

# RegIntel

## 2023 Recap and 2024 Outlook Report

## EXECUTIVE SUMMARY

In this end-of-year review, Plenitude's Regulatory Intelligence (RegIntel) team provides a comprehensive overview of the regulatory developments in 2023 and anticipates potential changes on the horizon for 2024. This paper explores the key amendments and implementations across four global financial hubs: the United Kingdom, European Union, Hong Kong and Singapore. These jurisdictions have been at the forefront of regulatory innovation, and will continue to lead development during 2024.

In this report, the team highlights legislative, regulatory, and industry developments occurring across the realms of anti-money laundering (AML), counter-terrorist financing (CTF), counter-proliferation financing (CPF), fraud, and sanctions, as well as notable enforcement and disciplinary actions from regulators. With the number, complexity, and speed of regulatory changes increasing from year to year, remaining up-to-date with new regulatory obligations is a necessity for Financial Crime Compliance teams.

Several external factors shaped the regulatory developments in 2023. The team highlights how global geopolitical changes have shaped governments' sanction and CTF/CPF regimes, the on-going push to regulate virtual assets, and how money laundering scandals have gained notoriety in Singapore and Hong Kong, resulting in renewed efforts to strengthen AML controls.

In the UK, firms should prepare for continuing regulatory developments across the realms of fraud, virtual assets, and sanctions. Several developments approved in 2023 are scheduled for implementation in 2024, including the full roll-out of the Consumer Duty in July and the mandatory reimbursement on APP fraud in October. In the coming year, firms should also expect greater clarity on the implementation timeline for the long-awaited Companies House reform and HMT cryptoasset regulatory regime, and should await the scheduled review of Senior Managers and Certification Regime between April and June.

Throughout 2023, the EU positioned itself at the forefront of global initiatives to regulate new technologies and cryptoassets. In 2024, firms can expect to see the implementation of the Markets in Crypto-Assets Regulation (MiCA), including MiCA's new regime on E-Money Tokens and Asset-Referenced Tokens in June, MiCA's new CASPs requirements in December, and the implementation of the Transfer of Funds Regulation (TFR) in December. In parallel, the EU demonstrated a commitment to strengthening its existing AML/CTF/CPF regime and maintained its central role in facilitating international collaboration to foster the successful implementation and enforcement of economic sanctions. Much like in the UK, firms should expect to see new sanctions packages and more stringent anti-circumvention regimes in the coming year. Firms can also await further information on the planned establishment of a new EU Anti-Money Laundering Authority (AMLA), which is expected to push the EU towards greater cross-country coordination in AML compliance.

High-profile money laundering and fraud scandals in Hong Kong and Singapore directed regulators' focus to emphasizing strengthened AML policies, promoting technology and information sharing in fraud prevention, and accelerating discussions on the future of virtual assets regulation. Following the implementation of Hong Kong's VASPs licensing requirements, 'Travel Rule', and AML requirement for VASPs in 2023, firms can anticipate continued discussion and additional details concerning the implementation of Singapore's Stablecoins regulation in the upcoming year. In the midst of Singapore's \$2.8 billion money laundering scandal, authorities have issued new AML guidelines for the wealth management sector, on the use of complex structures, and for AML controls concerning virtual assets. Firms should stay attuned to the further strengthening of AML requirements, as well as a renewed emphasis on combating fraud from regulators.

# Overview of changes to AML/CTF regimes across jurisdictions



## United Kingdom

### Implemented

- Economic Crime Plan 2023-2026
- Consumer Duty for new and existing products or services that are open to sale or renewal
- DAML, SAR process improvement, threshold increased from £250 to £1000 (POCA update)
- Obligation to report discrepancies in beneficial ownership to Companies House during the business relationship (MLRs update)
- Crypto transfer regime 'Travel Rule' (MLRs update)
- General (part I) and sector specific (part II) revisions made (JMLSG update)
- MLR amendment lowering risk of domestic PEPs (10 Jan 2024)

### Soon-to-be implemented

- FCA's review of PEP treatment (Jun 2024)
- Consumer Duty for closed products (31 Jul 2024)
- PSR mandatory reimbursement (FSMA, Oct 2024)
- Failure to prevent fraud offence (ECCTA, TBC)
- Companies House Reforms (ECCTA, TBC)
- Anti-Slapp protection (ECCTA, TBC)
- SAR process streamlining (ECCTA, TBC)
- New confiscation power for assets related to financial crime (POCA update, TBC)

### Awaiting confirmation

- New eld&V standard and discrepancy reporting (JMLSG update, TBC)
- HMT cryptoasset regulatory regime (TBC)
- Review of Senior Managers and Certification Regime (Apr-Jun 2024)
- AML/CTF supervisory regime reform (TBC)



## European Union

### Implemented

- Pilot Regime for the use of Distributed Ledger Technologies (DLT)
- MONEYVAL's strategy on AML, CTF and CPF for 2023-2027, and Typology report on ML/TF risks
- EBA's report on ML/TF risk in EU Financial sector

### Soon-to-be implemented

- MiCA's new regime on E-Money Tokens and Asset-Referenced Tokens (Jun 2024)
- MiCA's new CASPs requirements (Dec 2024)
- Transfer of Funds regulation (Dec 2024)

### Awaiting confirmation

- ESMA technical standard for MiCA (Jun 24)
- Draft AML legislations on establishment of AMLA and 'single rulebook' (TBC)
- Proposed new directive on asset recovery and confiscation (TBC)



## Hong Kong + Singapore

### Implemented

- HK: AMLO amendments for FIs and DNFBPs on due diligence procedures for virtual assets and PEPs
- HK: Introduction of Travel Rule under AMLO
- HK: VASPs subject to all AML requirements under AMLO
- HK: HKMA and SFC's AML guidelines for licensed VASPs, including incorporation of Travel Rule, and revisions to definition of PEPs
- HK: VASPs licensing requirements from SFC
- HK: SFC's Disciplinary Fining Guidance published
- HK: HKMA's Enhanced approach to combat digital fraud, including FINEST launched
- SG: New guidelines on AML for wealth management
- SG: New guidelines on AML controls on complex structures
- SG: ACIP's best practice on AML controls on virtual assets for FIs, DPTSPs, NBFIs

### Soon-to-be implemented

- SG: MAS & IMDA guidelines on Shared Responsibility Framework (SRF) (expected 2024)

### Awaiting confirmation

- SG: Regulation of Stablecoins

# Overview of specific sectors affected by AML/CTF changes\*



## United Kingdom

### JMLSG AML/CTF updated guidance

- Motor Finance
- Wealth Management
- Private Equity
- Non-life Providers of Investment Fund Products
- Financial Advisers
- Discretionary and Advisor Investment Management Operators
- Consumer Credit Providers
- Cryptoasset providers and custodian wallet providers

### Dear CEO Letters

- Wealth Management + Stockbroking Firms
- Corporate Finance Firms

### FSMA

- Cryptoasset providers

### MLRs updates

- VASPs + other FI's transferring cryptoassets

### ECCTA

- Real Estate
- Corporate Service Providers



## European Union

### Transfer of Funds Regulation (TFR)

- CASPs + other FI's transferring cryptoassets

### MiCA

- CASPs

### EBA Opinion on ML/TF risk

- Credit Institutions
- Payment Institutions
- E-Money Institutions
- Bureaux de Change
- Investment Firms
- Collective Investment Undertakings
- Fund Managers
- Credit Providers
- Life Insurance Undertakings & Intermediaries
- CASPs

### MONEYVAL Typology Report

- CASPs + other FI's exposed to crypto FC risks



## Hong Kong + Singapore

### AMLO updated guidance (HK)

- VASPs
- FIs
- DNFBPs

### Guidelines on AML/CTF (HKMA/SFC)

- VASPs

### Enhanced Approaches to Combat Digital Fraud

- Retail Banks

### AML/CTF Ordinance (Cap. 615) (HK)

- FIs
- DNFBPs

### Circular on ML/TF risk (SG)

- Wealth Management

### Consultation on SFR (SG)

- Telecom
- FIs

### Strengthening AML/CTF controls on misuse of legal person/arrangements (SG)

- FIs
- Lawyers
- Trust Companies
- Corporate Service Providers

\*While some regulation/guidelines are sector specific, all financial service firms should consider the expectations set out when building an effective and well rounded Financial Crime Compliance framework.



# CONTENTS

<b>Executive Summary</b> .....	<b>2</b>
• APPENDIX A: Overview of changes to AML/CTF regimes across jurisdictions .....	3
• APPENDIX B: Overview of specific sectors affected by AML/CTF changes .....	4
<b>Introduction</b> .....	<b>7</b>
<b>Section 1: United Kingdom</b> .....	<b>8</b>
• AML/CTF/CPF .....	10
◦ UPDATED: The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations [Apr to Dec 2023] .....	10
◦ UPDATED: Proceeds of Crime Act [5 Jan 2023 and forthcoming] .....	10
◦ NEW: Economic Crime and Corporate Transparency Act [26 Oct 2023] .....	11
◦ UPDATED: Joint Money Laundering Steering Group (JMLSG) Guidance [Sept-Oct 2023] .....	12
• Fraud .....	13
◦ NEW: Financial Services and Markets Act [29 Jun 2023] .....	13
◦ NEW: Economic Crime and Corporate Transparency Act [Forthcoming] .....	13
• Sanctions .....	14
• Enforcement and Disciplinary Actions .....	15
<b>Section 2: European Union</b> .....	<b>16</b>
• AML/CTF/CPF .....	17
◦ UPDATED: High-risk Third Countries (Commission Delegated Regulation (EU) 2016/1675) [Jun to Oct 2023] .....	17
◦ NEW: The Transfer of Funds Regulation [29 Jun 2023] .....	17
◦ NEW: The Markets in cryptoassets Regulation [29 Jun 2023] .....	17
• On the Horizon for the EU .....	18
◦ NEW REPORTS: MONEYVAL [Apr to Jul 2023] .....	18
◦ NEW REPORTS: European Banking Authority [Jul 2023] .....	18
• Sanctions .....	19

# CONTENTS

<b>Section 3: Hong Kong and Singapore</b> .....	<b>21</b>
• AML/CTF/CPF .....	22
◦ SG NEW: Circular on Money Laundering and Terrorism Financing Risks in the Wealth Management Sector [03 Mar 2023] .....	22
◦ HK UPDATED: Cap. 615 Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) [Apr and Jun 2023] .....	22
◦ HK UPDATED: Guideline on Anti-Money Laundering and Counter Financing of Terrorism (For Stored Value Facility Licensees) [01 Jun 2023] .....	23
◦ HK UPDATED: Guideline on Anti-Money Laundering and Counter Financing of Terrorism (For Licensed Corporations and SFC-licensed Virtual Asset Service Providers) [01 Jun 2023] .....	23
◦ HK NEW: Securities and Futures Commission (SFC) Disciplinary Fining Guidelines [01 Jun 2023] .....	23
◦ SG NEW: Management of money laundering, terrorism financing, and sanctions risks from customer relationships with a nexus to digital assets [11 Jul 2023] .....	24
◦ SG NEW: MAS Finalises Stablecoin Regulatory Framework [15 Aug 2023] .....	24
◦ SG NEW: Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures [30 Aug 2023] .....	24
◦ HK NEW: RegTech case studies, tools, and platforms [Throughout 2023] .....	24
• Fraud .....	24
◦ HK NEW: Enhanced approaches to combat digital fraud [12 Oct 2023] .....	24
◦ SG NEW: Consultation on Proposed Shared Responsibility Framework [25 Oct 2023] .....	26
• Enforcement and Disciplinary Actions .....	26
<b>Section 4: Global Outlook</b> .....	<b>29</b>
• The Wolfsberg Group .....	30
◦ UPDATED: Correspondent Banking Due Diligence Questionnaire and Financial Crime Compliance Questionnaire [10 Feb 2023] .....	30
◦ UPDATED: ABC Compliance Programme Guidance [17 Apr 2023] .....	30
◦ UPDATED: Payment Transparency Standards [17 Oct 2023] .....	30
<b>Conclusion</b> .....	<b>31</b>
<b>APPENDIX</b>	
• APPENDIX A: Summary Table of changes .....	32

## INTRODUCTION

As efforts to combat financial crime continued across the United Kingdom, European Union, and Asia, numerous notable developments occurred throughout 2023. In our review of the year's events, we highlight legislative, regulatory, and industry developments occurring across the realms of anti-money laundering (AML), counter-terrorist financing (CTF), counter-proliferation financing (CPF), fraud, and sanctions. Additionally, the paper identifies key areas of focus for 2024.

Several noteworthy common themes emerged throughout the year, from sustained international collaboration on financial sanctions and embargo enforcement, to global discussions on how a tailored approach to the regulation of digital assets would look. Envisioning the anti-financial crime agenda for 2024 and the key areas of pertinence for financial services firms begins with a holistic review of the events of 2023. This paper looks at regulatory changes across four jurisdictions: the UK, EU, Hong Kong, and Singapore, with a focus on the five risk areas alongside enforcement.

Government and regulators' focus on these themes has in part been influenced by continuing geopolitical trends and notable financial crime investigations. The issuing of new sanctions packages alongside renewed attention on tackling sanctions circumvention across the EU and the UK was underscored by the continuation of Russia's invasion of Ukraine, now approaching its second anniversary in 2024. The EU and the UK government have remained committed to their implementation of financial sanctions and restrictive measures on Russia.

Firms should expect a continuation, if not a reinforcement, of current restrictive measures in the coming year. The publication of reports, guidance, and alerts to firms throughout 2024 highlighted the importance of tightening anti-evasion and circumvention controls across the financial system.

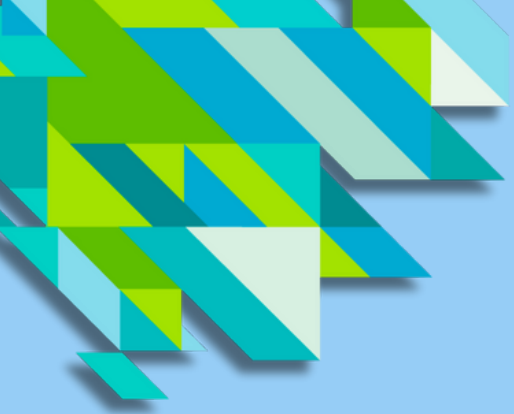
In the second half of 2023, ongoing instability in the Middle East heightened international focus on ensuring the effective implementation of rigorous CTF measures. New publications from the Financial Action Task Force (FATF) on '[Best Practices on Combating the Abuse of Non-Profit Organisations](#)' and '[Crowdfunding for Terrorism Financing](#)' highlighted concerns with inadequate control measures for evolving terrorist financing (TF) threats. Increased focus on modes of financing terrorism including cash smuggling and cryptocurrencies has reinforced the importance of implementing a regulatory framework dedicated to the emerging virtual currency landscape. Firms should expect new and improved CTF controls across several jurisdictions as a result of FATF reviews and ongoing geopolitical developments.

In 2024, the potential of new technologies to improve the traceability of transactions will continue to influence the application of anti-financial crime controls and the development of digital asset regulation. Several of the jurisdictions covered in this paper have made significant advances in mandating licensing for cryptoasset providers and approving new regimes for the issuance of cryptoassets and stablecoins.

The journey to regulating digital assets has only just begun, and firms should expect more consultations and new regimes covering areas such as Decentralised Finance (DeFi) in the coming years.

The push to regulate cryptocurrency across major financial hubs has been impacted by notable investigations into its abuse by fraudsters, money launderers, and sanctioned parties. In the US, cases included the [trial and conviction of the founder of FTX](#) on fraud charges and a record [USD 3.4bn settlement between Binance and the US Treasury](#), over unregistered activities and deficiencies in AML and Sanctions programs, while in Hong Kong a notable case was the arrest and investigation of several people surrounding [allegations of fraud involving crypto exchange platform JPEX](#). Likewise, the focus on developing stablecoin regulatory regimes in the EU, Hong Kong and Singapore is set to continue in the year ahead.

Finally, developments across the Asian financial community have accompanied news coverage of a [USD 2.8 billion money laundering scandal](#) spanning a global network of assets and criminal activities. The wealth management, accounting, and family office sectors have been under heightened scrutiny as one of the most common entry points for illicit funds to Asian financial hubs. Firms should expect continued restructuring and tightening of Singapore and Hong Kong AML practices and should take notice of the key role that monitoring and reporting played in bringing the network's activities to the attention of the authorities.



# SECTION ONE:

## United Kingdom



Plenitude Insights



# United Kingdom

The prevention and mitigation of financial crime remained a key Government focus during 2023. The year saw various areas of legislative, regulatory, and industry focus in the UK, as witnessed through the passing of landmark legislation strengthening corporate transparency, the issuance of Government strategies exploring fraud and economic crime and continued regulatory enforcement for non-compliance.

The Government's publication of its second [Economic Crime Plan](#) in March set forth its cross-cutting strategy for tackling economic crime between 2023 and 2026, with points of focus including sanctions evasion, anti-fraud, and cryptoassets. The plan laid the groundwork for further legislative and regulatory changes, which occurred in the months that followed.

In July, regulated firms were reminded to take a balanced approach to navigating Financial Crime Compliance (FCC) with customer protection, as the [Consumer Duty](#) partially came into effect for new and existing products or services that are open to sale or renewal.<sup>1</sup>

The development of a regulatory regime tailored to the evolving digital asset and virtual currency landscape proved a key theme throughout 2023. Relevant authorities amended existing laws and regulations to incorporate the technologies throughout the year. The [Financial Promotions regime](#) for cryptoassets entered into force in October, and the Financial Conduct Authority (FCA) continued to [provide insights and guidance](#) for cryptoasset firms across areas including good and poor quality registration applications.

Throughout 2023, the FCA maintained an active role in overseeing and guiding FIs. Examples of this included:

- In November, the FCA issued a [‘Dear CEO’](#) letter to wealth management and stockbroking firms, providing a comprehensive assessment of key sector harms and updated supervisory priorities. These priorities emphasised the continued importance of implementing rigorous controls to combat financial crime in the sector, whilst ensuring alignment with compliance requirements under the Consumer Duty.
- In April, the FCA issued a [warning](#) to banks to remain vigilant in the battle against money laundering through the Post Office.
- In August, the FCA launched a [review](#) into the treatment of politically exposed persons (PEPs), an area of heightened public interest throughout the year. A final report covering areas including proportionate risk assessments and decisions on account access and closure is expected by the end of June 2024, with the FCA having already published its [initial findings](#) on account access and closure presenting important insights and learnings for firms in September.<sup>2</sup>
- Near the year's close, the Government passed [amendments](#) to the Money Laundering Regulations that, now enacted on 10th January 2024, will clarify the requirement for banks and regulated firms to treat domestic PEPs as inherently lower risk than non-domestic PEPs. The legislative and regulatory landscape surrounding firms' treatment of PEPs will likely be subject to further discussion and reform in 2024.

In November, the FCA published its [planned regulatory initiatives](#) for next two years. The Consumer Duty is scheduled to come into effect for closed products on 31 July 2024. Additionally, a review of the Senior Managers and Certification Regime (SM&CR) is anticipated between April and June 2024. Continuing its development of a regulatory framework tailored to cryptoassets, the FCA will build on consultations held in 2023, with secondary legislation expected from HMT in 2024. A Government [review and call for evidence](#) on how the Payment Services Regulations should evolve ran from January to April, and efforts to prevent APP scams will remain a focus of the Payment Systems Regulator (PSR) throughout 2024, during which firms can take an active role.

<sup>1</sup> For further details on the Consumer Duty, see our paper which outlines key insights: [It's Your Duty to be \(Consumer\) Dutiful](#)

<sup>2</sup> For further information on the FCA's initial findings on bank account access and closures, read our article: [Account Access and Closure: What the FCA's Initial Findings Mean for Firms](#)

In the coming year, the regulatory landscape for anti-financial crime, consumer protection, and licencing is poised for further significant development. In [February](#), HMT published its consultation on the future regime for cryptoasset regulation, with its response to the consultation published in [October](#). Stakeholder feedback received during the consultation included proposals on the treatment of Non-Fungible Tokens (NFT) alongside the treatment of overseas firms and the geographical scope of future regulation. Separately, the FCA, PRA and Bank of England have collaborated on explorations into the case for a UK [central bank digital currency](#) (CBDC), or 'digital pound', and have also published papers that outline the approach to regulating the issuance of stablecoins. Concurrently, HM Treasury is in the process of reviewing feedback received during its [consultation](#) on reforming the AML/CTF supervisory regime in the UK, with four new supervision models proposed.

## AML/CTF/CPF

**UPDATED: [The Money Laundering, Terrorist Financing and Transfer of Funds \(Information on the Payer\) Regulations \[Apr to Dec 2023\]](#)**

Amendments to the Money Laundering Regulations (MLRs) in 2023 spanned areas including increased corporate transparency and coverage of cryptoasset transfers.

Changes to Regulation 30A under [The Money Laundering and Terrorist Financing \(Amendment\) \(No. 2\) Regulations 2022](#) entered into force in April. Firms are now required to report discrepancies in beneficial ownership to Companies House, both prior to establishing a business relationship (an existing requirement), as well as throughout the relationship (a new requirement).

A significant regulatory change surrounded the MLR's coverage of cryptoasset transfers. On 1st September 2023 [Part 7A](#), covering new Regulations 64A-64H on the 'travel rule' entered into force. The UK's implementation of the travel rule followed a [call to action](#) by the Financial Action Task Force (FATF) for member jurisdictions to enhance the transparency of the cryptoassets transfer process and reduce the potential for criminal misuse. The application of the 'travel rule' for cryptoassets transfers introduced the requirement for transfers to be accompanied by specific personal identifiable information on the originator and the beneficiary. Other key topics covered by the inserted Regulations include transfers involving unhosted wallets (64G), and the provision of information to law enforcement (64H).

The list of high-risk third countries under Schedule 3ZA was revised to align with changes made by the FATF to its 'grey list' of countries with strategic AML/CTF deficiencies. Cambodia, Morocco, Albania, the Cayman Islands, Jordan, and Panama were removed from the list in [June](#), while Bulgaria, Cameroon, Croatia, Nigeria, South Africa, and Vietnam were added in [December](#). The list is

reviewed throughout the year following FATF Plenaries, and firms should expect it to be under further review in 2024.

**UPDATED: [Proceeds of Crime Act \[5 Jan 2023 and forthcoming\]](#)**

New amendments made to The Proceeds of Crime Act (POCA) in 2023 have empowered authorities to identify and confiscate assets involved in financial crime.

One key change concerns the disclosure and information sharing requirements for FIs. The threshold amount specified under [Section 339A\(2\)](#) of POCA was significantly increased from £250 to £1,000 when enacted in January. This change increased the threshold at which firms are required to seek consent before processing such transactions from the National Crime Agency (NCA) through the submission of Defence Against Money Laundering (DAML) requests. Through further bureaucratic streamlining, revisions sought to lessen the regulatory burden on firms to submit, and law enforcement to process, DAML requests, in turn addressing the rise in ineffective Suspicious Activity Reports (SARs) and DAML requests received by the NCA. This is expected to enable the UKFIU to focus its resources on disclosures offering the likeliest opportunities for asset seizure.

Further amendments to POCA made by the Economic Crime and Corporate Transparency Act on 26th October have been published but are yet to enter into force.

Revisions include the addition of exemptions for mixed-property transactions and enhanced powers for law enforcement. Once in force, revisions made to the confiscation and civil recovery powers will provision further powers to law enforcement agencies in combatting the criminal use of cryptoassets. With the further implementation and impact of the ECCT to be seen in 2024, the date at which amending provisions enter into force will be communicated to RegSight subscribers through bi-monthly newsletters.

### [NEW: Economic Crime and Corporate Transparency Act \[26 Oct 2023\]](#)

The Economic Crime and Corporate Transparency Act (ECCT) was approved following the expedited passage into law of the [Economic Crime \(Transparency and Enforcement\) Act](#) in March 2022. The two pieces of legislation have enhanced law enforcement's powers of confiscation and asset recovery, including in the recovery of cryptoassets. One of the objectives of the ECCT is to tackle the risk of British real estate and corporate structures being exploited for money laundering and fraud. While regulatory innovation in the fraud sector will be addressed in the section below, this section looks at the ECCT's changes to four key areas of AML compliance: introducing reforms to Company House, enhancing corporate criminal liability, mitigating the protective effects of Strategic Lawsuits Against Public Participation (SLAPPs) on corruption, and innovating private-public AML information sharing.

The Act introduced long-anticipated reforms to Companies House to prevent the creation and the closure of fraudulent companies, as well as measures to curb the criminal misuse of limited partnerships. Newly-introduced [measures](#) include enhanced identity verification requirements for registered company directors and those with significant control, the provision of greater investigation and enforcement powers to Companies House, and facilitated information sharing. Through the ECCT, the Government has also [revised](#) rules on corporate criminal liability for economic crimes, allowing corporations to be held directly accountable.

Amendments to SLAPPs involving economic crimes has additionally been introduced through the ECCT and include increased protection for defendants through a new early dismissal mechanism and a cost-protection process. With at least 70% of SLAPPs referenced in an [April 2022 report](#) found to be connected to economic crime and corruption, the ECCT's addressing of the issue reiterates the requirement for professionals to be aware of their legal and client obligations.

Finally, businesses will be able to better share information related to the detection of economic crime with the authorities, thanks to bureaucratic streamlining of the SARs process. The Act waives the civil liability on breaches of confidentiality for information provided with the intention of combatting economic crime. This change empowers the UK Financial Intelligence Unit (UKFIU) to acquire information from firms regarding ML/TF without the

need for a pre-existing SAR.

The ECCT further broadens the categories of cases in which firms can deal with consumer property without first being required to submit a Defence Against Money Laundering (DAML) SAR. This revision is designed to reduce the onus on businesses to report suspicious activity, and conversely will direct private sector and law enforcement resources onto high-value activity.

The impact of the ECCT will continue to be seen in 2024, with the UK Government expected to release additional guidance in 2024, addressing effective implementation of the Act for firms.

### [UPDATED: Joint Money Laundering Steering Group \(JMLSG\) Guidance \[Sept-Oct 2023\]](#)

The JMLSG Guidance has undergone significant revisions this year to align with legislative and regulatory changes, providing enhanced best practice guidance for FIs in executing general AML/CTF/CPF requirements as well as issuing new and revised sector-specific standards.

[Revisions approved in 2023:](#) (next page)

## PART I

- EDD on High-Risk Third Countries (Paragraph 5.5.1, Annex 5-IV): Additional guidance on EDD and enhanced ongoing monitoring for high-risk third countries, applicable to new or existing business relationships in high-risk third countries or where any party to a transaction is established in a high-risk third country. Annex 5-IV, providing a list of EDD risk factor guidelines, was also revised and enhanced.
- Trusts (Paragraph 5.3.129A, 5.3.258-5.3.282): Prior to establishing a business relationship with a relevant trust, firms are required to obtain proof of registration with the Trust Registration Service (TRS) or an excerpt of the register of the trust from the agent or trustee. The revised Guidance reflects the expanded requirement for firms to report discrepancies during a business relationship with a trust.
- Proliferation Financing (Chapters 4 and 7 of Part I): In 2022, new amendments to the MLRs introduced the requirement for firms to conduct a PF risk assessment and implement PF policies, controls, and procedures.<sup>3</sup>

## PART II

- Sectoral Revisions: Revised sectoral guidance was updated for firms across several industries.
  - For motor finance firms, a new Annex on AML-CTF industry standards was added in Sector 11.
  - Additional guidance on ML risks, customer due diligence, and transaction monitoring for wealth management firms in Sector 5.
  - Additional guidance on customer due diligence alongside identification and verification, for financial advisers in Sector 6.
  - Additional guidance on taking a risk-based approach, customer due diligence, and correspondent securities relationships for non-life providers of investment fund products in Sector 8.
  - Additional guidance on taking a risk-based approach and customer information for discretionary and advisor investment management operators in Sector 9.

- Additional guidance on product risk for consumer credit providers in Sector 11A.
- Various wording revisions to guidance for private equity firms in Sector 13.
- Cryptoassets (Sector 22, Part II): New guidance was issued for cryptoasset providers and custodian wallet providers to accompany the new requirements for cryptoasset businesses introduced as amendments to the MLRs through Regulations 64A-64H.

### Changes expected for 2024:

- Identification and Verification (Part I, [Paragraph 5.3.89](#)): If approved, the guidance advises that firms manage the risk of impersonation fraud through directly linking the customer to their claimed identity by adopting processes including biometric and electronic verification.
- Discrepancy Reporting (Part I, [Paragraphs 5.3.129A-C](#)): Further guidance for firms on reporting material discrepancies in beneficial ownership information to Companies House or HMRC surrounding customers which are trusts. Additional guidance on the excerpts from the Trust Registration Service (TRS) and the Register of Overseas Entities (ROE) that firms should use, and the exemptions to registration which firms can determine through a risk-based approach are included in the revisions.

## Key takeaways: AML/CTF

- 1 Expanded requirement for firms to report beneficial ownership discrepancies to Companies House before establishing a business relationship and periodically thereafter under Regulation 30A of the MLRs
- 2 Continued importance of aligning country risk rating and enhanced due diligence processes to revisions made to the list of high-risk countries under Schedule 3ZA of the MLRs
- 3 Introduction of 'travel rule' requirements for transfers of cryptoassets under Regulations 64A-64H of the MLRs
- 4 Financial institutions should remain up to date on forthcoming revisions to Part I of the JMLSG Guidance and be ready to implement any appropriate actions in their identification and verification, and discrepancy reporting processes

<sup>3</sup> To learn more, take a look at our paper on '[Integrating Proliferation Financing Into Your Risk and Controls Framework](#)'.



## FRAUD

Fraud was the [most common offence in the UK](#), amounting to 41% of all crime committed in the year ending September 2022. Over the past year, the UK Government has intensified its efforts to combat serious fraud, identifying its potential to reduce the public's confidence in the rule of law and threaten the UK's national and economic security. On 3rd May, the UK Government published its [Fraud Strategy](#), setting out a 3-year programme, underpinned by a three-pronged approach to pursuing fraudsters, blocking fraud, and empowering people. By the close of 2025, the Government aims to promote meaningful collaboration across government agencies, regulatory authorities, law enforcement, industry, and the private sector, to produce tangible results in combating fraud. The strategy sets out the Government's ambition to reduce fraud by 10% from 2019 levels, estimated to prevent over 300,000 frauds. Firms in sectors ranging from finance to technology can be sure to see the continued phased implementation of the strategy during 2024.

### NEW: [Financial Services and Markets Act \[29 Jun 2023\]](#)

The Financial Services and Markets Act (FSMA) has ushered in a set of landmark reforms expanding the powers afforded to the UK financial regulators. The Act's key objective is boosting the productivity, growth, and competitiveness of the UK economy by introduced tailored financial services regulations following Brexit.

The Act expanded upon the existing framework introduced by the Financial Services and Markets Act 2000, granting further powers to the FCA Prudential Regulatory Authority (PRA) and the Bank of England (BoE). FSMA further allowed the revocation of retained EU law concerning financial services. It also allows for the scope of existing regulatory frameworks to be extended to cover cryptoassets-related activities.

FSMA introduced significant provisions designed to tackle scams, including authorised push payment (APP) fraud. The PSR is now required to introduce obligations for payment service providers to reimburse fraud victims, where payments resulting from fraud are conducted through the Faster Payments Service (FPS).

At the end of December, the PSR published its final reimbursement [policy statement](#), which confirmed the Regulator's position on areas including the level of excess and the maximum level of reimbursement. Firms can begin to prepare for the implementation of the reimbursement requirement in 2024.

### NEW: [Economic Crime and Corporate Transparency Act \[Forthcoming\]](#)

Besides making significant enhancements to AML compliance, the ECCT notably introduced a new ['Failure to Prevent Fraud'](#) offence. Although limited to large organisations, the new offence will hold firms accountable for profiting from fraud by their employees and will come into force once the Government issues guidance outlining reasonable fraud prevention procedures for subject firms to take. Under the offence, firms will be liable in cases where internal fraud has been committed and they did not have reasonable policies and procedures in place to prevent it.

The offence is designed to strengthen existing enforcement measures against internal fraud, as there will be no requirement to demonstrate that those holding senior positions within the firm had knowledge of or were involved in the fraud. Once enforced, the offence will apply to large body corporates, defined as firms meeting two out of three of the following criteria: having more than 250 employees, more than £36 million turnover, and/or more than £18 million in total assets. Subsidiaries and partnerships across all industries will also be liable under the ECCT.

As firms await the implementation of the landmark offence, the parliamentary focus on fraud will remain a key policy area throughout 2024.

### Key takeaways: Fraud

- 1 Firms should ensure that their fraud prevention controls meet regulatory expectations
- 2 Firms should begin preparations for the 2024 enforcement of the APP Fraud mandatory reimbursement requirement and the 'failure to prevent fraud' offence

## SANCTIONS

The 2022-23 financial year was hailed as [‘transformative’](#) by the Office of Financial Sanctions Implementation (OFSI) for the use of financial sanctions at national and international levels. Following a year of vast sanctions implementation in 2022, the focus in 2023 has further evolved to combating circumvention and improving overall enforcement. During the 2022-23 financial year, the UK Government, in continued collaboration with global partners, imposed financial sanctions on 35 regimes including Russia and Belarus, designated 3883 entities including Hamas and global human rights abusers, and made 503 licensing decisions. Further efforts to enhance government-industry-regulation engagement and collaboration for effective sanctions implementation were seen with 50 firms and businesses joining the new OFSI Legal Sector Engagement Forum (LSEF).

OFSI remained a key global player in the enforcement of anti-Russian sanctions. At the end of 2022, the [Oil Price Cap](#), a global collaboration to apply a cap to the price of Russian oil was announced with the aim of preventing Russia from benefiting from wartime price increases. The cap entered into force on 5th February, targeting Russian refined oil products. OFSI subsequently issued [guidance](#) alerting firms of their requirements and expected practice in areas including due diligence and licencing applications.

Throughout the year, regular revisions have been made to the [Financial Sanctions General Guidance](#),

as well as to the technical guidance on [enforcement and monetary penalties](#). OFSI has also maintained an active supervisory approach by consistently releasing new sector-specific and thematic guidance.

Publications included instructions on licence applications for the purpose of [travel, ransomware, and public officials and control of private entities](#), as well as guidance for [high-value dealers](#). In November, OFSI, in collaboration with the NCA and other partners, published [Red Alert](#) warning firms of the tactics believed to be employed by sanctioned entities to circumvent restrictions on gold, and providing recommendations on appropriate actions to be taken. In December, a second [Red Alert](#) was published, warning the financial sector of common techniques suspected to be adopted by Russia to evade sanctions on the export of high-risk goods.

Sanctions will continue to prove an important economic tool in the UK’s arsenal in 2024. In December, the new Office of Trade Sanctions Implementation ([OTSI](#)) was announced with the aim of detecting and disciplining companies evading sanctions. Set to launch in 2024, OTSI will aid businesses in complying with their sanction requirements, investigate potential breaches, and have the power to issue civil penalties and refer cases to HMRC for criminal enforcement where required. Firms can therefore expect their compliance with sanctions obligations to remain under the regulatory spotlight moving forward and should continue to review their internal controls and processes to ensure effective compliance.

### Key takeaways: Sanctions

- 1 The Oil Price Cap will continue into 2024, and firms must fulfil their compliance obligations
- 2 OFSI and other law enforcement partners continue to provide warnings and guidance for financial institutions and firms on the importance of remaining vigilant to sanctions circumvention and evasion techniques
- 3 Collaboration across UK agencies and with other jurisdiction unified effective sanctions implementation and enforcement
- 4 Announcement that OTSI is to be created in 2024



## ENFORCEMENT AND DISCIPLINARY ACTIONS

Throughout 2023, the FCA and OFSI remained actively committed to enforcing compliance and exercising their authority to impose disciplinary measures in response to regulatory violations.

Although the total amount of fines imposed has declined significantly since 2022, the FCA issued a total £20,618,700 across four [fines](#) on firms for deficiencies in their anti-financial crime controls, ranging from insufficient customer due diligence (CDD) to inadequate governance. [Guaranty Trust Bank \(UK\)](#) and [Al Rayan Bank PLC](#) were fined in January, with deficiencies found in both firms' AML/CTF control functions, notably concerning CDD and enhanced due diligence (EDD) processes. Staying attuned to regulatory enforcement will remain key, particularly if firms are to assess the applicability of the FCA's findings to their own internal systems and controls.

During the [2022-23 financial year](#), 473 suspected breaches of financial sanctions (excluding oil price cap and counter-terrorism breaches) were recorded by OFSI, an increase from the 147 recorded during 2021-22. The agency has also continued to crack down on increased third-country facilitation of sanctions circumvention by sharing information and intelligence, including through its new Enforcement Coordination Mechanism (ECM). OFSI used its [power](#) to authorise the disclosure of information for the first time in August. OFSI implemented its new Disclosure Enforcement Tool to publicly release details of financial sanctions breaches it deemed insufficiently serious as to warrant a civil monetary penalty.

**£20.6M in fines across 4 firms for deficiencies in anti-financial crime controls, from insufficient CDD to inadequate governance**

Firms can anticipate further use of the power moving forward. Rigorous policies and controls designed to prevent the access of funds to designated persons or entities must continue to be reviewed and reinforced across firms' defence lines to ensure adherence to compliance requirements.

The FCA also published its [planned regulatory initiatives](#) for next two years in November. The [Consumer Duty](#) is scheduled to come into effect for closed products on July 31, 2024. Additionally, [a review of the Senior Managers and Certification Regime \(SM&CR\)](#) is anticipated between April and June 2024 which firms can already begin to prepare for. Continuing its development of a regulatory framework tailored to cryptoassets, the FCA will build on consultations held in 2023, with secondary legislation expected from HMT in 2024. Reforms to the Payment Services Regulations, enabling a risk-based approach to payments, are expected to be laid before Parliament for debate, and efforts to prevent APP scams will undergo continued consultations by the PSR throughout 2024, during which firms can take an active role.





# SECTION TWO:

## European Union





# European Union

Throughout 2023, the European Union 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 cryptoassets. In parallel, the EU demonstrated a commitment to strengthening its existing AML/CTF/CPF regime, implementing reforms, and introducing proposed directives to enhance its effectiveness. Concurrently, the EU maintained its central role in facilitating international collaboration to foster the successful implementation and enforcement of economic sanctions.

## AML/CTF/CPF

In 2023, the European Commission made significant headway in its development of a regulatory regime tailored to the unique landscape of cryptoassets. The formal implementation of the [Pilot Regime for the use of Distributed Ledger Technologies \(DLT\) for Market Infrastructures](#) allowed firms to gain legal certainty in forthcoming regulation through continued private-public sector collaboration. Additionally, the passing of two landmark frameworks for cryptoasset markets illustrated the importance of regulating digital and virtual currency to the European Parliament. Alongside developing new frameworks, the EU has continued to concurrently work on the enhancement of those already in place, supported and supplemented by agencies like MONEYVAL and the European Banking Authority (EBA) to actively help firms align with regulatory expectations.

### UPDATED: High-risk Third Countries (Commission Delegated Regulation (EU) 2016/1675) [Jun to Oct 2023]

Corresponding to the standards set by FATF's country-risk classifications, the European Commission updated its list of high-risk third countries with anti-financial crime deficiencies twice. In June, Nigeria and South Africa were added to the list whilst Cambodia and Morocco were removed, with Cameroon and

Vietnam added in October. As the list of high-risk jurisdictions undergoes regular revisions, firms must ensure that internal controls and databases align with changes as they arise. This is crucial to ensure that geographical risk ratings are appropriate and effective.

### NEW: [The Transfer of Funds Regulation](#) [29 Jun 2023]

In line with the FATF call to action that prompted the introduction of the 'travel rule' for cryptoassets in the UK, the EU adopted the Transfer of Funds Regulation (TFR) in June. The TFR will require Virtual Asset Service Providers (VASPs) to disclose details on transfer recipients and beneficiaries, aligning with existing practice in traditional finance. All VASPs operating in the EU will be subject to the TFR in December 2024, with further guidance on its implementation to follow, a preview of which could be seen in the consultation on such guidelines by the EBA [published](#) in November.

### NEW: [The Markets in cryptoassets Regulation](#) [29 Jun 2023]

The eagerly awaited Markets in cryptoassets Regulation (MiCA) introduced common rules on the issuance of cryptoassets, including stablecoins (known under the regulation as E-Money Tokens (EMT) and Asset-Referenced Tokens (ART), and on compliance expectations for cryptoasset service providers (CASPs). MiCA establishes uniform requirements for firms in areas including disclosures to investors, governance, prudential safeguards, and consumer protection. Notably, MiCA provides a first-of-its-kind framework for the issuance of stablecoins that includes stringent requirements in terms of disclosures, reserve requirements and risk management, that includes further measures in the case of 'significant' ART and EMT. These provisions may set the precedent for developing frameworks elsewhere, including in the UK.

MiCA introduces several new requirements for CASPs operating in the EU, including the management of conflicts of interest, measures to prevent market abuse, and a range of consumer protection and transparency measures. This has effectively incorporated many elements present in existing national regimes, like France's, that will be replaced by this new EU-wide framework. In [July](#) and [October](#), two of three consultation packages on the technical standards that clarify the implementation of various MiCA provisions were published.

The [third](#) is expected to be published in Q1 of 2024, and set to cover all remaining requirements, including provisions on the qualification of cryptoassets as financial instruments, investor protection, and market abuse.

Stablecoin-related provisions are set to enter into application in June 2024, with requirements for CASPS and issuance of other cryptoassets entering into application in December 2024. As firms operating across the digital currency landscape prepare for the new rules to come into force, vigilance and awareness will remain key not just for those regulated under MiCA, but traditional financial firms too, who may have operational exposure to cryptoassets.

### On the Horizon for the EU

In March, three significantly stricter AML/CTF [measures](#) designed to close existing regulatory gaps in the current EU regulatory regime moved closer towards implementation. Members of the European Parliament (MEPs) approved three pieces of draft legislation on the financing provisions of the EU AML/CTF policy. If passed, the policies would introduce a 'single rulebook' of consolidated AML/CTF requirements, amend the Sixth Anti-Money Laundering Directive (6AMLD), and establish a unified [Anti-Money Laundering Authority](#) (AMLA) promoting cooperation and consistency among member states' AML/CTF authorities. [Nine](#) member states submitted applications to host AMLA, with the host city set to be announced in 2024.

In December, the European Parliament and Council [agreed to establish AMLA](#). The primary objectives of

the authority will be to act as a central hub supervising high-risk financial entities across member states, coordinating supervisors, ensuring uniform practices, and assisting FIUs in analysing suspicious transactions. Provisional agreements in December have brought the development of the EU's AML/CTF framework a step closer to fruition. Also included were proposals for revised whistleblowing reporting channels and rules tackling financial sanctions circumvention. As these measures progress closer to enforcement, firms should stay vigilant, monitoring the progress and potential implications of the provisions for their own processes.

Towards the year's close, the European Parliament and Council proposed [a new directive](#) on asset recovery and confiscation. If approved, the law will establish minimum EU-wide regulations for tracing, identifying, freezing, confiscating, and managing criminal assets. Proposed provisions include strengthening the member states' asset recovery entities, implementing property freezing measures for subsequent confiscation, allowing the seizure of criminal instruments and proceeds upon conviction, and mandating asset recovery authorities to manage frozen or confiscated property. Pending member states' endorsement, the new directive would further strengthen the ability of state authorities to seize and recover criminal assets, for which the continued diligence and active participation of European firms would remain key.

### NEW REPORTS: MONEYVAL [Apr to Jul 2023]

In April, the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism

(MONEYVAL) published its [strategy](#) on AML, CTF, and CPF for 2023-2027. Over the next five years, the Committee has pledged to strengthen its efforts to combat the risks across EU member states and territories, encouraging policy and process enhancement at legislative, institutional, and operational levels.

Continuing its focus on preventing the misuse of virtual assets, MONEYVAL issued a [Typologies Report](#) on ML/TF Risks in the sector in July. The report highlighted that different entities pose different risk levels depending on factors including products, services, customers, geography, business models, and the rigour of the entity's compliance framework. As the virtual and digital asset landscape continues to develop in the EU, new risks are likely to be identified moving forward. Firms' effective preparation for forthcoming and future regulatory regimes will be underpinned by consideration of evolving sectoral risks and measures to mitigate them.

### NEW REPORTS: European Banking Authority [Jul 2023]

The EBA issued an updated [assessment](#) of ML/TF risks across the EU financial sector in July, as required under the [Fourth EU Anti-Money Laundering Directive](#). The report detailed new and emerging cross-sectoral risks, continuing risks, and risks specific to firms including life insurance undertakings, investment firms, and cryptoasset service providers. The report clarified the importance for firms of having strong control functions including monitoring and reporting in place if such risks are to be addressed and mitigated.

## Key takeaways: AML/CTF/CPF

- 1 Firms are reminded to align their country risk and EDD processes to the regularly revised list of high-risk third countries
- 2 CASPs are required to disclose details on transfer recipients and beneficiaries under the TFR entering into force at the end of 2024
- 3 MiCA has introduced common rules on the issuance of E-Money Tokens and Asset-Referenced Tokens (i.e. stablecoins, in force from June 2024) and new requirements on issuers of cryptoassets and CASPs (in force from December 2024)

## SANCTIONS

In a year which included the first anniversary of Russia's invasion of Ukraine in February, the European Commission doubled down on its implementation of financial sanctions, having adopted its 12th package of restrictive measures against Russia in December.

The [10th package](#) of sanctions against Russia introduced significant new export bans and restrictions on dual-use and advanced technologies, as well as additional financial restrictions and anti-circumvention enforcement measures. The [11th package](#) introduced new anti-circumvention measures, including the ability for the EU to restrict the sale, transfer, and export of designated categories of goods to third countries that are judged to be at high risk of circumvention.

Most recently implemented, the [12th package](#) continued to highlight the need for stronger anti-circumvention measures. It included the introduction of a new obligation for operators to contractually prohibit the re-export of sensitive goods to Russia and, significantly for the financial sector, a new measure requiring the

notification of certain transfers of funds out of the EU from EU entities directly or indirectly owned by more than 40% by Russians or entities established in Russia. New measures in this package such as the ban on imports of Russian diamonds mirror similar changes in the UK's sanctions regime, underscoring the continued diplomatic alignment and coordination between the UK and EU in combating Russia's proliferation financing and money laundering threats. Firms should take notice of this trend in continuing cross-jurisdictional cooperation and collaboration, as effective sanction implementation can only happen if all parties involved commit sufficient resources to it. The financial sector should be prepared to continue to review and strengthen its sanctions controls in 2024.

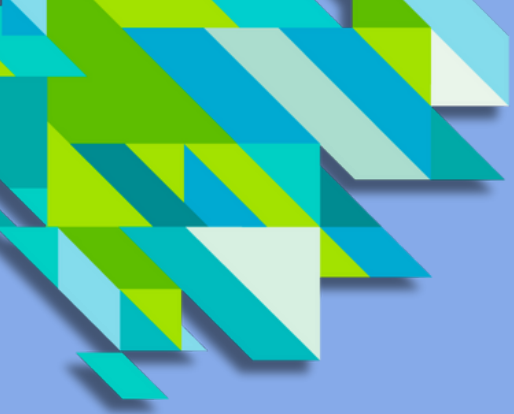
More broadly, key restrictive measures targeting individuals and entities around the world were extended. In October, the European Council prolonged a ban on [chemical weapons](#), extending its sanctions regime against the proliferation and use of chemical weapons until 2026, and prolonging existing measures against persons and entities for another year, until October 2024. In December, the [Global Human Rights Sanctions Regime](#) was bolstered through a three-year extension until 2026, allowing the EU to target individuals, entities, and bodies, including state and non-state actors responsible for global violations and abuses, during which firms' compliance will remain key.

With the EU expanding and extending various restrictive measures, firms should ensure that their compliance processes align with regulatory and legal expectations which are often subject to rapid ongoing development. Compliance with financial sanctions obligations remains essential for mitigating circumvention and evasion risks, upholding the stability of the financial system, and maintaining a positive public reputation. With the EU set to remain committed to its implementation of restrictive measures into 2024, firms' coverage of sanctions risks and requirements within internal frameworks will continue to be crucial.

## Key takeaways: Sanctions

- 1 Firms should ensure that they comply with their financial sanctions obligations and regularly review their screening processes to ensure alignment with EU designations and restrictions
- 2 Bolstered financial sanctions and embargoes targeting Russia indicate that the EU will continue to implement restrictive measures
- 3 EU prolonged restrictive measures concerning chemical weapons and global human rights abuses, extending firms' compliance requirements





# SECTION THREE:

## Hong Kong + Singapore



Both Hong Kong and Singapore's financial sector have experienced significant growth over the past few years, establishing themselves as two of the leading financial hubs in Asia. This development has consequently led to the progression of the FCC landscape in both jurisdictions, with the growth of a strong legal and institutional framework for combating ML/TF/PF and Fraud. However, Hong Kong and Singapore's roles as major global financial centres inevitably exposes them to vulnerabilities as a transit point for foreign proceeds of crime.

In August, Hong Kong authorities carried out a large-scale arrest operation, named '[WISEWORD](#)', which resulted in 314 money laundering related arrests. The suspected crime proceeds amount to HK\$470 million, stemming from online shopping and employment scams, telephone deception, romance scams, and gambling related offences. The Hong Kong Monetary Authority (HKMA) has therefore focused much of its guidance on enhancing customer due diligence and transaction monitoring controls for FIs and encouraging the innovation of network analysis to combat fraud exposure. Additionally, the financial crime risks associated with the emergence of virtual assets have been addressed by Hong Kong's legislative amendments to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), focusing on strengthening the oversight of VASPs to address vulnerabilities of the virtual asset space to criminal exploitation.

Similarly, Singapore's exposure to financial crimes was highlighted in the [transnational money](#)

[laundering case](#) that surfaced in August, involving over S\$2.8 billion in seized or frozen assets, leading to the arrests of 10 suspects on charges related to money laundering and fraud. The case directed the Monetary Authority of Singapore's (MAS) efforts towards strengthening AML/CTF controls on high-risk industries, such as wealth management, and the regulator's determination to mitigate the risks of misusing legal persons/arrangements and complex structures. Additionally, Singapore has mirrored Hong Kong's recognition of the evolving challenges in digital markets and virtual assets, calling for greater attention to risk management and the customer due diligence frameworks of both FIs and VASPs to combat illicit cash flows.

## AML/CTF/CPF

### [SG NEW: Circular on Money Laundering and Terrorism Financing Risks in the Wealth Management Sector \[03 Mar 2023\]](#)

A MAS Circular on ML/TF risks in the wealth management sector outlined important guidelines for the industry on effectively tackling recognised risks. It established how MAS expects FIs to review their current AML/CTF controls, particularly by encouraging heightened transparency and reporting. The circular urges FIs to identify their high growth areas, taking steps to ensure that controls remain adequate to combat the evolving ML and TF risks. This includes:

- Strengthening Board and Senior Management functions

- Enhancing CDD practices in high growth areas to particularly scrutinise higher risk customers
- Increasing vigilance towards high-risk customer transactions, understanding key controllers behind the structures/arrangements used for the purpose of wealth management.

The paper further stresses the importance of collaboration with regulatory authorities and law enforcement to combat financial crime, which has since the publication of the circular become an issue of further pertinence in Singapore following investigations into the S\$2.8 billion money laundering scandal. According to the on-going investigation, Singapore's wealth management sector had been exploited by criminals as one point of entry for laundering illicit funds. The circular emphasised the need for enhanced customer due diligence measures and transaction monitoring processes to reinforce proactive measures and collaborative endeavours, ensuring regulatory compliance.

### [HK UPDATED: Cap. 615 Anti-Money Laundering and Counter-Terrorist Financing Ordinance \(AMLO\) \[Apr and Jun 2023\]](#)

New amendments to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance have established special requirements for virtual asset transfers and strengthened due diligence requirements for FIs and DNFBPs. The legislative changes emphasise the alignment of VASPs with Hong Kong's AML/CTF requirements, holding VASPs accountable to the regulatory obligations of banks and securities firms.



In particular, section 13A under Schedule 2 orders VASPs to apply for a licence from the Securities and Futures Commission (SFC) and record detailed information before conducting these transfers. This means that the ordering financial institution is now mandated to record the originator's name, account details, address, and customer identification and submit this information to the beneficiary institution for all transfers exceeding HK\$8000. These changes demonstrate Hong Kong's commitment to address the risks of money laundering and terrorist financing in virtual asset services; the new requirements are expected to bolster transfer transparency and hold licensed VASPs accountable to existing AML/CTF provisions.

Additional amendments within Schedule 2 (sections 3, 5 and 20) have further developed due diligence procedures for virtual assets and PEPs, applicable across FIs and DNFBPs. The changes require FIs and DNFBPs to establish and maintain effective procedures for identifying and handling customer relations.

**HK UPDATED:** [Guideline on Anti-Money Laundering and Counter Financing of Terrorism \(For Stored Value Facility Licensees\)](#) [01 Jun 2023]

The HKMA's revisions to its AML/CTF Guidance for Stored Value Facility Licensees has reflected the legislative amendments to the AMLO, by now recognising VASPs as a viable medium of exchange and currency. In consideration of the requirement for VASPs to obtain a license under the SFC regime, the

HKMA has now acknowledged the evolving banking landscape. Subsequently, the HKMA has reinforced the new compliance requirements that align VASP regulatory obligations to those applicable to other FIs. These include adherence to CDD, information-sharing, transaction screening, and record-keeping standards. Additionally, the HKMA replaced the terminology of 'Foreign PEP' with 'Non-Hong Kong PEP' and encouraged firms to review PEP and trust relationships, ensuring alignment with the new regulations and guidance and the appropriate application of CDD procedures.

**HK UPDATED:** [Guideline on Anti-Money Laundering and Counter Financing of Terrorism \(For Licensed Corporations and SFC-licensed Virtual Asset Service Providers\)](#) [01 Jun 2023]

In response to the concomitant AMLO updates in Hong Kong, the SFC's updated Anti-Money Laundering Guidelines introduced a new Chapter 12 addressing the money laundering and terrorist financing risks associated with 'Virtual Assets'. The chapter outlines the AML/CFT regulatory requirements, including:

- Conducting risk assessments under an RBA
- Virtual asset specific requirements in conducting CDD and ongoing monitoring
- Requirements in relation to virtual asset transfers and third-party deposits and payments in the form of virtual assets

Significantly, the updates incorporate the 'Travel Rule', requiring payment issuing institutions to

provide customer identifying information to receiving institutions along with every transaction, akin to existing requirements for wire transfers. Other key revisions include an updated definition for PEPs and beneficial owners of trusts. The SFC's new identification of 'Non-Hong Kong PEPs' and 'Hong Kong PEPs' from section 4.11.7 onwards has clarified due diligence requirements for firms by replacing the former and less distinctive terms 'foreign PEP' and 'domestic PEP'. The amendments to section 4.3.10 remove the former 25% vested interest threshold in the trust property, to now include a beneficiary or a class of beneficiaries and trustees; thus expanding the SFC's supervision of beneficial owners of trust customers. In light of these changes, the SFC has recommended licensed corporations and associated entities to conduct a thorough review of their AML/CFT policies and procedures to ensure continued compliance with all applicable requirements.

**HK NEW:** [Securities and Futures Commission \(SFC\) Disciplinary Fining Guidelines](#) [01 Jun 2023]

Testament to Hong Kong's ongoing alert to evolving financial crime risks and in immediate response to the drastic amendments of the AMLO, the SFC

published guidance outlining its disciplinary power to impose fines on regulated persons in June. According to these guidelines, the SFC, empowered by section 53ZSP of the AMLO, may impose fines based on intentional conduct, damage to Hong Kong's reputation, and facilitation of money laundering. Through these considerations, the SFC will reflect on the number of affected persons as a multiplier for the fine issued but will assess each case individually. The guidelines emphasise deterrence, protecting Hong Kong's financial reputation, and ensuring proportionality and consistency in the application of penalties.

**SG NEW: [Management of money laundering, terrorism financing, and sanctions risks from customer relationships with a nexus to digital assets](#) [11 Jul 2023]**

The AML/CFT Industry Partnership (ACIP) of Singapore's best practices report provided a foundational framework to advance the understanding and management of money laundering, terrorist financing and sanctions risks in the Digital Assets space. The report reiterated that firms ought to enhance their risk assessment procedures when identifying customers with a nexus to cryptocurrencies. It also recommended due diligence and ongoing monitoring measures for Digital Payment Token Service Providers (DPTSPs), and for FIs and non-bank FIs (NBFIs) dealing with digital assets.

**SG NEW: [MAS Finalises Stablecoin Regulatory Framework](#) [15 Aug 2023]**

Following its [public consultation](#) launched in October 2022, MAS finalised its policy position on a new regulatory framework for stablecoins in August. Its principal objective was to ensure a high degree of value stability, as stablecoins are digital payment tokens designed to maintain constant value against at least one non-digital native asset, usually one or more fiat currencies. MAS' regulatory framework applies specifically to single currency stablecoins (SCS) pegged to the Singapore Dollar or any G10 currency issued in Singapore. Issuers of these stablecoins must now adhere to key requirements related to value stability, capital, disclosures, and redemption at par (with an issuer requirement to return par value of SCS five days upon a holder return request).

This framework is instrumental in allowing stablecoin issuers to meet all criteria

to apply for MAS recognition, designating their stablecoins as a 'MAS-regulated stablecoins'. This will help users differentiate regulated from unregulated digital payment tokens, ultimately with the hope of safeguarding consumers as well as macro-economic stability. While firms await MAS' issuance of draft legislative revisions including [amendments to the Payment Services Act](#), the promotion of the use of regulated stablecoins will support wider efforts to reduce user exposure to fraud.

**SG NEW: [Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures](#) [30 Aug 2023]**

MAS' paper on strengthening AML/CTF controls to mitigate risks of misuse of legal persons/arrangements and complex structures stemmed from an inspection of multiple FIs. It was also issued against the backdrop of the S\$2.8 billion money laundering scandal, where [shell companies](#) had been used to obfuscate the ultimate beneficial ownership, as well as the origins of the funds. MAS had previously initiated inspections which detected multiple FIs facilitating potentially suspicious fund flows through legal persons/arrangements and complex structures.

The publication set forth MAS' supervisory expectations, providing clear guidance on the responsibilities of FIs, lawyers, trust companies, and corporate service providers in identifying and mitigating risks associated with legal persons and complex structures. The typologies and case studies observed by MAS's investigation highlighted the need for robust customer due diligence processes, ongoing monitoring of customer relationships, and the reporting of suspicious activities. Above all, MAS emphasised the importance of senior management in monitoring the effective implementation of AML/CFT controls to ensure the maintenance of a strong culture of compliance.

**HK NEW: [RegTech case studies, tools, and platforms](#) [Throughout 2023]**

Since the HKMA's [AML/CFT RegTech Forum in November 2019](#), the number of banks deploying RegTech solutions for AML has increased by almost 30%, with more frequent and open collaboration across the financial system. The HKMA has continued to promote the responsible adoption of RegTech across the industry by publishing two new reports, which introduce innovative ways of



reducing and preventing the harm and losses from fraud and financial crime. The [‘AML RegTech: Network Analytics’](#) report highlighted the potential for integrating intelligence-led analytical tools with rules-based monitoring systems, aiming to leverage internal and external data analysis to reinforce the transaction monitoring and due diligence framework of banks. The guidance will serve as a key reference point for banks in their exploration and adoption of network analytics to encourage enhanced capabilities in preventing, detecting, and disrupting financial crimes. The report included the experiences of banks who have already deployed this type of AI-enhanced RegTech solutions, providing practical insights and expert perspectives to other FIs exploring the adoption of network analytics.

The [‘AML/CFT RegTech: Case Studies and Insights Volume 2’](#) looked at the experience of banks that have incorporated more sophisticated technologies to increase their effectiveness in combating digital fraud and financial crime. The report provided a comprehensive view of 4 broad areas of RegTech implementation, including real-time fraud monitoring, machine learning for transaction monitoring alerts handling, natural language processing for media monitoring, and analytics providing a ‘single view of the customer’. These strategies aim to enhance Know your customer (KYC) frameworks and transaction monitoring capabilities of firms by increasing their ability to detect suspicious accounts and providing greater support to their data analytics. Understanding that there is no ‘one-size-fits-all’ RegTech solution for FIs, the HKMA recommends banks to refer to each case study to facilitate internal discussions on what more can be achieved in further raising AML/CFT effectiveness through RegTech adoption.

Overall, by aiming to strengthen the banks' gatekeeper role in its fight against financial crime, HKMA's promotion of RegTech solution cements its determination to preserve the integrity and stability of the financial system.

### Key takeaways: AML/CTF

- 1 Introduction of section 13A of Schedule 2 in the AMLO for VASPs
- 2 In response to AMLO amendments on VASPs, the HKMA and SFC's AML/CTF Guidelines have been updated to include requirements on VASPs and revisions to the definition of PEPs
- 3 VASPs must apply for a license from the SFC
- 4 New MAS guidelines on the wealth management sector reinforce CDD requirements
- 5 MAS spotlighted the associated risks with legal persons/arrangements and complex structures
- 6 MAS' finalised its policy position on a stablecoin regulatory framework
- 7 ACIP's best practices report called for strong risk management frameworks for FIs, DPTSPs, and NBFIs given the rising risks in the Digital Asset space

## FRAUD

Considerable emphasis has been placed on further developing fraud detection systems, which are expected to reduce the risk exposure of FIs. Combating fraud has become an even increasingly pertinent objective for HK authorities following a number of law enforcement operations in Hong Kong, which have uncovered the extent of the post-pandemic growth in local fraud operations.

### HK NEW: [Enhanced approaches to combat digital fraud \[12 Oct 2023\]](#)

The HKMA continues to actively monitor the prevalence of digital fraud and has prioritised efforts to fortify the banking sector's response by providing regulatory support in guidance papers. The HKMA published its paper outlining the enhanced approaches to combat fraud that firms can take to combat digital fraud. This, as the paper itself remarks, came against the backdrop of a significant surge in fraud-related banking complaints in the first nine months of 2023, totalling 954 cases— surpassing the total 555 cases in 2022. The report underscored the importance of allocating sufficient resources for the successful implementation of systems and controls. As part of this initiative, the HKMA highlighted the Fraud and Money Laundering Intelligence Taskforce (FMLIT)

championing a bank-to-bank information sharing platform, known as Financial Intelligence Evaluation Sharing Tool (FINEST). FINEST encourages Authorised Institutions (AIs) to expand data inclusion and deploy real-time network analytics in their fraud monitoring systems, while actively developing a pre-transaction alert mechanism. These combined efforts stress the commitment to strengthening information sharing, transaction monitoring, and customer alert mechanisms, to collectively reinforce the resilience of the banking sector against the ongoing exposure to digital fraud.

### [SG NEW: Consultation on Proposed Shared Responsibility Framework \[25 Oct 2023\]](#)

In response to the global increase in digitally enabled scams and corresponding financial losses, the MAS and Infocomm Media Development Authority (IMDA) published its consultation on a proposed Shared Responsibility Framework (SRF). This aims to distribute accountability for scam losses among FIs, telecommunication operators (Telcos), and consumers, particularly for unauthorised transactions resulting from phishing scams. Recognising that the responsibility for scam prevention extends beyond consumers, the Government is proposing that FIs and Telcos should share the responsibility and provide compensation to victims of specified phishing scams if anti-scam duties are violated. FIs will be expected to ensure that crucial communication channels are in place to keep consumers informed.

To safeguard these aims, MAS and IMDA have proposed:

- Imposing a 12-hour cooling off period upon activation of digital security tokens during which 'high-risk' activities cannot be performed
- Provide outgoing transaction notification alert(s) on a real-time basis
- Notification alert(s) for the activation of digital security token and conduct of high-risk activities on a real-time basis; and
- Provide a (24/7) reporting channel and self-service feature ('kill switch') to report and block unauthorised access to their accounts

MAS and IMDA will have received feedback on the key areas of the framework and will implement SRF via a set of Guidelines ('SRF Guidelines') following the close of the consultation period on 20 December 2023.

## Key takeaways: Fraud

- 1 HKMA underlines effort to combat digital fraud, urging FIs to develop network analytics in their transaction monitoring framework
- 2 MAS and IMDA releases consultation on the proposed SRF aiming to increase the accountability of FIs and Telcos to support scam prevention controls

## ENFORCEMENT AND DISCIPLINARY ACTIONS

### [HK: Westpac Banking Corporation, Fined HK\\$4,000,000](#)

On 31 January 2023, the HKMA concluded its investigation and disciplinary proceedings concerning Westpac Banking Corporation, Hong Kong Branch (WBCHK). The HKMA levied a monetary penalty of HK\$4,000,000 on WBCHK for violations of the Anti-Money Laundering Ordinance (AMLO). The deficiencies identified in the investigation pertain to delays in conducting periodic reviews for certain customers in the timeframe from June 1, 2016, to May 31, 2017. This underlies the HKMA's intolerance for weak systems and controls relating to KYC and monitoring.

### [HK: EFG Bank AG, Fined HK\\$16,000,000](#)

On August 15, the HKMA disclosed the completion of its investigation and disciplinary procedures pertaining to EFG Bank AG, Hong Kong Branch (EFGHK). HKMA enforced a financial penalty of HK\$16,000,000 on EFGHK for breaches of the (AMLO). The investigation revealed the gaps in controls for CDD on customers transferred from another financial institution during the period from 21 February 2016 to 16 January 2018. In addition to this, from 1 April 2012 to 31 October 2018, the HKMA found the EFGHK failed to establish and maintain effective procedures for

carrying out its duties under the AMLO in relation to CDD and on-going monitoring of business relationships with customers. Therefore, given the multiple deficiencies in EFGHK's controls framework, the bank amassed the largest compliance fine of 2023 from the HKMA.

### HK: [CA Indosuez \(Switzerland\) SA, Fined HK\\$3,500,000](#)

On 29 November 2023, the HKMA took disciplinary action against CA Indosuez (Switzerland) SA following control failures relating to the AMLO. A penalty of HK\$3,500,000. The HKMA's discovery of control deficiencies at CAHK, linked to the failures in consistently monitoring the business relationship with certain customers. Hence leading to the ineffective scrutiny on transactions. In imposing this fine, the HKMA emphasised the importance of sending a strong warning to CAHK and the entire industry regarding the significance of having robust risk management controls and procedures in place to tackle the risks associated with money laundering and terrorist financing.

### HK: [TNG \(Asia\) Limited \(TNG\), Fined HK\\$1,575,000](#)

On 18th December, the HKMA reprimanded and ordered TNG to pay a penalty of HK\$1,575,000 following the contravention of section 8Q of the Payment Systems and Stored Value Facilities Ordinance. From 2016 to 2020, TNG failed to establish adequate and suitable systems of control. This included lapses in governance structures, inefficient transaction monitoring and risk management frameworks, and weak internal controls that could support effective and efficient operations. The fine reinforced the HKMA's emphasis on the fundamentals for a sound risk management framework, stressing the importance of SVF licensees to maintain robust governance structures, internal control systems, and a high level of compliance awareness among both management and staff members.

### SG: [MAS Penalises 3 Banks and an Insurer for Breaches of Anti-Money Laundering Requirements](#)

On 21st June, MAS imposed composition penalties amounting to S\$3.8 million on Citibank N.A., Singapore Branch (Citibank), DBS Bank Ltd (DBS), OCBC Singapore (OCBC), and Swiss Life (Singapore) Pte. Ltd. (SLSG) after being found to have inadequate AML/CFT controls in place when they dealt with persons who were involved in transactions with, or had links to, Wirecard AG or its related parties.

- **Citibank:** MAS issued a fine of S\$400,000 for failure to adequately understand the control structure of two corporate customers. Deficiencies in identifying the customers' beneficial owner (BO), despite having access to the customer information, suggested that the control structure and BOs declared by the customers were incorrect.
- **DBS:** The largest fine of the group, S\$2.6 million, was issued to DBS for deficiencies in the maintenance of CDD information relating to customers' beneficial ownership, failure to update customers' ML/TF risk ratings, inadequacies in establishing the source of wealth (SoW) of higher risk customers and their BOs and the failure to inquire into the background and purpose of unusually large transactions that were not consistent with its knowledge of the customers or had no apparent economic purpose. These breaches concerned the accounts maintained by 11 corporate customers, hence the severity of MAS's penalties.
- **OCBC:** MAS has imposed a penalty of S\$600,000 for the bank's failure to inquire into the background and purpose of transactions despite not being consistent with OCBC's knowledge of the customer and its business. OCBC's further failure to probe into this single corporate customer's ownership and control structure when the customer's declared BO was not a party named in the customer's corporate registration documents, therefore increased the severity of the penalty.
- **SLSG:** Following breaches in May 2017, SLSG was been fined S\$200,000. Relating to an investment-linked life insurance policy underwritten, failures to sufficiently understand the reasons behind the higher risk customer's complex ownership, control structure and the failure to adequately corroborate the SoW of the customer's BO has resulted in MAS's enforcement action.

In response to this scrutiny, MAS recognised that the involved FIs enhanced their procedures, processes, and training to improve staff vigilance in detecting and escalating risk concerns.

## Key takeaways: Enforcement + Disciplinary Action

- 1 The SFC reinforces its enforcement powers
- 2 HKMA has fined the Westpac Banking Corporation and EFG Bank a combined \$20,000,000
- 3 MAS imposed penalties on Citibank, DBS Bank Ltd, OCBC Singapore, and Swiss Life





# SECTION FOUR:

## Global Outlook



## The Wolfsberg Group

The Wolfsberg Group, the non-governmental group of thirteen banks, continued to provide enhanced guidance to FIs during 2023. The Group updated several of its resources which continue to benchmark the global industry standard in combating financial crime and guide FIs in their compliance processes. The Group contributed its industry insights to FATF consultations on [combatting the abuse of NPOs, beneficial ownership and transparency of legal arrangements](#), the EBA's [call for evidence](#) on revised AML/CTF guidelines, and the HMT [consultation](#) on reforming the AML/CTF supervisory regime in the UK.

**UPDATED:** [Correspondent Banking Due Diligence Questionnaire and Financial Crime Compliance Questionnaire \[10 Feb 2023\]](#)

The Wolfsberg Group released version 1.4 of the Correspondent Banking Due Diligence Questionnaire (CBDDQ) and version 1.2 of the Financial Crime Compliance Questionnaire (FCCQ), accompanied by additional guidance and FAQs for FIs designed to allow banks and other firms to assess their financial crime risks. Changes across the two documents included the addition of new guidance on fraud and additional questions on whistleblower policy, virtual bank licenses, and sanctions policy endorsement. The Group's recommended timeframe for the update of the Questionnaires was increased from 12-18 months as to better align with the CDD review periods for firms.

**UPDATED:** [ABC Compliance Programme Guidance \[17 Apr 2023\]](#)

The Wolfsberg Group replaced its 2017 anti-bribery and corruption (ABC) Compliance Programme Guidance in April with an updated publication, providing guidance on the development and implementation of an effective risk-based approach to ABC compliance. The publication provided further information and direction for firms on areas including a firm-wide ABC policy, governance, periodic risk assessments, training and awareness, monitoring, and testing, amongst others. The publication was released as part of the Group's objective to promote a culture of ethical ABC practices and compliance with legal and regulatory requirements.

**UPDATED:** [Payment Transparency Standards \[17 Oct 2023\]](#)

Continuing with its revision of previously published guidance, the Group issued revised Payment Transparency Standards in October, so as to reflect various changes that have occurred across the payment methods sector since the original document was published in 2017. The updated guidance included an expanded list of key stakeholders previously addressed and clarified the roles and responsibilities of intermediary agents. The applicability, roles, and responsibilities of the Standards relevant to key stakeholders within the payment chain were detailed, with further guidance provided on payment flows and the challenges and limitations surrounding payment transparency.

## CONCLUSION

In 2023, common trends and distinct variations emerged across the regulatory frameworks of the four jurisdictions examined in this paper. Firms should remain aware of these trends in anticipating continued regulatory action in 2024.

Fraud was a central focus for regulators in the UK and Hong Kong. After announcing the PSR mandatory reimbursement and the upcoming Failure to Prevent Fraud Offence, the UK will continue to combat fraud in 2024 in line with the ECCT's objectives. The focus on fraud was illustrated through the bolstering of powers for authorities in Hong Kong, several high profile arrests and raids by the HKPF targeting the increase in domestic scam networks, the publication of guidance papers and reports, and the launch of bank-to-bank information sharing platform, FINEST. Hong Kong authorities are set to continue to clamp down on fraud in 2024 both in law enforcement operations as well as from a regulatory perspective. In Singapore, fraud is expected to become a major financial crime focus in 2024, following the publication of MAS & IMDA's consultation on a proposed SRF towards the end of 2023.

Corporate transparency has been another cross-cutting theme. NBFIs and non-financial sectors have received particular attention, combatting their potential vulnerabilities for money laundering and sanction evasion. Across the UK and Singapore, regulators have established new AML standards for the wealth management sector, calling firms to step up their compliance controls. Similarly, precious metals and stones dealers have been the focus of alerts and further compliance expectations in both jurisdictions, which can be partially attributed to the role that gold and diamond trading is expected to be playing in Russian sanctions circumvention. Firms can expect regulators to exercise greater scrutiny on the implementation of AML and sanction controls to non-bank institutions.

Significant progress was made by all four jurisdictions towards regulating digital assets and alternative currencies in 2023. The EU was instrumental in developing a regulatory regime tailored to the complexities of new currencies (MiCA and TFR) and corresponding guidance for its implementation. Firms should pay particular focus to MiCA's implementation in 2024, as the landmark regime is shaping regulatory developments in other jurisdictions. For example, this has already been seen in the outline of the proposed future regime for regulating cryptocurrencies in the UK, which follows the MiCA blueprint albeit with some variations.

Hong Kong and Singapore are similarly scheduled to develop their own tailored regimes. Overall, regulators in 2023 have started to move from registration-based regimes, where firms' AML / CTF were the main aspect considered, to fuller licensing regimes that require a holistic approach to compliance. Regulatory Regimes are beginning to cover all other aspects of regulation hitherto applicable to their counterparts in traditional finance. Issuers of stablecoins and other cryptocurrencies will be increasingly subject to disclosure and prudential requirements. Lastly, from 2024 firms are likely to see further movement towards the regulation of areas including DeFi and NFTs.

Sanctions have remained a major point of focus for the EU and the UK and will continue to remain so for the upcoming year. Firms should bolster their sanctions controls and pay attention to on-going alerts and other guidance on countering sanctions evasion. Sanctions remain an important economic tool, with impact intrinsically linked to effective implementation and enforcement. It is therefore the duty of all regulated firms to ensure they comply with existing sanctions by establishing controls in line with national and international standards, and by adopting industry best practices. OFSI's unprecedented use of its Disclosure power in 2023 served as a warning to firms of the financial and reputational cost of failing to prevent sanction evasion.

Lastly, an increase in cross-jurisdictional and inter-agency collaborations was notable in 2023. From EU-UK coordination on Russian sanctions to international partnerships on fraud and AML/CTF, the transnational nature of financial crime in a globalised world has reinforced the importance of taking a transnational approach to tackling it. It is thus necessary for jurisdictions to aim towards greater cross-jurisdictional cooperation in both the prevention and persecution of financial crimes, even if progress may be slowed by the complexities of international coordination.

Inter-agency cooperation achieved faster progress across several jurisdictions. In the UK for instance, the NCA and OFSI cooperated in releasing two Red Alerts, and the FCA, the Bank of England, and the PRA partnered on exploring the future use of alternative currencies. The HKPF has established a dedicated working group in collaboration with the SFC to monitor and investigate illegal activities related to VASPs. In Singapore, a new inter-ministerial committee was launched, with the purpose of reviewing and strengthening Singapore's AML regime. Firms should monitor these initiatives and expect greater integration between government agencies and regulators at the enforcement level in 2024, during which their involvement will prove key.

Plenitude Insights



# APPENDIX A: Summary Table of changes

	CDD & Corporate Transparency	AML / CTF/CPF Information Sharing	Cryptoassets	Sanction	Fraud
UK	<ul style="list-style-type: none"> <li>Expanded requirement for firms to report beneficial ownership discrepancies to Companies House before establishing a business relationship and periodically thereafter under Regulation 30A. [MLRs update, p. 10]</li> <li>Companies House reform [ECCT, p. 11]</li> <li>Updated EDD requirements for high-risk countries and trusts [JMLSG update, p. 12]</li> <li>New AML guidance for sectors including wealth management firms and financial advisors [JMLSG update, p. 12]</li> <li>Anti-SLAPPs protections [ECCT, p.11]</li> <li>Changes in corporate criminal liability [ECCT, p. 11]</li> <li>OFSI's first use of its Disclosure of Information power [p. 15]</li> <li>Requirement for firms to conduct a PF risk assessment implement PF policies, controls, and procedures [JMLSG update, p. 12]</li> <li>New revisions to ID&amp;V and Discrepancy Reporting expected to gain approval in 2024 [JMLSG update, p. 12]</li> </ul>	<ul style="list-style-type: none"> <li>Lessen the regulatory burden on firms to submit, and law enforcement to process, DAML, and arising SARs [POCA update, p. 10]</li> <li>Increase in threshold amount from £250 to £1,000 [POCA update, p. 10]</li> <li>Bureaucratic streamlining of SAR process by waiving the civil liability on breaches of confidentiality for information provided with the intention of combatting economic crime [ECCT, p.11]</li> </ul>	<ul style="list-style-type: none"> <li>Introduction of Travel Rule [MLRs update, p. 10]</li> <li>New guidance for cryptoasset providers and custodian wallet providers [JMLSG update, p. 12]</li> <li>Enhanced powers of law enforcement of recovering cryptoassets [ECCT, p. 11]</li> <li>Extension of the Financial Promotions regime to cryptoassets [FSMA, p. 9]</li> </ul>	<ul style="list-style-type: none"> <li>OFSI's guidance on the Oil Price Cap [p.14]</li> <li>Guidance on Enforcement and Monetary policies [p. 14]</li> <li>Guidance on licence applications [p.14]</li> <li>Guidance for high-value dealers [p. 14]</li> <li>OFSI's Red Alerts on sanction evasion in gold trading and sanction evasion for high-risk goods [p. 14]</li> <li>Establishment of Office of Trade Sanctions Implementation (OTSI) [p.14]</li> </ul>	<ul style="list-style-type: none"> <li>PSR mandatory reimbursement for APP Fraud [FSMA, p. 13]</li> <li>'Failure to Prevent Fraud' Offence [ECCT, p. 13]</li> </ul>
EU	<ul style="list-style-type: none"> <li>Updated list of high-risk countries [European Commission, p17]</li> <li>Updated AML/CTF risk assessment across EU financial sector [EBA report, p. 18]</li> <li>MONEYVAL's strategy on AML, CTF and CPF for 2023-27 [p.18]</li> </ul>	<ul style="list-style-type: none"> <li>Progress toward single AML authority (AMLA) and single AML 'rulebook' across EU [proposed amendment to 6AML, p. 18]</li> </ul>	<ul style="list-style-type: none"> <li>CASPs AML guidance, E-Money Tokens, and Asset-Referenced Tokens issuance rules [MiCA, p. 17]</li> <li>Pilot Regime for the use of Distributed Ledger Technologies (DLT) [p. 17]</li> <li>New CDD requirements for cryptoasset transfers [Transfer of Funds regulation, p. 17]</li> </ul>	<ul style="list-style-type: none"> <li>Restrictive measures prolonged [EU Global Human Rights Sanctions Regime, p. 19]</li> <li>12th package of sanctions against Russia launched [p. 18-19]</li> <li>Extended regime against chemical weapons proliferation [p.19]</li> </ul>	
HK	<ul style="list-style-type: none"> <li>Strengthened AML requirements for FIs and DNFBPs [AMLO update, p.22]</li> <li>SFC's new guidelines for disciplinary fining [p. 23]</li> </ul>	<ul style="list-style-type: none"> <li>Strengthened due diligence requirements for FIs + DNFBs [AMLO update, p. 22]</li> <li>New PEPs definition [HKMA's Guidelines on AML/CTF, update, p. 23]</li> <li>New report on potential for integrating intelligence-led analytical tools with rules-based monitoring systems [AML RegTech: Network Analytics, p. 25]</li> <li>HKMA, HKAB, and HKPF launched Financial Intelligence Evaluation Sharing Tool (FINEST), a bank-to-bank information sharing platform to combat fraud [p. 26]</li> </ul>	<ul style="list-style-type: none"> <li>VASPs licensing regime [AMLO update, p. 23]</li> <li>AML controls on cryptoasset transfers [AMLO update, p.23]</li> <li>Guidelines on AML/CTF for licensed VASPs [SFC's AML Guidelines update, p. 23; HMKA's AML Guidelines update, p. 23]</li> </ul>		<ul style="list-style-type: none"> <li>Enhanced approaches to combat digital fraud [p. 25]</li> <li>Report on RegTech solution to live Fraud monitoring [AML/CFT RegTech: Case Studies, p. 25]</li> </ul>
SG	<ul style="list-style-type: none"> <li>New AML/CTF guidelines for wealth management [Circular on AML/CTF risk in WM, p. 22]</li> <li>Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures [p. 24]</li> </ul>		<ul style="list-style-type: none"> <li>MAS finalised regulatory framework for stablecoins [p. 24]</li> <li>Management of ML/TF and sanctions risks from customer relationships with a nexus to digital assets [ACIP, p.24]</li> <li>New proposed for 12h cooling off period upon activation of digital security tokens during which 'high-risk' activities cannot be performed [Consultation on SFR, p. 26]</li> </ul>		<ul style="list-style-type: none"> <li>New consultation on proposed Shared Responsibility Framework (SRF) [p. 26]</li> </ul>

**Authors: Imogen Cronin, Orel Garcia, Valentina Pegolo**

**Contributors: Giles Christou, Eleanor Hancock, Kaitlin Long, Leeroy Masamba**

---

## Plenitude RegSight

Plenitude RegSight is the simplest and most effective way to manage your Financial Crime Compliance obligations and provides assurance that your organisation is meeting these obligations, in a world of ever increasing regulation and heightened regulatory scrutiny. Our subscription newsletter aims keep you informed of the evolving regulatory landscape in the UK, EU, and Hong Kong. Our team conducts weekly horizon scanning to identify new and amended laws, regulations or guidance impacting your organisation's Financial Crime Compliance obligations.

To learn more, or if you wish to subscribe to our newsletter, email us at [enquiries@plenitudeconsulting.com](mailto:enquiries@plenitudeconsulting.com) or visit us at [www.plenitudeconsulting.com/what-we-do/plenitude-regsight/](http://www.plenitudeconsulting.com/what-we-do/plenitude-regsight/)

## About Plenitude

Plenitude is a niche consultancy, specialising in Financial Crime Risk and Compliance and are appointed to the Financial Conduct Authority's Skilled Persons panel for Financial Crime (Lot E). Our focus is firmly on addressing the legal, regulatory, reputational and social imperative for financial institutions to take diligent and rigorous steps to mitigate financial crime risks.

We help our clients meet their regulatory obligations and reduce their financial crime risk exposure by providing deep subject matter expertise, advisory and transformation services. Our services are augmented with RegTech subscription products that gives our clients enhanced insight into the vast array of Financial Crime Compliance (FCC) laws, regulations, guidance and risk indicators, to more effectively manage financial crime risk while reducing overall costs.

We work with a wide array of financial institutions including retail, commercial and investment banks, insurance companies, asset management, payment services, electronic money, FinTech, professional services and crypto firms across the UK, Germany, France, Luxembourg, Nordics, Asia and the EU, and have provided advisory services on some of the largest and most complex FCC transformations in the industry, across multiple sectors and jurisdictions.