, & the enablers who support and facilitate their wealth and malign actions, should be on notice."**
>
> Stephen Dougherty, Sanctions Minister

UK Sanctions Key Actions

1 Strengthen Governance and Oversight

- **Boards and CEOs**: Establish clear accountability for sanctions compliance, ensuring leadership oversight of reporting, asset management, and adherence to regulatory changes.
- **Compliance Teams**: Implement governance frameworks that align with OFSI and OTSI requirements, ensuring timely escalation of sanctions-related risks.

2 Enhance Reporting and Transparency

- **Legal and Compliance Teams**: Prepare for annual reporting requirements on designated person (DP) assets by implementing robust tracking and reporting systems.
- **High-Value Dealers, Art Market Participants, & Letting Agencies:** Begin reviewing internal processes to comply with expanded reporting obligations effective May 2025.

3 Strengthen Trade Finance Controls

- **Trade Finance and Operations Teams:** Develop and enforce robust trade sanctions compliance processes to meet OTSI's new enforcement standards.
- **Legal Teams:** Review contracts for trade activities to ensure they comply with new licensing provisions and sanctions amendments.

4 Foster Collaboration and Preparedness

- **Boards and Compliance Teams:** Promote cross-functional collaboration to address sanctions compliance comprehensively, involving legal, trade, and operations teams.
- **External Stakeholders:** Engage with regulators, industry bodies, and peers to stay informed of best practices and emerging regulatory changes.

5 Leverage Technology for Compliance

- **Operations and Technology Teams:** Invest in advanced sanctions screening tools to identify and manage risks associated with designated persons, assets, and transactions.
- **Compliance Teams:** Integrate technology solutions for real-time monitoring, ensuring proactive detection of potential breaches and enabling efficient reporting.

2.4 Digital Assets

In April, the Bank of England, in tandem with the FCA, set out proposals to implement and operate the Digital Securities Sandbox (DSS), which aims to enable participants to utilise Distributed Ledger Technology (DLT) to undertake the activities typically linked with Central Securities Depositories and Trading Venues. The joint response to the consultation was published in October, along with the DSS Rules Instrument, guidance on the operation of the DSS and application forms, marking the opening of the Sandbox to applicants, and a crucial step to facilitate the adoption of digital assets in the UK. However, a comprehensive UK regulatory framework for digital assets has yet to emerge. Following the publication of the response to HMT's consultation on the proposed future financial services regime for crypto assets in October 2023, the Bank of England and the FCA published proposals for the regulation of stablecoins, which are expected to constitute the first phase of such a regime. Towards the end of the year, the FCA published its 'crypto roadmap' of its planned activities for 2025/26. By 2026, it is anticipated that a regulatory regime will be in place with all final rules and guidelines published, with a 'gateway' period in place allowing firms ample preparation time. To get to this point, numerous policy publications and consultations are scheduled to go live in 2025, including standards for financial crime and the Consumer Duty in Q3.

> **"We are committed to working closely with the Government, international partners, industry, and consumers to help us get the future rules right."**
>
> Matthew Long, FCA Director of Payments and Digital Assets

UK Digital Assets Key Actions

1 Prepare for Regulatory Changes

- **Boards and CEOs**: Oversee strategic planning for compliance with upcoming regulations on stablecoins and crypto assets, ensuring readiness for the anticipated 2026 regime.
- **Legal and Compliance Teams:** Monitor and respond to forthcoming policy publications and consultations in 2025, focusing on financial crime and Consumer Duty standards.

2 Engage with the Digital Securities Sandbox (DSS)

- **Innovation Teams**: Explore opportunities within the DSS to pilot Distributed Ledger Technology (DLT)-enabled activities, such as trading and settlement, to gain a competitive edge.
- **Compliance Teams**: Familiarise with the DSS Rules Instrument and ensure alignment with its operational guidance when participating in the sandbox.

3 Implement Robust Financial Crime Controls

- **Fraud and Compliance Teams:** Begin aligning anti-financial crime frameworks with anticipated crypto standards to address evolving risks tied to digital assets.
- **Boards and CEOs**: Allocate resources to strengthen fraud prevention and monitoring systems tailored to DLT-based transactions.

4 Leverage Technology for Operational Readiness

- **Operations and Technology Teams**: Invest in blockchain analytics tools and DLT platforms to enhance transparency, transaction monitoring, and compliance in digital asset operations.
- **Legal Teams**: Collaborate with technology teams to ensure operational systems are equipped for future regulatory requirements.

5 Engage with Policy Development

- **Boards and Legal Teams**: Actively participate in consultations and discussions shaping the UK's digital asset regulatory framework to influence policy direction and gain early insights.
- **Industry Representatives**: Build coalitions with trade bodies and regulators to advocate for balanced and innovation-friendly policies.

2.5 Enforcement

Fines issued by the FCA on regulated firms for financial crime non-compliance amounted to over £49m during 2024. In July, CB Payments, a Coinbase affiliate firm, was fined for failing to implement a Voluntary Application for Imposition of Requirements (VREQ) effectively, which meant that high-risk customers were able to make prohibited deposits for crypto asset transactions. In October, Starling Bank was fined for failures relating to its financial sanctions screening and breach of the regulator's-imposed requirement to cease the onboarding of high-risk customers – failures Therese Chambers, joint executive director of enforcement and oversight called "shockingly lax". The following month, Metro Bank was penalised for deficiencies in its transaction monitoring systems, which failed to adequately oversee over 60 million transactions totalling more than £50 billion, exposing the bank to money laundering risks. These enforcement actions, alongside the FCA's growing use of s166 reviews for financial crime, underscore the critical need for regulated firms to stay vigilant and address the consequences of non-compliance.

Financial services firms should continue to closely monitor FCA enforcement actions to understand regulatory expectations, identify potential weaknesses in their compliance frameworks, and mitigate any identified or shared risks. By assessing their own processes against enforcement action notices, firms can enhance their risk management practices, avoid regulatory breaches, protect their reputation, and maintain customer trust, together producing a sustainable approach to compliance.

Key statistic

Penalty fines issued by the FCA on regulated firms for financial crime non-compliance amounted to over £49m during 2024

3 European Union

In 2023, the European Union (EU) positioned itself at the forefront of global initiatives aimed at formulating regulatory frameworks tailored to the challenges and opportunities presented by the evolving landscape of new technologies and digital assets. The incremental implementation of these initiatives took centre stage in 2024. In France, national legislation was updated during the year to transpose various financial crime provisions of EU law, in areas from beneficial ownership transparency to the treatment of PEPs.

The staggered implementation of selected provisions of the landmark EU law on crypto assets, the Markets in Crypto Assets Regulation (MiCA) began in June and will continue in December. It will implement a common regulatory standard across the EU for compliance for the crypto-asset market, to ensure consumer protection, market integrity, and financial stability in the use of crypto assets. Three years after first being tabled, the EU passed a new AML/CTF package of laws in June, strengthening financial crime frameworks across the bloc and introducing forthcoming requirements for a new host of financial and non-financial sectors. On sanctions, the EU doubled down on its emphasis on a common and rigorous approach to the implementation and enforcement of restrictive measures.

France has made significant progress in strengthening measures to combat financial crime, focusing on improving transparency and enhancing oversight of Politically Exposed Persons (PEPs). These efforts highlight France's leadership in aligning domestic regulations with European standards, demonstrating its commitment to robust frameworks and effective enforcement. This paper highlights developments which have occurred in French regulation in line with Plenitude's French RegSight register.

3.1 AML/CTF/CPF

France

UPDATED: Monetary and Financial Code (Code Monetaire et Financier)

In April, amendments to the financial crime provisions of the Monetary and Financial Code introduced changes aimed at enhancing transparency and accountability. Provisions within Section 9: Information on Beneficial Owners were inserted as to require in-scope firms to declare updated information relating to their beneficial owners. If discrepancies between reported and available information are identified by administrative authorities, the organisation will be alerted. The onus remains on firms to ensure their beneficial ownership information is not just accurate and verified but reviewed on an ongoing basis and reflective of any changes.

NEW: AMF Sectoral Risk Analysis: AML/CTF

In June, the Autorité des Marchés Financiers (AMF) released an updated version of its sectoral risk analysis (SRA) for ML/TF. The focus sectors assessed for ML/TF risks included asset management, with distinctions made between collective management of financial instruments, investment capital, real estate management and individual portfolio management; financial investment advisors, and firms operating in digital assets. Firms operating in the highlighted sectors under AMF supervision are encouraged to review the SRA as a benchmark for their own risk assessments. The report can also be used to provide insights into the new and ongoing supervisory objectives of the AMF, and where the Authority may focus its professional reviews.

UPDATED: ACPR guidance on PEPs

The PEP guidance published in July by the Autorite de Controle Prudential (ACPR) offered an in-depth and clarified explanation of its definition of a PEP. In a similar approach to that of the UK, which clarified its definition and risk-based approach to PEPs for firms to adopt, the ACPR highlighted in its guidance that the categorisation of a customer as PEP should not lead to the generalised label of high-risk being applied.

The ACPR requires credit and financial institutions to take appropriate measures to establish the origin of assets and funds involved in any relationship (or occasional transaction) with a customer or beneficial owner which has PEP status. The guidance aids firms in this exercise by stipulating the identification and verification (ID&V) documentation which should, as a baseline, be requested. This information can directly feed into firms' internal PEP policies and procedures, as well as customer and business-wide risk assessments

European Union

The New EU AML/CTF Package

The European Union passed a new AML/CFT package of laws to strengthen the EU's toolkit to fight money laundering and terrorist financing in June. Aimed at strengthening the AML/CTF systems and promoting a harmonised approach to tackling financial crime across the EU, the package consists of the Sixth Anti-Money Laundering Directive (6AMLD), the 'Single Rulebook' (AMLR), and the Anti-Money Laundering Authority (AMLA) Regulation. Designed to implement a common, harmonised approach to AML/CTF across the EU and the financial and non-financial sectors operating within and across them, to reflect ever-emerging risks, the package is comprised of:

NEW: Regulation (EU) 2024/1624 on preventing the use of the financial system for the purposes of money laundering or terrorist financing [AMLR]

The EU's revised Anti-Money Laundering Directive (6AMLD) will significantly impact the financial sector, particularly crypto-asset service providers, real estate agents, art dealers, and certain professional services firms. Key changes include:

- Crypto asset service providers (CASPs), real estate agents, art dealers, and certain professional services firms must adapt AML/CTF policies to comply with the stricter regulations.
- Stricter CDD measures will apply to high-risk customers, including high-net-worth individuals and PEPs.
- CDD procedures must be revised to reflect stricter requirements for high-risk customers, including high-net-worth individuals and PEPs.
- The threshold for disclosing beneficial ownership of companies will be lowered to 25%, making it easier to identify the ultimate owners of companies and prevent the misuse of corporate structures for illicit purposes. Member states will be able to propose lower thresholds to the European Commission for high-risk industries of no less than 15%.
- Firms must review and adapt reporting mechanisms to reflect the new requirement to disclose beneficial ownership at 25%.
- The directive will introduce stricter regulations for crypto-asset service providers to mitigate the risks associated with digital currencies.

NEW: Directive (EU) 2024/1640 on the mechanisms to be implemented by Member States to prevent the use of the financial system for the purposes of money laundering or terrorist financing [6MLD]

The Sixth AML Directive introduces new measures for member states to implement in strengthening their national AML/CTF systems and transpose into law by 10 July 2025. It will remain important for firms to be aware of the growing powers of the Financial Intelligence Units [FIUs] of their operating jurisdictions, as to ensure full communication and compliance with any supervisory expectations and requests. 6MLD will:

- Require member states to store all beneficial ownership information in a central register and make it available to competent authorities, obliged entities conducting CDD, and to members of the public displaying legitimate interest, as well as verifying that the information is accurate and up to date.
- Further empower EU FIUs, who will be able access financial, administrative and law enforcement information, and have powers to suspend the use of a bank account or payment account, crypto-asset account, or a business relationship to analyse suspicious behaviour and share these results with authorities.
- Encourage further cross-border communication and collaboration between FIUs to further harmonise approaches to fighting financial crime across the EU.

NEW: Regulation (EU) 2024/1620 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism [AMLA]

The establishment of the Anti-Money Laundering Authority (AMLA) in Frankfurt marks a significant step towards strengthening the EU's fight against financial crime. The AMLA will oversee high-risk financial institutions, impose penalties for serious breaches, and enhance whistleblowing mechanisms. It will also collaborate with the European Banking Authority (EBA) to develop joint guidelines and improve coordination between prudential and financial crime regulators. Firms will need to adapt to the new regulatory landscape and ensure compliance with the AMLA's requirements.

Entities including financial and credit institutions, CASPs, high-value goods dealers, and now professional football clubs and agents can already begin to prepare for new and amended forthcoming requirements. Internal policies, procedures, and controls will require review and revision to reflect the new rules and regulations. EU authorities will look to ensure the harmonised approach aimed for is reflected at firm-level. Once each legal instrument is applied, it will be important for obliged entities to ensure that they are operating in line with the most recent legal developments. Firms should continue to be aware of the EU's supranational position on AML/CTF rules and how EU regulations will be transposed into law by individual member states.

NEW: The Instant Payments Regulation (EU) 2024/886

The introduction of the Instant Payments Regulation in March introduced new verification and screening requirements for PSPs. By amending Regulation EU 260/2012 on credit transfers and direct debits, PSPs are now required to conduct regular and periodic sanctions screening of customers, against real-time EU restrictive measure lists and designations, highlighting the immediate need for firms to adopt systems capable of keeping pace with regulatory changes. With the rapid nature of payment transfers only getting quicker, firms will need to ensure their automated screening systems screen the EU database in real time, as to screen payments before execution, and effectively filter true and false matches effectively and rigorously.

2025 Outlook

NEW: AMLA countering money laundering and the financing of terrorism

Set to centralise and strengthen oversight by integrating its own operations with those of Member States' AML/CFT authorities, AMLA will also establish a cooperative framework for FIUs across the EU, ensuring a unified approach to combating illicit financial activities. The adoption of Regulation (EU) 2024/1620, published in June 2024, formalised AMLA's mandate, with operations set to commence in July 2025.

The process leading to AMLA's establishment gained significant attention throughout 2023 and 2024. After reaching a provisional agreement in December 2023, the European Parliament and the Council engaged in deliberations to determine the seat of the Authority. Multiple Member States bid to host AMLA, emphasising the strategic importance of housing this institution.

In February 2024, Frankfurt was selected as the headquarters, outpacing other contenders due to its status as a financial hub, home to the European Central Bank, and its robust infrastructure for supporting large-scale regulatory bodies. Frankfurt's selection underscores the EU's intention to leverage existing financial expertise and institutions to maximise AMLA's effectiveness. Frankfurt's role as the Authority's base symbolises a centralised commitment to transparency and stringent oversight in financial transactions.

The Authority is expected to bolster confidence in the EU's financial markets, both internally and globally, by directly supervising high-risk financial entities from 2028 and intervening where national regulators fail. As preparations advance, including the formation of a five-member executive board and the recruitment of 450 experts, AMLA's leadership, under the newly appointed Bruna Szego, is focused on building capacity, stakeholder engagement, and enhancing cross-border collaboration.

> **Given the cross-border nature of financial crime, the new authority will boost the efficiency of the anti-money laundering and countering the financing of terrorism framework, by creating an integrated mechanism with national supervisors to ensure obliged entities comply with AML/CFT-related obligations in the financial sector.**
>
> European Council Press Release

EU AML Key Actions

1 Strengthen Beneficial Ownership Compliance

- **Boards and CEOs:** Ensure oversight of beneficial ownership reporting processes to comply with France's updated Monetary and Financial Code and upcoming EU requirements under 6AMLD.
- **Compliance Teams**: Implement ongoing verification and monitoring systems to ensure beneficial ownership data is accurate & up-to-date.

2 Adapt to Evolving PEP Requirements

- **Compliance Teams:** Revise PEP policies to align with ACPR guidance, ensuring risk-based approaches distinguish between varying risk levels for domestic and foreign PEPs.
- **Operations Teams:** Enhance ID&V documentation processes to verify the source of funds for PEP-linked transactions, as mandated by the ACPR and EU regulations.

3 Leverage Sectoral Risk Assessments (SRAs)

- **Fraud and Risk Teams:** Use the AMF's updated SRA as a benchmark to identify ML/TF risks in sectors like asset management & digital assets.
- **Boards and Compliance Teams:** Align BWRA's with supervisory priorities identified in the AMF's sectoral reviews.

4 Prepare for New EU Regulations

- **Compliance Teams:** Begin adapting internal policies & controls to meet requirements under the EU AMLR, 6AMLD, & AMLA, including stricter CDD for high-risk customers & revised crypto-asset regulations.
- **Legal Teams:** Collaborate with FIUs and ensure mechanisms are in place to comply with expanded beneficial ownership and reporting obligations by 2025.

5 Implement Real-Time Monitoring for Instant Payments

- **Tech and Operations Teams:** Invest in automated screening systems to ensure real-time compliance with the Instant Payments Regulation's sanctions screening requirements.
- **Compliance Teams:** Train staff to manage and mitigate false positives in sanctions screening processes, reducing friction while maintaining regulatory compliance.

3.2 Fraud

The European fraud landscape is becoming increasingly complex for FIs to navigate. As fraud risks and threats evolve, the regulatory landscape is in turn shifting to strengthen customer protection, placing greater responsibility on FIs.

NEW: Council Directive (EU) 2020/284

To increase transparency rules and assist EU states crack down on Value Added Tax (VAT) fraud, the EU introduced new rules for PSPs at the beginning of the year. As of January 1st, PSPs offering payment services in the EU were required to monitor the beneficiaries of cross-border payments, and from April, required to transmit information on those who receive more than 25 cross-border payments per quarter to the administrations of EU Member States. The new requirements reflected the key role played by PSPs in anti-fraud including banks, EMIs, and PIs, which significantly contribute to the handling of over 90% of online purchases in the EU. Transparency and information sharing requirements on these firms will provide Member States with payment information allowing them to detect VAT fraud more effectively and rapidly, key to prevent payment fraud in its rapid nature.

NEW: EU Artificial Intelligence Act

In May, the EU AI Act was passed by the EU Commission, establishing guidelines for the development, deployment, and use of AI systems based on their associated risks. The Act adopts a risk-based framework, regulating only those AI systems deemed to carry specific levels of risk. It classifies AI systems into four categories: 1) unacceptable risk, 2) high risk, 3) limited risk, and 4) minimal risk. High-risk AI systems will be subject to rigorous evaluations to ensure compliance with standards for data quality, technical documentation, record-keeping, transparency, and human oversight. While internal assessments may be conducted by providers, sensitive applications require review by external "notified bodies."

It is important to note that although the AI Act doesn't focus on regulating AI use in the financial sector, there are direct implications for FIs. If tools being deployed by a firm are rated high risk, the firm will have more stringent compliance requirements concerning their governance. This will extend to AI models being used for fraud prevention processes, as is being encouraged of FIs across jurisdictions. Once the rules come into effect, firms operating across the EU who adopt AI technology into their controls processes will need to navigate dual compliance with their existing financial crime compliance requirements. The Act will be fully in force in August 2026, but some provisions will be applicable sooner, including the ban of AI systems posing unacceptable risks, codes of practice, and transparency requirements. High-risk systems will have additional time to prepare for forthcoming requirements as their obligations will be applicable from the beginning of 2026.

> **"It remains crucial that we work together like never before to protect the financial interests of the EU. Fraudsters use new technologies without any legislative or ethical limitations, they do not respect borders and their criminal activities exploit any loopholes they discover in multiple jurisdictions. That is why we, in the anti-fraud community, need to make sure that we have procedures in place to respond quickly, collectively and as efficiently as possible."**
>
> OLAF Director-General Ville Itälä

EU Fraud Key Actions

1 Strengthen Cross-Border Payment Monitoring

- **Compliance Teams**: Implement systems to track and report beneficiaries of cross-border payments exceeding 25 transactions per quarter, ensuring compliance with the EU VAT Directive.
- **Operations Teams:** Develop robust workflows to share payment data with relevant EU Member State authorities to support VAT fraud prevention.

2 Ensure Transparency in AI Usage

- **Boards and CEOs**: Oversee AI deployments, ensuring they comply with the EU AI Act's transparency and risk classification requirements.
- **Technology and Compliance Teams:** Conduct regular assessments of AI systems, focusing on data quality, documentation, and human oversight for high-risk applications.

3 Enhance Fraud Detection with Advanced Technology

- **Fraud and Risk Teams:** Leverage AI and machine learning tools for fraud detection while aligning these systems with the EU AI Act's standards to mitigate compliance risks.
- **Technology Teams:** Integrate real-time monitoring and record-keeping to detect anomalies and minimise false positives.

4 Foster Cross-Border Collaboration

- **Legal Teams:** Engage with regulators and counterparts across Member States to streamline reporting processes and share insights into emerging fraud risks.
- **Operations Teams**: Build communication channels with EU authorities to ensure seamless data transmission and compliance with reporting obligations.

5 Prepare for Future Regulations

- **Boards and Legal Teams**: Stay ahead of regulatory developments, including AI and fraud-related directives, by allocating resources for compliance reviews and staff training.
- **Compliance Teams**: Regularly update internal policies to reflect evolving requirements under the EU VAT Directive and AI Act, avoiding potential penalties.

3.3 Sanctions

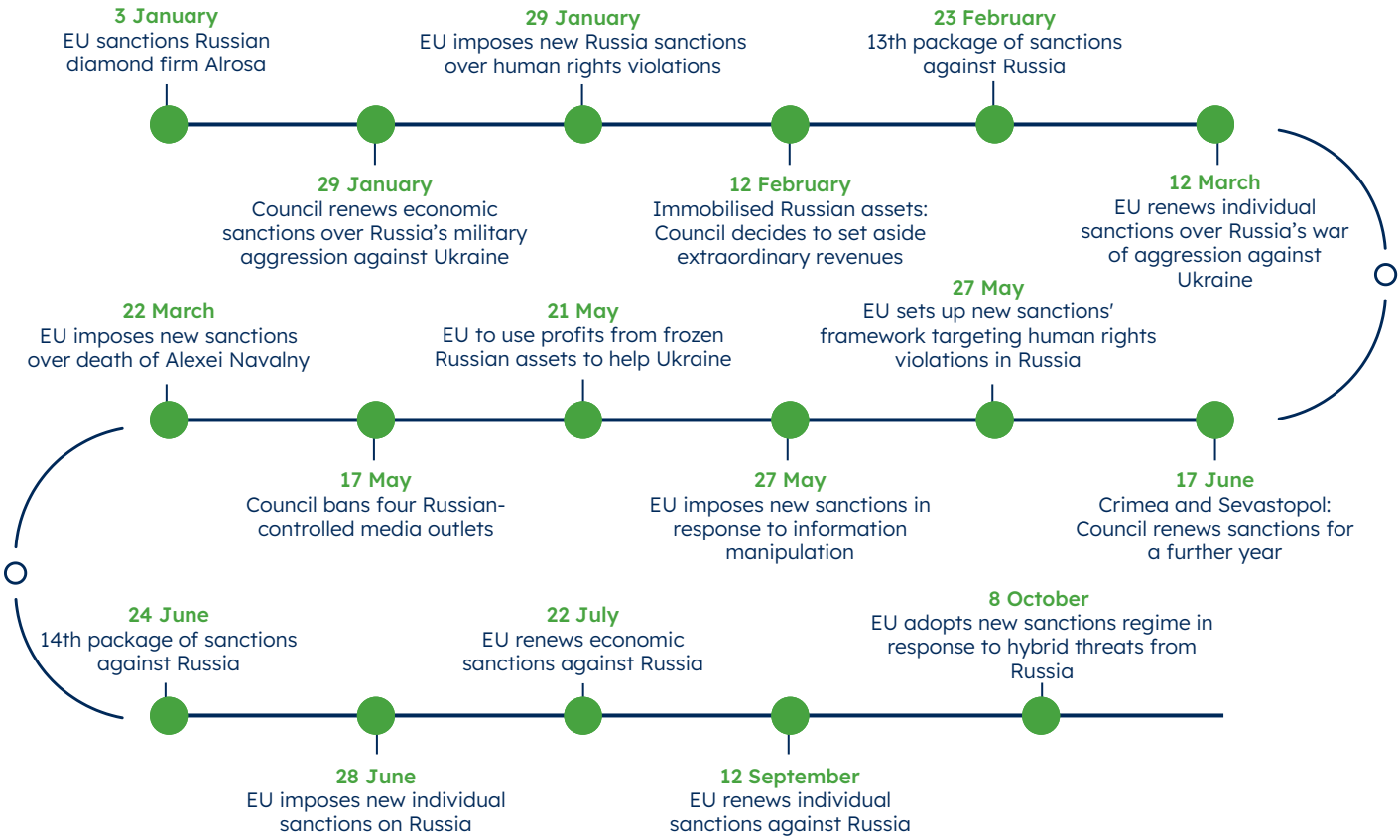
NEW: Directive EU) 2024/1226

In May, new EU-wide rules to harmonise criminal offences and penalties for violating EU sanctions came into force. Member States are now required to impose effective and proportionate criminal penalties for intentional sanctions breaches including making funds available to or failing to freeze assets of sanctioned entities and entering into prohibited transactions with sanctioned states. Aligning with EU objectives to enhance corporate transparency and liability in financial crime compliance, in-scope corporations are also liable if offences are committed by leaders within the organisation, facing penalties such as disqualification from business activities and licence revocation.

Russian Sanctions

In a year which included the second anniversary of Russia's invasion of Ukraine in February 2023, the EU double downed on its implementation and enforcement of targeted financial sanctions, having adopted its 13th and 14th packages of restrictive measures against Russia.

The 13th sanctions package, introduced in February on the second anniversary of Russia's invasion of Ukraine, targeted businesses connected to Russia's military-industrial complex, imposing broad sanctions on multiple sectors. The 14th sanctions package, implemented in June 2024, focused on specific sectors like energy and technology, particularly targeting liquified natural gas (LNG) imports and advanced technology exports. The targeted sanctions have forced businesses to re-evaluate their compliance protocols and supply chains to ensure they align with the evolving regulatory landscape.



Source: Timeline - EU sanctions against Russia

EU Sanctions Key Actions

1 Strengthen Internal Governance and Oversight

- **Boards and CEOs**: Ensure comprehensive governance frameworks to address new EU sanctions rules, including accountability for intentional breaches and corporate liability.
- **Legal and Compliance Teams:** Establish clear escalation protocols to manage risks tied to sanctioned entities, ensuring alignment with EU objectives.

2 Enhance Sanctions Screening and Monitoring

- **Operations and Technology Teams:** Upgrade sanctions screening systems to monitor evolving EU sanctions lists, particularly for sectors targeted by the 13th and 14th packages.
- **Compliance Teams**: Conduct ongoing due diligence on supply chains and business relationships to ensure alignment with new sanctions on LNG imports and advanced technology exports.

3 Implement Robust Training & Awareness Programmes

- **Boards and Compliance Teams:** Develop training sessions tailored to leadership and frontline staff to ensure awareness of criminal penalties for intentional breaches.
- **Legal Teams**: Provide updates on sanctions compliance protocols and the implications of the new directive for in-scope corporations.

4 Conduct Regular Risk Assessments

- **Risk Management Teams:** Evaluate potential exposure to sanctioned entities and activities, including transactions linked to Russia's military-industrial complex.
- **Operations Teams**: Incorporate sector-specific risk assessments, particularly in energy and technology, to adapt to targeted sanctions measures.

5 Prepare for Enforcement Actions

- **Legal and Compliance Teams**: Establish a response plan for regulatory inquiries, ensuring documentation of actions taken to freeze assets or block prohibited transactions.
- **Boards and CEOs**: Allocate resources to address potential penalties such as disqualification from business activities or licence revocation for non-compliance.

3.4 Digital Assets

France

NEW: **Ordinance No. 2024-936**

The Ordinance, published in October, aligns French national law with the EU updated framework on crypto assets, and specifically the Market in Crypto-Assets (MiCA) Regulation. The Ordinance has and will enter into effect in increments, with some provisions, for instance those related to e-money tokens having entered into force in October, with others relating to the regime to supervise crypto assets service providers entering into force on December 30th. Further provisions will enter into force when the grandfathering period for currently registered crypto asset service provided ends, on 1 July 2026.

European Union

NEW: Markets in Crypto Assets (MiCA)

Certain provisions of MiCA entered into force in increments throughout the year. The landmark Regulation introduced common rules on the issuance of crypto assets, including stablecoins (known under the regulation as E-Money Tokens (EMT) and Asset-Referenced Tokens (ART), and on compliance expectations for CASPs. The increased focus on mitigating risks in the digital asset space signals a need for stronger governance, and CASPs will need to remain cognisant of the evolving regulations and their new requirements.

Chapters covering the issuance of ART and EMT entered into effect on 30th June. The new rules also cover the offering to the public and admission to trading of EMTs and require Issuers of ART and EMT to be established and authorised in the EU. The rules also include disclosure obligations, requirements to adopt systems and controls to identify and manage certain risks, custody and reserve asset requirements, and additional requirements for issuers of "significant" EMT / ART, amongst other measures. On 30th December, the remaining provisions of MiCA will come into force, including chapters related to issuance and offering of non-ART or non-EMT (e.g. utility tokens), requirements for CASPs and market abuse. Existing CASPs within EU have 18 months transition period to meet the requirements and secure authorisation under MiCA before 1st June 2026.

The European Securities and Markets Agency (ESMA) published two sets of drafted Technical Standards in March and June to accompany the application of MiCA provisions, which firms should ensure are reviewed to aide compliance with new MiCA requirements.

NEW: EBA 'Travel Rule' Guidance on ML/TF risks

Following the 2023 implementation of the FATF 'Travel Rule' principle in EU law, whereby CASPs are required to include information about the originator and beneficiary for transparency and traceability of digital asset transactions, the EBA released guidance for CASPs on their requirements. The guidelines provide detailed instructions on the specific information that must be collected, the format in which it should be transmitted, and the steps to be taken when information is missing or incomplete. The guidelines are designed to promote a common and harmonised implementation of the travel rule across the EU, ensuring consistent and effective enforcement across not only Member States, but the CASPs operating within them.

EXTENDED: EBA ML/TF Guidelines to CASPs

In January, the EBA extended its Guidelines on ML/TF risks to CASPs, highlighting the risk factors and mitigating measures firms must consider and adopt. The non-exhaustive list of risk factors, which may indicate the CASP's exposure to higher or lower levels of the ML/TF risk due to its customers, products, delivery channels and geographical locations, are a vital tool for firms completing their firm-wide risk assessments. The extended Guidelines are in part addressed to credit and financial institutions that have CASPs as their customers or which through their operations are exposed to crypto assets. The EBA's granular guidance on ongoing and emerging sector-specific risks is relevant to CASPs as well as adjacent sectors. Firms should evaluate whether their current risk management frameworks adequately address these new requirements, particularly concerning due diligence and record-keeping processes.

EU Digital Assets Key Actions

1 Align with MiCA Requirements

- **Boards and CEOs**: Oversee strategic adjustments to meet MiCA requirements, including governance, risk management, and reserve asset obligations for ART and EMT issuers.
- **Compliance Teams:** Review and update policies to address MiCA provisions entering into force in December 2024 and the 18-month transition period for CASPs to secure authorisation by June 2026.

2 Implement the Travel Rule and EBA Guidelines

- **Compliance Teams**: Ensure adherence to the FATF Travel Rule by implementing robust systems to collect and transmit originator and beneficiary data for digital asset transactions.
- **Operations Teams**: Collaborate with technology providers to integrate data-sharing tools that meet EBA's harmonised implementation standards.

3 Strengthen ML/TF Risk Assessments

- **Fraud and Risk Teams:** Leverage EBA's extended ML/TF Guidelines to enhance firm-wide risk assessments, focusing on customer profiles, product delivery channels, and geographic exposure.
- **Boards and CEOs**: Allocate resources to ensure ML/TF mitigation measures align with the higher-risk nature of crypto transactions.

4 Prepare for Implementation of French Ordinance

- **Legal Teams**: Monitor the phased rollout of France's Ordinance No. 2024-936 and its alignment with MiCA to ensure compliance with national and EU-wide requirements.
- **CASPs**: Update operational processes to meet specific provisions for EMTs and ARTs, ensuring readiness for the July 2026 grandfathering deadline.

5 Engage with ESMA and EBA Technical Standards

- **Compliance Teams:** Regularly review ESMA's drafted Technical Standards and EBA guidelines to integrate regulatory updates into compliance frameworks.
- **Legal Teams:** Maintain proactive communication with regulators to understand expectations and ensure seamless adoption of technical standards.

3.5 Enforcement

A major criminal network involved in a sophisticated VAT fraud scheme was dismantled through the combined efforts of Europol, the European Public Prosecutor's Office (EPPO), and law enforcement authorities from 16 EU countries. The investigation, codenamed Admiral 2, uncovered a vast operation in which criminals exploited EU VAT exemptions on cross-border transactions. The fraud, centred around popular electronic goods, resulted in an estimated VAT loss of €297 million.

During the coordinated action day, 32 individuals were arrested, and authorities seized over €47.5 million worth of smartphones and other electronics, several luxury cars, and €126,965 in cash. Additionally, 62 bank accounts holding a combined total of over €5.5 million were frozen. These preliminary figures are expected to evolve as investigations continue.

The Admiral 2 investigation is linked to a previous probe, Operation Admiral, which was launched in November 2022. This earlier operation revealed the largest VAT fraud scheme ever uncovered in the EU, with estimated damages now reaching €2.9 billion. Both investigations uncovered that the same criminal network used similar methods and infrastructure as those in Operation Admiral. The network involved the creation of companies across 15 EU Member States that sold electronic goods valued at €1.48 billion. While end customers paid VAT, the selling companies disappeared without remitting the collected tax to national authorities, while other fraudulent companies claimed VAT reimbursements, contributing to the massive loss.

This case highlighted the complex and evolving nature of financial crimes, particularly within the context of EU VAT regulations, underscoring the need for heightened vigilance and enhanced enforcement measures across the region.

Key statistics

- **VAT Loss: €297 million (Admiral 2) and €2.9 billion (Operation Admiral)**
- **Seized Assets: Electronic goods worth €47.5 million, cash €126,965, luxury cars, 62 frozen bank accounts with a combined total of over €5.5 million**
- **32 individuals were arrested during the coordinated action day**

4 Hong Kong & Singapore

Hong Kong and Singapore continued to cement their positions as leading Asian financial hubs in 2024, which has included fostering the growth of a robust legal and regulatory framework to combat financial crime.

In Hong Kong, initiatives such as the Hong Kong Monetary Authority (HKMA) consultation on information sharing and the progression of the **AMLS** Project underscored the regulator's commitment to fostering an outcomes-based approach to compliance and promoting firms' adoption of technological solutions including RegTech to combat financial crime. Meanwhile, Singapore has solidified its position as global financial hub through legislation such as AML and Other Matters Bill, the Corporate Service Providers Bill, and initiatives like the COSMIC platform, which enhance inter-firm collaboration to tackle ML/TF. Both jurisdictions are emphasising collaboration between regulators and, industry players, at home and abroad, while integrating cutting edge technologies to address evolving threats like cyber-enabled fraud and the exploitation of new technologies for illicit means.

For 2025, a focus on fraud will remain on the agenda for regulators in both Hong Kong and Singapore. In Hong Kong, the HKMA will continue to promote proportionate and outcomes-based approaches to financial crime risk mitigation and prevention, whilst in Singapore, Monetary Authority of Singapore (MAS) will continue to promote pragmatism and proactivity at firm level in the identification and assessment of evolving threats and vulnerabilities.

4.1 AML/CTF/CPF

Hong Kong

NEW: HKMA Consultation on A.I Information Sharing

In January, the HKMA launched a public consultation on its proposal to allow Authorised Institutions (A.Is) to share information on customer accounts with the aim of preventing and detecting financial crime. The approach reflects the centrality of information sharing and regulator-industry collaboration to the HKMA's anti-financial crime strategy. AIs may identify suspicious activities within their own systems but may not have visibility into broader networks of accounts used by criminals. Sharing information between AIs would help close this gap.

The consultation results indicated that most respondents supported a voluntary information sharing initiative. In future legislative amendments and guidance, the HKMA will not propose a statutory obligation on AIs to share information, specify that information shared should be limited to what is relevant and necessary to detect crime, and that information sharing won't constitute 'tipping off'. Although not a requirement, information sharing will be encouraged by the HKMA. If they are to get involved, firms will need to establish formal agreements and protocols with other institutions for secure data sharing, which align with data protection requirements.

NEW: HKMA Effective Execution of Risk-based Approach for CDD

In February, the HKMA published its observations from ongoing supervisory engagement with AIs on the execution of the

risk-based approach (RBA) for CDD. The HKMA recommended that, beyond adopting a risk-based approach to CDD at onboarding, CDD measures should be aligned with the associated risks throughout the process, including customer information requests. Firms were reminded to focus on risk differentiation, proportionality, and avoiding a "zero failure" regime when designing and implementing an RBA which balances regulatory requirements and customer-centric practices In February, the HKMA published its observations from ongoing supervisory engagement with AIs on the execution of the risk-based approach (RBA) for CDD. The HKMA recommended that, beyond adopting a risk-based approach to CDD at onboarding, CDD measures should be aligned with the associated risks throughout the process, including customer information requests. Firms were reminded to focus on risk differentiation, proportionality, and mitigation when designing and implementing an RBA which balances regulatory requirements and customer-centric practices

NEW: HKMA AML/CTF Surveillance Capability Enhancement Project (AMLS)

The HKMA provided an update on the progress of its previously launched "AML/CTF Surveillance Capability Enhancement Project" (AMLS), a response to the need to modernise AML supervision amidst the risks and opportunities presented by new and emerging technologies, and the rapid, global nature of financial crime flows. AMLS was found to assist AIs in shifting from regulatory compliance to proactively prioritising outcomes in managing financial crime risks. The Project is illustrative of the HKMA's increasing prioritisation of assessing the adoption of new technologies and RegTech solutions to produce outcomes-based AML. The impact of AMLS on A.Is' attitudes towards risk has resulted in the HKMA's supervision being targeted to higher risks areas. Manual processes are increasingly being eradicated in favour of automation, including horizon scanning processes underpinned by specialised and granular data which have promoted pragmatic approaches to risk identification and response.

NEW: HKMA Guidance on the use of Artificial Intelligence for Monitoring Suspicious Activities

Based on insights gained through AMLS, the HKMA committed to issuing practical information to Authorised Institutions on the responsible use of AI in AML, focusing on screening and transaction monitoring. The HKMA has been at the forefront of promoting risk-based experimentation with AI, having published principles for Authorised Institutions on its use in 2019. In its most recent publication, the HKMA encouraged A.Is to enhance their monitoring of technology-based risks, while maximising industry intelligence sharing in their adoption. The use of AI has proven to make firms' ongoing monitoring systems more risk-based and therefore targeted to higher-risk activities. Authorised Institutions are required to undertake a feasibility assessment on the use of AI in their own systems and processes, and based on its outcome, an implementation plan which considers all risks, dependencies, and required actions. The feasibility study and implementation plan must be submitted to the HKMA by the end of March 2025.

2025 Outlook

Hong Kong Monetary Authority (HKMA)

The HKMA's approach to regulation and supervision will remain grounded in proportionate and outcomes-based strategies in 2025. Supervised firms will be encouraged to test and implement new technologies, including AI in this manner, striving for efficiency and effective results. As the final year of the 'Fintech 2025' strategy, announced in 2021, approaches, the HKMA remains committed to driving full bank digitalisation and readying the financial landscape for a Hong Kong Central Bank Digital Currency (CBDC) by the end of 2025. This will involve the continued promotion of various new technologies, including AI, to streamline the assessment and response to financial crime risks across A.Is.

Securities and Futures Commission (SFC)

At the beginning of the year, the SFC outlined its strategic priorities for 2024-26, emphasising the role of enhanced regulatory oversight and

increased public-private collaboration to combat evolving financial crime threats. The priorities will impact the SFC's supervision of licensed corporations, financial institutions, market participants, investors, and technology providers. The SFC's emphasis on the need for supervised entities to proactively respond to the new financial crime threats presented by new technologies highlights the growing need for continued technological investment at firm-level. The strategy is reflective of a shift to sophisticated, tested approaches to financial crime prevention and compliance, beyond tick-box and potentially outdated frameworks.

Singapore

NEW: Prevention of Proliferation Financing and Other Matters Act 2024

Singapore passed a new Act aimed at strengthening laws against the financing of weapons of mass destruction (WMD) sectors in a broader range of sectors, introducing stricter regulations and enforcement powers to align with international standards. This was in line with FATF recommendations, which emphasise the need for countries to implement robust measures to prevent the funding of activities related to WMD proliferation. The now in-scope sectors are precious metals and stones dealers, moneylenders, pawnbrokers, as well as select legal service providers. The legislation aligns existing CPF requirements for the sectors, including audit and reporting obligations, in line with FATF recommendations. As well as broadening the applicability of CPF obligations to more firms, the enforcement and oversight powers of Singaporean authorities are also enhanced by the amending act, with enforcements in place for inaccurate or incomplete regulatory reporting. Newly in-scope firms will need to review and update their procedures, reporting practices, and provide further training and awareness to staff as to ensure their CPF frameworks are compliant.

NEW: Anti-Money Laundering and Other Matters Act

In August, the Anti-Money Laundering and Other Matters Act (AMLOM) was passed in Parliament. Having been first introduced in July, the Act has enhanced the powers of law enforcement agencies to escalate and prosecute ML offences and align the ML/TF requirements of casino operators in Singapore with FATF standards. The Act introduced new provisions and amendments to the Casino Control Act, requiring casino operators to conduct more robust CDD checks. Government agencies' abilities to detect ML/TF will be strengthened through improved data sharing and prosecutorial powers to handle seized or restrained assets linked to financial crime.

NEW: Corporate Service Providers Act and the Companies and Limited Liability Partnerships (Miscellaneous Amendments) Act

The Ministry of Finance of Singapore and the Accounting and Corporate Regulatory Authority (ACRA) introduced new legislative changes with the passage of the Corporate Service Providers (CSP) Act and the Companies and Limited Liability Partnerships (Miscellaneous Amendments) Act passed in July. The Acts are designed to operate in tandem to strengthen the regulatory regime for CSPs and enhance the transparency of beneficial ownership data held by government and regulatory authorities. All registered CSPs will be in scope of AML/CTF/CPF requirements, with criminal liability on breaches in place for CSPs and senior management. Nominee directors and shareholders will be required to disclose their nominee status and the identities of their nominators to ACRA, with individuals prohibited from acting as nominee directors for business purposes unless appointed by registered CSPs.

NEW: The Money Laundering National Risk Assessment (ML NRA)

The ML NRA released in June saw the consolidation of new and emerging threats identified by MAS, Singapore law enforcement agencies, and FIU. Singapore's key ML risks derived from predicate offences committed abroad for 2024 included cyber-enabled fraud, organised crime, and corruption. Banking was assessed as the having the highest sectoral risk, vulnerable to potential exploitation such as self-laundering and third-party laundering.

Payment Institutions, Asset Managers, and Licensed Trust Companies were among the sectors identified as medium risk. Firms across Singapore, not least those assessed within the NRA specifically, can use the NRA to enhance their risk detection, monitoring, and response frameworks, ensuring that these are reflective of the most pertinent risks facing their sector.

NEW: Terrorism Financing National Risk Assessment (TF NRA)

The MAS published its Terrorism Financing National Risk Assessment and National Strategy for CTF in July, offering a current evaluation of terrorism financing risks within Singapore. This comprehensive update is intended to help both private and public sector stakeholders across financial and non-financial sectors gain a clearer understanding of present threats and vulnerabilities affecting the region. Money remittance services were designated as high-risk, while cross-border online payments were flagged as an emerging channel potentially enabling terrorism financing activities. Banks and digital payment token (DPT) service providers were categorised as medium-high risk, while non-profit organisations, cross-border cash transfers, and dealers in precious goods were assessed as medium-low risk sectors.

To counter these risks, MAS pledged to advance its CTF strategy with a stronger and more systematic approach. It has committed to a rigorous framework for identifying risks, enforcing robust regulatory measures, taking decisive enforcement actions, and fostering new, collaborative partnerships across sectors. Firms, particularly those in the financial and payment services industries, should proactively strengthen their internal CTF controls, conduct comprehensive risk assessments, and actively engage in MAS's collaborative efforts to address and mitigate terrorism financing risks. By adopting these measures, firms can play a crucial role in reinforcing Singapore's defences against terrorism financing.

NEW: COSMIC

On April 1, 2024, MAS launched COSMIC, the 'Collaborative Sharing of ML/TF Information and Cases', a centralised digital platform aimed at enhancing the sharing of customer information among FIs to combat ML/TF/PF globally.

Backed by six major commercial banks in Singapore including Citibank and HSBC, COSMIC is allowing FIs to share information with one another on customers presenting multiple 'red flag' indicators of suspicious behaviour and potential financial crime threats. With red flags based on defined indicators of suspicious activity, the inter-firm sharing mechanism is designed to foster common knowledge of new and emerging suspicion indicators, while protecting legitimate customers' privacy. The platform targets key financial crime risks, including the misuse of legal persons and trade finance for illicit purposes allowing. COSMIC to bolster Singapore's ability to maintain a well-regulated financial ecosystem.

2025 Outlook

MAS have refreshed their Financial Services Industry Transformation Map (ITM) 2025 which sets out their growth strategies to further strengthen Singapore's position as a leading international financial centre in Asia.

A key strategy includes "Shape the Future of Financial Networks":

- Expand cross-border payment linkages with regional economies (e.g. real-time payment linkages, Project Nexus)
- Explore potential of distributed ledger technology in promising use cases (e.g. cross-border payments
- Support tokenisation of financial and real economy assets
- Enable digital currency connectivity

Asia AML Key Actions

1 Leverage Information Sharing for Risk Mitigation

- **Boards and CEOs:** Support participation in platforms like HKMA's proposed voluntary information-sharing initiatives or Singapore's COSMIC to strengthen financial crime prevention efforts.
- **Compliance Teams**: Establish secure data-sharing agreements & protocols to align with regulatory expectations while maintaining data privacy standards.

2 Enhance Risk-Based CDD Practices

- **Compliance Teams**: Align CDD practices with HKMA's recommendations by adopting proportional, risk-differentiated approaches throughout the customer lifecycle.
- **Operations Teams**: Implement advanced analytics & AI to ensure customer monitoring adapts to evolving risk profiles, avoiding a "zero-failure" mindset.

3 Adopt and Scale New Technologies

- **Fraud and Tech Teams:** Conduct feasibility studies on the use of AI for TM and suspicious activity detection, as mandated by HKMA, and submit implementation plans by March 2025.
- **Boards and CEOs:** Prioritise investment in tech to meet digitalisation goals under initiatives like HKMA's AMLS and Singapore's ITM 2025.

4 Strengthen Sector-Specific Compliance Frameworks

- **Regulated Firms (Singapore):** Update internal policies to meet new CPF requirements under the Prevention of PF Act and enhance DD for high-risk sectors like precious goods dealers & money remittance services.
- **Licensed Corporations**: Use risk assessments such as Singapore's ML NRA & TF NRA to align practices with sector-specific vulnerabilities & emerging risks.

5 Foster Cross-Border Collaboration and Compliance

- **Legal and Compliance Teams:** Engage with regional regulators to harmonise AML/CTF frameworks, focusing on cross-border payment linkages & shared intelligence on red flags.
- **Risk Management Teams:** Incorporate findings from international initiatives into monitoring systems to strengthen global compliance capabilities.

4.2 Fraud

The increasing digitalisation of financial services across Asia has widened customer access to quicker and easier payments, but this has been coupled with the increasing exploitation of new technologies for criminal activity, including digital fraud. In 2023, the HKMA estimated fraud losses to victims to have reached HK$7.2bn. In Singapore, MAS collaborated with regulated firms throughout the year in promoting holistic anti-fraud efforts in areas including phishing scams. The importance of government and regulatory collaboration with industry was highlighted once more towards the end of the year, with the introduction of the Protection from Scams Bill. Fraud mitigation and prevention will certainly remain on the legislative and regulatory agendas in both Hong Kong and Singapore in 2025.

Hong Kong

NEW: Anti-Scam Consumer Protection Charter 2.0.

The HKMA continued to enhance its efforts in combating digital fraud with the launch of the Anti-Scam Consumer Protection Charter 2.0 in April. Following the success of the original Charter, the second iteration includes more FIs across more financial sectors, reflecting the growing industry need for collaborative action. The Charter outlines four key principles to help the public identify credit card scams and digital frauds, including a commitment by participant firms not to send instant electronic messages containing embedded hyperlinks and to disseminate anti-scam education. For participating firms, the Charter translates into operational requirements, such as the enhancement of real-time fraud monitoring and detection tools to better identify suspicious activities. With the support of regulatory bodies and the broader business community, the Charter reinforces the importance of robust safeguards to protect the public from rising fraud threats, in which all firms involved in the financial services landscape serve a critical role.

2025 Outlook

NEW: HKMA Public Consultation Paper on proposal for information sharing among Authorised Institutions to aid in prevention or detection of crime

In January 2024, the HKMA published a consultation paper detailing proposals for enhanced information sharing among Authorised Institutions (AIs) as a strategic measure to prevent and detect financial crime, including fraud. This initiative is a significant step in modernising Hong Kong's financial crime prevention framework and has sparked a broader review of the Banking Ordinance, highlighting the need for legislative alignment with contemporary risks and technological advancements. The proposed measures aim to facilitate greater collaboration between financial institutions, enabling them to identify and disrupt complex illicit financial networks more effectively.

The consultation underscored the critical importance of balancing data privacy with the need for transparency, a challenge that resonates globally as financial institutions prepare for heightened regulatory expectations. The planned integration of these proposals into a Bill for introduction to the Legislative Council in 2025 signals the HKMA's proactive stance in addressing the evolving threat landscape. This legislative effort is expected to enhance regulatory clarity and operational efficiency for firms, setting a new benchmark for compliance standards in the region.

For firms operating in or with Hong Kong, these developments carry significant implications. Enhanced information-sharing mechanisms will require institutions to invest in advanced compliance systems and robust data governance frameworks. The alignment of these measures with global trends, such as the AMLA initiatives, reinforces the need for firms to adopt a proactive and harmonised approach to financial crime compliance. As 2025 approaches, HKMA's proposals will serve as a critical reference point for financial institutions aiming to remain at the forefront of regulatory excellence while safeguarding the integrity of the financial system.

Singapore

NEW: MAS Eradication of OTPs

In July, MAS and the Association of Banks in Singapore (ABS) announced that major retail banks will begin phasing out the use of One-Time Passwords (OTPs) for customers who use digital tokens, enhancing protection against phishing scams. Customers now authenticate bank logins via their digital tokens, eliminating the need for OTPs that scammers could steal or trick customers into disclosing. This measure, introduced to address evolving scam tactics like fake banking websites, will strengthen the login process and help safeguard bank accounts. In line with the regulator's ongoing commitment to cross-sector collaboration, MAS will continue to collaborate with firms on improving anti-scam measures and educating consumers on practical steps they can take to detect and avoid fraud.

2025 Outlook

NEW: The Protection from Scams Bill

In November, the Singapore Parliament introduced the Protection from Scams Bill. The bill comes as scam cases have multiplied exponentially in Singapore, increasing by 5 times between 2019 and 2023. The bill introduces restriction orders, which if issued by Police, will restrict banking transactions of an individual if there is a reasonable belief that they will transfer funds to a scammer. Orders can initially be imposed for a maximum of 30 days, with the possibility of up to five extensions, and they will only be issued for scam cases that are conducted substantially via digital or telecommunication channels. If a restriction order is issued, it will by default be issued to the seven Domestic Systemically Important Banks in Singapore, the major retail banks which manage most of the country's consumer deposits, as to ensure anti-fraud operations across the financial sector do not operate in siloes but are instead built on communication and collaboration.

Key statistics

- In the first half of 2024, Hong Kong recorded **19,897** deception cases, accounting for **43.9%** of all crimes during this period. Notably, **62.3%** of these cases were internet-related, with total financial losses amounting to **HK$4.48** billion

- Between January and June 2024, Singapore reported **26,587** scam cases. The total financial loss from these scams was at least **S$385.6** million

Asia Fraud Key Actions

1 Adopt and Enhance Real-Time Fraud Monitoring

- **Compliance Teams**: Implement advanced fraud detection tools to align with HKMA's Anti-Scam Consumer Protection Charter 2.0, focusing on real-time detection of suspicious transactions.
- **Technology Teams:** Invest in automation and AI-based monitoring to identify fraudulent patterns and respond swiftly to potential threats.

2 Strengthen Authentication Protocols

- **Boards and Technology Teams:** Phase out outdated authentication methods like OTPs and transition to secure alternatives, such as digital tokens, in line with MAS recommendations.
- **Operations Teams**: Educate customers on using new authentication methods to ensure a smooth transition and minimise fraud risks.

3 Enhance Cross-Industry Collaboration

- **Boards and Compliance Teams:** Participate in collaborative anti-fraud initiatives like Singapore's Protection from Scams Bill and HKMA's Anti-Scam Charter to strengthen sector-wide defences.
- **Legal Teams**: Establish protocols for responding to restriction orders, ensuring timely compliance and seamless interbank communication.

4 Promote Consumer Awareness and Education

- **Marketing and Communications Teams**: Disseminate anti-scam education materials to help customers identify phishing scams and other fraud threats.
- **Boards and CEOs**: Champion public-facing initiatives that demonstrate the firm's commitment to safeguarding customers.

5 Develop Fraud Resilience Strategies

- **Risk Management Teams:** Conduct scenario-based testing to assess the effectiveness of fraud prevention measures and identify gaps.
- **Boards and Technology Teams**: Allocate resources to emerging anti-fraud technologies, ensuring scalability and adaptability to evolving scam tactics.

4.3 Digital Assets

Hong Kong

NEW: HKMA Legislative Proposal to Introduce Stablecoin Regulatory Regime

The Financial Services and the Treasury Bureau (FSTB) and the HKMA published the conclusions of the consultation on the proposed regulatory regime for Hong Kong stablecoin issuers was published in July. The legislative proposal aims to establish licensing requirements for fiat-referenced stablecoin (FRS) issuers, accompanied by requirements aligned with international standards in terms of reserve requirements, stabilisation mechanisms, disclosures, redemption requirements, amongst others, enhancing transparency and governance. Issuers must have a physical presence in Hong Kong, and there is a prohibition on paying interest akin to that in the EU's MiCA regime. Only stablecoins issued by a license issuer can be offered to retail investors. The FSTB and HKMA will progress in finalising the legislation and introduce a bill to the Legislative Council.

NEW: Stablecoin Issuer Sandbox

The FSTB and HKMA also announced the launch of a stablecoin issuer sandbox aimed at providing a structured environment for firms planning on developing fiat-referenced stablecoins to engage with regulators, test their business models and gain a better understanding of how to comply with regulatory requirements. The sandbox offers a controlled scope for testing stablecoin issuance under regulatory oversight, enabling participants to address potential risks and ensure compliance. In July, HKMA announced a first batch of three sandbox participants for Virtual Assets regulation.

NEW: Government Consultation on Legislative Proposal to Regulate OTC Virtual Asset Trading

In February, the Hong Kong government initiated a public consultation on the introduction of a licensing regime for providers of over the counter (OTC) virtual asset (VA) trading services. This proposal builds upon the regulatory framework introduced in June 2023, which mandated licensing for VA trading platforms under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615). The new licensing regime focuses on regulating VA spot trading services, with the aim of mitigating ML/TF risks and enhancing customer protection. Under the proposal, providers of OTC VA trading services would be required to obtain a license from the Commissioner of Customs and Excise (CCE). The consultation closed in April 2024, and results may be seen in 2025.

NEW: Project Ensemble Sandbox

In August, the HKMA launched the Project Ensemble Sandbox, designed to facilitate firms' testing of tokenisation use cases in their operations and aide the financial sector's exploration of how tokenisation could improve efficiency. Similarly to other HKMA initiatives throughout the year, the sandbox is built on industry collaboration, involving banks, technology companies and regulators to develop industry standards on the use of tokenisation. The sandbox will provide a controlled testing environment with regulatory oversight, helping to strengthen Hong Kong's position at the centre of technological experimentation in finance, both across Asia and globally.

Singapore

UPDATED: Payment Services Act

MAS implemented significant amendments to the Payment Services Act, expanding the scope of regulated payment services to cover DPT providers offering custody or facilitating the transmission or exchange of DPT. These changes, effective from April 2024, impose AML/CFT, customer protection and financial stability requirements on these providers, who require a successful licence application to continue providing these activities. Impacting actors involved in digital payments, cryptocurrencies, and cross-border money transfers, these new regulations require firms to

review their operational processes, segregate customer assets, ensure compliance with the new requirements, and submit detailed reports to MAS. Firms must also meet transitional deadlines to continue offering services, including submitting license applications and external auditor reports. Failure to comply may result in having to cease operations.

NEW: Expansion of Asset Tokenisation for Financial Services

MAS expanded its asset tokenisation initiatives aimed at testing and developing use cases for asset tokenisation in financial services in partnership with industry associations and global financial institutions, with a focus on creating industry-wide standards for tokenisation in fixed income, foreign exchange (FX), and asset and wealth management. A key development is the Global Layer One initiative, which aims to establish a shared ledger infrastructure for tokenised assets, supporting international financial transactions. The initiative impacts sectors like asset management, banking, and foreign exchange, with an emphasis on improving the efficiency of cross-border transactions. This initiative, which builds on previous ones like Project Guardian, is testament to how asset tokenisation is being increasingly seen by regulators and leader financial institutions as presenting significant potential to enhance the operation of cross-border financial transactions. For firms, this means they should consider how they can be amongst the leaders in exploring these use cases, and reflecting on how to adapt their processes and controls frameworks to the use of blockchain technology in their operations.

Key statistics

With the region's adoption of crypto estimated at **22%** , APAC stands significantly above the global average of approximately **7.8%** . This surge isn't driven by a single factor but by a complex interplay of factors —rising internet penetration, evolving regulatory environments, speculative interest, practical utility, growing understanding, and most compellingly, a deep-seated belief in crypto as the future.

Source

Asia Digital Assets Key Actions

1 Prepare for Stablecoin Regulations

- **Stablecoin Issuers:** Begin aligning with HKMA's proposed requirements, including physical presence, reserve management, and redemption mechanisms, to secure future licensing.
- **Compliance Teams**: Evaluate processes for disclosure, governance, and interest restrictions in preparation for HK's forthcoming stablecoin legislation.

2 Leverage Regulatory Sandboxes

- Tech and Innovation Teams: Participate in initiatives like HK's Stablecoin Issuer Sandbox and Project Ensemble Sandbox to test and refine stablecoin and tokenisation models under regulatory oversight.
- Boards and Risk Teams: Use insights gained from sandbox participation to adapt risk management frameworks and operational controls to meet regulatory expectations.

3 Adapt to Expanded Payment Services Act Requirements (SG)

- **Payment Providers**: Review and update AML/CFT processes, customer asset segregation practices, and reporting mechanisms to comply with MAS's expanded licensing requirements for DPT services.
- **Operations Teams:** Ensure transitional compliance deadlines are met to avoid disruptions to service offerings.

4 Explore Tokenisation Use Cases

- Financial Institutions: Engage with MAS and HKMA initiatives to explore tokenisation's potential for fixed income, FX, & cross-border payments.
- Tech Teams: Develop blockchain capabilities to support tokenised assets, considering shared ledger infrastructure like Singapore's Global Layer One initiative.

5 Strengthen Governance for Virtual Asset VA Trading

- OTC VA Providers (HK): Prepare for upcoming licensing requirements by enhancing AML/CFT frameworks and customer protection measures.
- Compliance Teams: Monitor developments from HK's OTC VA trading consultation & proactively adapt policies to align with anticipated regulations

4.4 Enforcement

The regulatory landscape in the Asia-Pacific (APAC) region is rapidly evolving, with increased scrutiny on AML and fraud controls. Highlighted in the Plenitude Navigating the Maze Paper published in August, recent high-profile cases in Singapore and Hong Kong have exposed significant vulnerabilities, leading to stricter regulations and greater enforcement.

MAS imposed a composition penalty of S$2.5 million on Swiss-Asia Financial Services Pte. Ltd. (SAFS) for multiple breaches of AML/CFT regulations. In addition, MAS issued formal reprimands to SAFS' CEO, Olivier Pascal Mivelaz, and COO, Steve Knabl, for failing to ensure the company's compliance with these critical regulatory requirements.

Between September 2015 and October 2018, SAFS, a wealth and fund management firm, underwent substantial business growth. However, its AML/CFT controls failed to evolve in line with this expansion, leaving the company exposed to heightened financial crime risks. An inspection by MAS uncovered serious shortcomings, including initiating customer relationships before completing CDD, inadequate oversight of high-risk customers, and failing to file suspicious transaction reports (STRs) despite credible indications of potential financial crimes. The company also failed to conduct internal audits to evaluate the effectiveness of its AML/CFT measures.

MAS specifically criticised SAFS' enterprise-wide risk assessment (EWRA) for not adequately addressing key risk factors. Both the CEO and COO were held accountable for endorsing this deficient EWRA and for neglecting to implement regular internal audits over a four-year period, despite the company's significant growth during this time.

This case served as a reminder of the importance of robust AML/CFT controls, particularly for rapidly expanding organisations. It also highlighted the serious regulatory consequences for financial institutions and their leadership when compliance frameworks fail to meet required standards.

HKMA imposed a pecuniary penalty of HK$875,000 on WeChat Pay Hong Kong Limited (WPHK) for breaches of the Payment Systems and Stored Value Facilities Ordinance (PSSVFO). This disciplinary action was taken following an investigation which found that WPHK had contravened section 8Q of the PSSVFO by failing to meet the minimum criterion under section 6(2)(b) of Part 2 of Schedule 3 to the PSSVFO.

The investigation was initiated after WPHK filed a self-report, prompting further examination by the HKMA. The findings revealed that, between 25 August 2016 and 24 October 2021, WPHK did not maintain adequate and appropriate systems of control to comply with the relevant paragraphs of the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Stored Value Facility Licensees). Specifically, WPHK's deficiencies were related to two critical areas: conducting CDD reviews upon trigger events and implementing enhanced due diligence measures to mitigate the risks inherent in high-risk situations involving potential ML/TF.

In determining the disciplinary action, the HKMA considered several factors, including the severity of the findings, the necessity of sending a clear deterrent message to the industry, and WPHK's remedial actions to rectify the identified deficiencies and strengthen its systems of control. Mr Raymond Chan, Executive Director (Enforcement and AML) of the HKMA, emphasised the importance of enhanced due diligence in situations with heightened risks of money laundering and terrorist financing.

This enforcement action underscored the critical need for SVF licensees to establish and maintain robust systems of control to address money laundering and terrorist financing risks effectively.

5 Global

The global section of this report highlights the evolving landscape of financial crime regulation, focusing on the pivotal roles of the Financial Action Task Force (FATF) and the Wolfsberg Group.

In 2024, FATF drove AML/CTF priorities through updated standards, strategic initiatives, and a focus on transparency, beneficial ownership, and Virtual Asset Service Providers (VASPs). Key developments included revised guidance on national risk assessments (NRA) and the broader application of Recommendation 25, alongside efforts to balance financial inclusion with effective risk management under its Mexican Presidency. Updates to high-risk jurisdiction ratings and enhanced public-private collaboration further underscored FATF's adaptive approach.

The Wolfsberg Group complemented these efforts by refining guidance on financial crime risk management, counter-terrorist financing, and suspicious activity monitoring, promoting stronger partnerships and innovative processes.

Financial Action Task Force (FATF)

FATF has continued to actively shape the AML/CTF landscape in 2024 through high-risk listings, renewed strategic priorities, and bolstered benchmark standards. Key priorities have included enhancing guidance on national risk assessments, beneficial ownership transparency, and changes to the jurisdictional assessment process. The FATF has intensified its focus on combating ML/TF/PF in both traditional finance and virtual asset landscapes, issuing a global call to action for member states to strengthen their AML/CTF frameworks across traditional and emerging technologies. Recognising the pivotal role of the Private Sector in achieving this aim, the FATF has fostered stronger public-private partnerships to facilitate the implementation of standards and guidance, particularly in areas including payment transparency and corporate transparency, where private sector participation is key. With the Mexican Presidency of FATF having now commenced, the global standard-setter is set to prioritise financial inclusion, proportionate assessments, and the enhancement of standards on asset recovery, beneficial ownership, and their application to virtual asset service providers (VASPs).

FATF Plenaries: February, June, and October

Three FATF Plenaries took place in 2024, resulting in various changes to assessment ratings and the lists of high-risk jurisdictions, and updated or newly released guidance and best practices.

UK Firms: Firms subject to requirements under the UK Money Laundering Regulations 2017 are reminded that following January updates to the legislation and the removal of Schedule 3ZA, high-risk jurisdiction indexes for EDD purposes must now be based on the latest FATF list. Proactive monitoring of changes to the FATF list is essential as for risk assessment and due diligence methodologies to be up to date.

Grey list additions: Kenya, Namibia, Monaco, Venezuela, Algeria, Angola, Côte d'Ivoire, and Lebanon.

Grey list removals: Barbados, Gibraltar, Uganda, UAE, Jamaica, Türkiye, and Senegal were removed after addressing their deficiencies.

Strategic Initiatives	
Beneficial Ownership	Updated guidance on beneficial ownership to enhance transparency and combat financial crime
Non-Profit Organisations	A renewed focus on protecting non-profit organisations from misuse for terrorist financing
Payment Transparency	Proposed amendments to Recommendation 16 to improve payment transparency
VASPs	The FATF continues to support jurisdictions in regulating and supervising VASPs following a year of slow progress
National Risk Assessments	Revised guidance on national risk assessments to strengthen their effectiveness
Financial Inclusion & Risk-Based Approach	The launch of new initiatives to balance financial inclusion with effective risk management under the new Mexican Presidency

NEW: Guidance on Beneficial Ownership and Transparency of Legal Arrangements

Following the February 2023 revisions to FATF Recommendation 25 on beneficial ownership and the transparency of legal arrangements, the accompanying risk-based guidance was updated in March this year, also as to align with existing guidance on the treatment of legal persons. Practical guidance on identifying and managing risks associated with legal arrangements including trusts are offered for firms, indicative of the international community's ongoing focus on corporate transparency and due diligence. Recommendation 25 was broadened to encompass more legal arrangements and structures, introduce enhanced requirements for identifying and verifying ultimate beneficial owners, and encourage information sharing at firm, state, and international levels. By obtaining input from public consultations and private sector engagement throughout the consultation process, the updated guidance for Recommendation 25 reflects the FATF's holistic approach to improving the transparency of beneficial ownership globally, by working with the many stakeholders required to achieve this.

NEW: Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs

The FATF's latest report highlights the slow pace of global progress in implementing AML/CFT regulations for VASPs. The report found that 75% of jurisdictions were either partially compliant or non-compliant with FATF standards, with no improvement made to this figure since April 2023. The lack of regulatory progress across jurisdictions poses significant risks, as virtual assets and VASPs can be exploited as avenues for financial crime. However, as has been seen across jurisdictions covered in this paper, the digital and virtual asset regulatory landscape continues to make gradual but nonetheless significant strides in experimentation and development, with limiting and mitigating the financial crime vulnerabilities for the technologies a key priority across the UK, EU and some Asian nations.

NEW: Changes to Technical Compliance Assessment Ratings

In October, the FATF updated its process for assessing and identifying high-risk jurisdictions. In line with the new Mexican Presidency's focus on financial inclusion, the revisions will allow the FATF to take a more proportionate approach to reviews, prioritising countries posing the greatest risk to the international financial system while offering more support to developing nations. Under the revised criteria, countries will be prioritised for review if they are FATF members, high-income countries (excluding those with very small financial sectors), or countries with significant financial assets. Less developed countries will largely not be prioritised for review unless they pose a significant risk to the global financial system. If they do and are prioritised, they may see a longer observation period for review.

UPDATED: Money Laundering National Risk Assessment Guidance

Conducting a NRA is a crucial step in understanding and managing ML risk at state and firm level, enabling countries to systematically evaluate and address their specific threats and vulnerabilities. The enhanced FATF NRA guidance provides a detailed framework for conducting NRAs, covering essential aspects such as preparation, risk assessment methodologies, and post-NRA actions, designed to aide countries in strengthening their AML frameworks.

2025 Outlook:

NEW: Public Consultation on Recommendation 16 on Payment Transparency

In 2025, we may see the publication of forthcoming amendments to FATF's Recommendation 16 on Payment Transparency, which were subject to public consultation in 2024. The proposed amendments aim to enhance transparency and security in financial transactions. Key measures include stricter requirements for exemptions on card purchases, limiting cash withdrawals and purchases under specific conditions, improving the quality of payment message information, imposing verification obligations on beneficiary financial institutions, and clarifying the definition of payment chains and net settlement conditions.

NEW: Public Consultation on AML/CTF and Financial Inclusion: Changes to FATF Standards

In line with the Mexican Presidency's new focus on financial inclusion, the end of the year saw proposed uplifts to FATF Standards (specifically Recommendation 1) open to public consultation, the results of which may be published in 2025. The proposed revisions seek to improve financial inclusion by adopting and promoting a more proportionate and simplified risk-based approach, providing greater flexibility and confidence to countries, regulators, and financial institutions when implementing simplified AML/CTF measures, ultimately promoting accessibility to financial services for a wider range of individuals and businesses.

> **"For the next two years under the Mexican Presidency, the FATF will be guided by the principles of inclusivity, diversity, and transparency."**
>
> Elisa de Anda Madrazo, FATF President

The Wolfsberg Group

The Wolfsberg Group, a non-governmental consortium of thirteen leading global banks, continued to play a pivotal role in strengthening the fight against financial crime throughout 2024. Renowned for setting global industry standards, the Group expanded its guidance and resources, responding to the evolving challenges faced by financial institutions. Key updates included enhancements to its **guidance on Swift Relationship Management Application** (RMA) Due Diligence, which provides guidance to FIs for managing non-customer RMAs.

In addition, the Wolfsberg Group actively engaged in consultations to shape the regulatory landscape. Notably, it provided detailed responses to consultations on the **EBA consultation on Travel Rule Guidelines**. These contributions emphasised the Group's commitment to fostering a unified approach to combating illicit financial activity and addressing vulnerabilities in global financial systems.

2024 also marked a significant transition in the Wolfsberg Group's leadership. With the appointment of its **next Executive Secretary**, the group signalled its intention to further amplify its influence on global AML/CFT strategies, prioritising collaboration between financial institutions, regulators, and international organisations. This leadership change aligns with the Group's mission to remain at the forefront of combating emerging threats in an increasingly complex financial environment.

As the financial sector prepares for the heightened regulatory demands of 2025, the Wolfsberg Group's enhanced guidance and tools will be indispensable in helping institutions navigate new compliance requirements while upholding the principles of transparency, accountability, and integrity. By setting robust benchmarks and actively engaging in the global regulatory dialogue, the Group continues to be a cornerstone of the industry's collective efforts to combat financial crime.

2025 Outlook

NEW: Financial Crime Risk Management (FCRM) programmes for effectiveness

New principles were developed to aide FIs' internal audit (IA) teams assess the effectiveness of their Financial Crime Risk Management (FCRM) programs. Centred around compliance with regulations, implementing robust risk controls, and providing valuable information to authorities, audit teams can strengthen FCRM to support in regulatory oversight and assurance, ultimately contributing to a more secure financial system. By reviewing IA processes alongside the Wolfsberg Factors, teams can measure FCRM outcomes and improve their effectiveness. The guidance recommends that IA teams assess the firm's compliance with local laws and regulations, evaluate the effectiveness of its controls, and promote information sharing with relevant authorities.

UPDATED: Statement on Countering Terrorist Financing

The Group revised its 2002 CTF statement to reflect changes in global CTF measures and developments in public-private cooperation. The updated statement incorporates risk-based approaches, enhanced awareness of terrorist financing techniques, and streamlined reporting by firms, technology advances, and stronger public-private partnerships, which have since 2002, significantly improved the detection and prevention of terrorist financing activities.

NEW: Effective Monitoring for Suspicious Activity

Seeking to adopt and promote a more holistic approach to monitoring suspicious activity (MSA), the Group published guidance which broadened MSA to more than transaction monitoring, as to reflect that increasingly, customer behaviour and customer attributes, when combined with the consideration of transactions, can provide a broader insight into potentially suspicious activity. Fundamentally, the Group believes that the increasing volume of suspicious activity report (SARs)/ suspicious transaction reports (STRs) seen across firms

and states is producing disproportionate and ineffective results for broader FCRMs. In its new guidance, the Group encouraged all parties at and below state level to be proactive in the development of innovative techniques to deliver more effective end-to end risk detection capabilities. For FIs, enforcement with government and regulatory authorities is pivotal to produce MSA outcomes which reduce negative impacts on customers, result in valuable information for authorities, and more effectively identify criminal activity. By focusing on high-quality SARs/STRs, firms will be well placed to reduce the burden of low-value reports and improve the overall efficiency of MSA processes not only within their firm, but across the financial system.

Money laundering, terrorism financing, and their predicate offences are fuelling instability, violence, and exploitation worldwide. Safeguarding financial integrity is vital to promoting peace and security, driving sustainable development, and shielding the most vulnerable.

Joint statement by heads of FATF, INTERPOL and UNODC

Global Key Actions

1 Enhance Beneficial Ownership Transparency

- **Compliance Teams:** Align with FATF's updated Recommendation 25 guidance by improving systems to identify and verify ultimate beneficial owners of legal entities and arrangements.
- **Boards**: Oversee the integration of information-sharing protocols to enhance corporate transparency and compliance with beneficial ownership requirements.

2 Adopt Proportionate Risk-Based Approaches

- **Financial Institutions**: Leverage FATF's revised NRA guidance to refine risk-based AML/CTF measures, focusing on balancing financial inclusion with effective risk management.
- **Internal Audit Teams:** Use Wolfsberg Group guidance to assess the effectiveness of FCRM programs, ensuring compliance and alignment with global standards.

3 Improve Suspicious Activity Monitoring (SAM)

- **Risk and Compliance Teams:** Implement Wolfsberg Group recommendations to go beyond transaction monitoring by integrating customer behaviour and attributes for holistic SAM.
- **Technology Teams:** Invest in advanced analytics and AI tools to reduce low-value SARs/STRs and improve detection of high-risk activities.

4 Strengthen Collaboration in Virtual Asset Regulation

- **VASPs and Digital Asset Firms**: Address FATF's findings on non-compliance in virtual asset sectors by adopting robust AML/CTF frameworks, including reporting and monitoring mechanisms.
- **Regulators and FIs**: Participate in public-private partnerships to enhance regulatory oversight & operational compliance for VA's.

5 Focus on High-Quality Reporting & Info Sharing

- **Compliance Teams:** Prioritise the generation of high-quality SARs/STRs to provide actionable intelligence for authorities, reducing the burden of low-value reporting.
- **Regulatory Authorities and FIs**: Foster public-private collaboration to streamline information-sharing processes and improve end-to-end risk detection capabilities.

6 Conclusion

The 2024 edition of Plenitude's RegIntel report underscores the dynamic and increasingly complex nature of financial crime regulation across major global financial jurisdictions. This year's developments have emphasised the importance of harmonising international standards while responding to emerging threats, from digital asset vulnerabilities to cyber fraud and the transformative potential of AI technologies.

In the United Kingdom, the regulatory landscape underwent a notable shift following the Labour Party's election in July. While the Second Economic Crime Plan 2023–2026, introduced by the previous Conservative government, laid the groundwork for addressing payment fraud and corporate liability, Labour's renewed emphasis on tackling money laundering and corruption has reinforced the country's dedication to robust anti-financial crime measures. Central to this effort in 2025 will be the implementation of the Failure to Prevent Fraud offence, compelling businesses to adopt stricter internal controls to mitigate fraud at its root.

Across the European Union, the establishment of the AMLA marks a transformative step in the fight against financial crime, not only within the EU but on a global scale. As financial crime becomes more complex, AMLA is designed to strengthen the EU's regulatory framework by serving as a centralised, independent body. Its mission is to ensure consistent and effective AML/CFT measures across Member States. This significant development aligns with broader international progress, including the UK's focus on fraud prevention under its new government and Asia's adoption of innovative RegTech solutions in Hong Kong and Singapore. Together, these initiatives underscore a shared global commitment to transparency and integrity in financial systems.

Within the EU, AMLA plays a central role in a comprehensive regulatory overhaul, which includes the 6AMLD and the Single Rulebook. These initiatives aim to unify and enhance compliance standards across the Union. AMLA will collaborate with national regulators, intervene where national authorities fail, and take direct responsibility for supervising high-risk financial entities from 2028. Its establishment is backed by Regulation (EU) 2024/1620, adopted in May 2024, with operations set to begin in July 2025. Frankfurt, selected as AMLA's headquarters following a competitive bidding process, highlights the EU's strategic decision to situate the Authority within a financial ecosystem that already hosts the European Central Bank.

In Asia, financial hubs such as Hong Kong and Singapore have also advanced their regulatory agendas. Hong Kong's public consultation on information sharing and the AMLS project exemplify a forward-thinking approach to harnessing RegTech, while Singapore's AML and Other Matters Bill and Corporate Service Providers Bill further solidify its position as a global leader in compliance. Both jurisdictions have prioritised cross-sector collaboration and the integration of advanced technologies, recognising the critical importance of these strategies in addressing dynamic and evolving financial threats.

Looking ahead to 2025, the global focus on aligning cutting-edge technologies with comprehensive regulatory frameworks will take centre stage. The European AI Act, now in force, offers a blueprint for striking a balance between fostering innovation and implementing safeguards against misuse—principles that are expected to influence regulatory strategies worldwide. However, at the heart of these advancements within the European Union lies the pivotal role of the AMLA.

As AMLA begins operations in July 2025, it will bring transformative change to the EU's approach to combating financial crime. By directly supervising high-risk financial entities, AMLA will address gaps in national oversight, ensuring that financial crime is met with robust and effective countermeasures. For financial institutions operating within the EU, AMLA's establishment represents both an opportunity and a challenge. The Authority's mandate to enforce stricter compliance measures will require institutions to adopt more sophisticated frameworks that leverage technologies such as RegTech and AI to meet the enhanced regulatory demands. Institutions will need to remain agile, not only to comply with AMLA's oversight but also to anticipate and address the broader regulatory expectations set by evolving frameworks like the 6AMLD and the Single Rulebook.

Globally, AMLA's role in 2025 will resonate beyond Europe, influencing international standards and inspiring similar initiatives in other jurisdictions. Its operational debut signals a heightened commitment to transparency, accountability, and collaboration in addressing the interconnected nature of financial crime. By fostering cross-border cooperation and setting a new benchmark for regulatory excellence, AMLA aims to restore and enhance confidence in the integrity of financial systems worldwide.

In conclusion, as financial crime grows more sophisticated and interconnected, so too must the measures to combat it. This RegIntel report provides the critical insights necessary for financial institutions to navigate this evolving landscape, equipping them to meet the demands of 2025 and beyond. Through vigilance, collaboration, and innovation, the financial sector can uphold the principles of transparency, accountability, and integrity in an increasingly complex global market.

> **"The UK and its allies will continue to work together to crack down on illicit finance and the criminality it enables."**
>
> Dan Jarvis,
> Minister of State for Security of the United Kingdom

Overall Key Takeaways

2024 Key Themes

- **Regulatory Evolution**: Significant updates across AML/CTF/CPF, sanctions, and digital asset frameworks globally, emphasising compliance and risk management.
- **Digital Asset Oversight:** Introduction of structured frameworks, including MiCA and stablecoin-specific regulations, highlighting the need for enhanced governance and transparency.
- **Technological Integration:** Adoption of AI and RegTech tools for fraud detection and compliance, with increased scrutiny on AI-related risks.
- **Collaboration:** Strengthened public-private partnerships to tackle financial crime, improve transparency, and drive innovation in compliance practices.
- **Beneficial Ownership and Transparency**: Renewed focus on corporate accountability and enhanced disclosure requirements for beneficial ownership.

2025 Focus Areas

- **Regulatory Preparation**: Adapt to phased regulatory implementations, including stricter AML/CTF measures, digital asset compliance frameworks, and fraud prevention mandates.
- **Risk-Based Approaches**: Prioritise proportional risk management strategies, balancing regulatory requirements with operational efficiency and financial inclusion goals.
- **Technology-Driven Compliance**: Expand the use of advanced tools like AI, blockchain, and real-time monitoring to streamline compliance and mitigate emerging threats.
- **Cross-Border Consistency**: Align with global standards such as FATF recommendations and regional frameworks to ensure harmonised compliance across jurisdictions.
- **Future-Proofing Operations:** Monitor ongoing consultations and emerging regulations, ensuring agility and preparedness for evolving compliance landscapes.

> 2024 was the year for planning, 2025 will be the time for implementation and execution

Plenitude RegSight

Plenitude RegSight and its subscription newsletter keep you informed of the evolving regulatory landscape in the UK, France, and Hong Kong. We conduct weekly horizon scanning to identify new and amended laws, regulations or guidance impacting your organisation's financial crime compliance obligations. As always, we are happy to engage and discuss these developments with you further.

Plenitude has supported several firms, big and small, in implementing financial crime transformation programmes, including robust enhancements of financial crime risk assessment methodologies and risk appetite statements, implementation of financial crime management information and detailed assessments of transaction monitoring capabilities. If you would like to have a chat on what steps might be most appropriate for your firm, drop us an email at enquiries@plenitudeconsulting.com

About this paper:

Authors: Giles Christou, Eleanor Hancock, Leeroy Masamba
Contributors: Tom Hudson, Mohammed Hussain, and Ciarán McMullan
Editors: Imogen Cronin, Orel Garcia

Due to length constraints, we have intentionally excluded some events from this paper. However, we have made every effort to include the key developments that have shaped the industry.
This paper serves as a guiding framework and should not be considered legal advice.

7 Appendix: Key Dates

United Kingdom					
Document	**Source**	**Risk Type**	**Sector**	**Date in Force**	**Page #**
The Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017	UK Government	AML/ CTF/ CPF	All firms regulated under the MLRs	10/01/24 23/01/24	8
The Economic Crime and Corporate Transparency Act 2024	UK Government	AML/ CTF/ CPF & Fraud	Companies; CASPs	21/03/24 26/04/24 01/09/25	9
Financial Services and Markets Act 2023	UK Government	Fraud	PSPs, EMIs, Banks, Building Societies	07/10/24	13
Financial Crime Guide	FCA	AML/ CTF/ CPF	All firms regulated under the MLRs	29/11/24	8
The Sanctions (EU Exit) (Miscellaneous Amendments) (No.2) Regulations 2024	UK Government	Sanctions	UK nationals and legal entities	05/12/24 14/05/25	17
Guidance on the Treatment of PEP's	FCA	AML/ CTF/ CPF	All firms regulated under the MLRs	2025	10

European Union					
Document	**Source**	**Risk Type**	**Sector**	**Date in Force**	**Page #**
ML/TF Guidelines extended to CASPs	EU – European Banking Authority	AML/ CTF/ CPF	CASPs	16/01/24	31
Council Directive (EU) 2020/284	EU – European Parliament	Fraud	PSPs	09/03/24	27
The Instant Payments Regulation (EU) 2024/886	EU – European Parliament	AML/ CTF	PSPs	02/04/24	24
Monetary and Financial Code (Code Monetaire et Financier)	French Parliament	AML/ CTF/ CPF	All firms regulated under the CMF	22/04/24	22
Directive EU 2024/1226	EU – European Parliament	Sanctio ns	Financial Institutions and DNFBPs	19/05/24	29
Sectoral Risk Analysis: AML/CTF	France - Autorité des Marchés Financiers	AML/ CTF/ CPF	CASPs/DASPs, Asset Management, Financial Investment Advisors and other AMF regulated firms	10/06/24	22

European Union					
Document	**Source**	**Risk Type**	**Sector**	**Date in Force**	**Page #**
Ordinance No. 2024-936	France – French Parliament	AML/ CTF/ CPF	CASPs	15/10/24	31
Markets in Crypto Assets Regulation (MiCA)	EU – European Securities and Markets Authority	AML/ CTF/ CPF	CASPs	30/12/24 **01/07/26**	31
The Sixth Anti-Money Laundering Directive (6MLD)	EU – European Parliament	AML/ CTF/ CPF	Financial Institutions and DNFBPs	10/07/25	23
The Anti-Money Laundering Regulation (AMLR)	EU – European Parliament	AML/ CTF/ CPF	Financial Institutions and DNFBPs including Credit Institutions; CASPs; High-Value Goods Dealers; Professional Football Clubs and Agents	10/07/27	23

Hong Kong & Singapore					
Document	**Source**	**Risk Type**	**Sector**	**Date in Force**	**Page #**
Effective Execution of Risk-based Approach for Customer Due Diligence	HKMA	AML/ CTF/ CPF	Authorised Institutions	08/02/24	34
Payment Services Act 2019	Singapore Parliament	AML/ CTF/ CPF	Financial Institutions and DPT Providers	04/04/24	42
Anti-Scam Consumer Protection Charter 2.0.	HKMA	Fraud	Financial Institutions	10/04/24	39
Prevention of Proliferation Financing and Other Matters Act	Singapore Parliament	AML/ CTF/ CPF	Financial Institutions and DNFBPs	01/05/24	36
Terrorist Financing National Risk Assessment	MAS	CTF	Financial Institutions and Firms including Money Remittance Services, DPT Providers, NPOs, High Value Goods Dealers	01/07/24	37
Corporate Service Providers Act 2024 and Companies and Limited Liability Partnerships (Miscellaneous Amendments) Act 2024	Singapore Parliament	AML/ CTF/ CPF	In scope companies	31/07/24	36

Hong Kong & Singapore					
Document	**Source**	**Risk Type**	**Sector**	**Date in Force**	**Page #**
Anti-Money Laundering and Other Matters Act	Singapore Parliament	AML/ CTF/ CPF	Financial Institutions and Casino Operators	26/08/24	36
Guidance on the use of AI for Monitoring Suspicious Activities	HKMA	AML/ CTF/ CPF	Authorised Institutions	09/09/24	34
Conclusions of HKMA Consultation on Information Sharing among AI's	HKMA	AML/ CTF/ CPF	Authorised Institutions	30/09/24	34
Money Laundering National Risk Assessment	MAS	AML	Financial Institutions and Firms including Payment Institutions, Asset Managers, and Licensed Trust Companies	30/10/24	36

Global					
Document	**Source**	**Risk Type**	**Sector**	**Date in Force**	**Page #**
Guidance on Beneficial Ownership and Transparency of Legal Arrangements	FATF	AML/ CTF/ CPF	Financial Institutions	11/03/24	47
Statement on Countering Terrorist Financing	The Wolfsberg Group	CTF	Financial Institutions	11/03/24	49
Principles for Auditing for Effectiveness	The Wolfsberg Group	AML/ CTF/ CPF	Financial Institutions	26/03/24	49
Effective Monitoring for Suspicious Activity	The Wolfsberg Group	AML/ CTF/ CPF	Financial Institutions	01/06/24	49
Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs	FATF	AML/ CTF/ CPF	VASPs	09/07/24	47
Money Laundering National Risk Assessment Guidance	FATF	AML	Financial Institutions	11/07/24	48