waystone | Compliance Solutions

Regulatory Update

Middle East, March 2026

Issued 14 April 2026

Table of Contents

1. DIFC AND DFSA LATEST DEVELOPMENTS

1.1 DFSA Publishes Dear SEO Letter

On 1 March, the Dubai Financial Services Authority ('DFSA') issued a Dear SEO Letter "Regional Uncertainties" outlining its supervisory expectations in light of the rapidly evolving situation in the Middle East and the potential implications for financial markets, firm operations, and the wider economic environment. The DFSA emphasised its close coordination with the UAE and Dubai authorities to support financial stability, market confidence, and the orderly functioning of the DIFC.

The DFSA confirmed that it has activated its business continuity arrangements to ensure uninterrupted delivery of its regulatory and supervisory functions. Supported by ongoing investments in digitalisation and regulatory technology, the DFSA stated that its operations continue with minimal disruption.

In the current environment, the DFSA also reminded firms of the importance of maintaining robust operational resilience and effective risk-management frameworks. Firms were expected to:

- assess and, where necessary, enhance business continuity and contingency arrangements, including for critical third-party and cross-border dependencies
- ensure governance, escalation, and management-information processes remain effective
- remain vigilant to heightened liquidity, credit, market, operational, and cyber risks, and take appropriate mitigating actions
- communicate openly with the DFSA regarding any material issues, disruptions, or emerging risks that may affect their ability to operate in an orderly manner or meet regulatory obligations.

You can read the DFSA Dear SEO Letter here.

1.2 DFSA Issues Notice for NASDAQ

On 2 March, the DFSA announced the temporary closure of Nasdaq Dubai for Monday, 2 March until 4 March. The decision was communicated as part of the DFSA's ongoing monitoring of regional developments and their potential impact on financial markets and operational continuity.

You can read the DFSA notices in full here and here.

1.3 DFSA Issues Notice to Investors

On 3 March, the DFSA reminded investors to exercise heightened caution during periods of global tension. The regulator notes that short-term market volatility, misinformation, and phishing attempts tend to increase in uncertain environments. Investors are urged to verify that any online information comes from legitimate and reliable sources and to avoid sharing or amplifying unverified content.

You can read the DFSA notice in full here.

1.4 DFSA Publishes Amendments to Its Regulatory Framework

On 5 March, the DFSA issued miscellaneous amendments to the Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module ('AML'), the Fees Module ('FER'), and the Prudential – Investment, Insurance Intermediation and Banking Business Module ('PIB').

Key updates to the FER Module include:
- introduction of application fee for Designated Non-Financial Businesses and Professions ('DNFBPs'), covering both application and initial registration periods
- the initial annual fee is determined by multiplying US$ 6,000 by the number of full calendar months remaining in the year from the date of registration, divided by 12.

Key updates to the PIB Module include:
- addition of "regulated bank or deposit-taker" for liquid assets being held as deposits
- removal of requirements for an Authorised Firm to exclude from its total ASA any amounts already captured within its K-AUM Requirement
- Removal of the requirement for an Authorised Firm to exclude from its total ASA any amounts that are already included in the firm's calculation of its K-ASA Requirement under Rule 3.8C.4(2)(a).

Under the AML Module, amendments were limited to the addition of "main activities" under section 15.1.4 for DFNBPs concerning notification to the DFSA.

DFSA also updated its Frequently Asked Questions on Anti-Money Laundering, Counter-Terrorist Financing, and Countering Proliferation Financing. The revised AML FAQ is available on the DFSA website.

You can find the DFSA notice of amendments here and here.

1.5 DFSA Publishes Dear SEO Letter on Business Continuity Measures

On 11 March, the DFSA issued a Dear SEO Letter titled "Business Continuity Measures – Regional Uncertainties", reminding all regulated entities of their ongoing obligations to maintain effective and operationally sound business continuity arrangements. The DFSA emphasised the need for Authorised Firms to remain adequately prepared to manage operational disruptions and to ensure continuity of critical business functions without material impact.

The DFSA also reiterated that Authorised Firms must promptly notify the regulator of any significant impacts on their operations, staff, customers, or financial condition. As part of this communication, all Firms, regardless of whether a previous business continuity plan ('BCP') notification had been submitted, were instructed to complete the Business Continuity Measures Form available on the DFSA ePortal.

On 24 March, the DFSA issued a direct communication to SEOs, SOs, MLROs, and Principal Representatives advising that all Firms are required to provide an updated assessment of their BCP arrangements by completing the Business Continuity Measures Form on the DFSA ePortal by 27 March 2026.

You can read the Dear SEO Letter in full here.

1.6 DIFC Issues Phishing Alert

On 25 March, the DIFC sent an email directly to firms operating within the Centre, warning them about a rise in phishing attempts impersonating the DIFC and its senior management. The email emphasised that cybercriminals were using increasingly sophisticated methods to make fraudulent communications appear legitimate. Firms were urged to exercise caution when receiving unsolicited messages claiming to originate from the DIFC.

The DIFC highlights several key precautions:
- verify the sender's email address carefully
- be alert to urgent or unusual requests, noting that the DIFC will never ask for sensitive information such as passwords, banking details, or OTPs
- avoid clicking on suspicious links or attachments
- treat any emails impersonating DIFC leadership with caution
- independently verify unexpected requests through official DIFC channels.

The DIFC stresses the importance of vigilance and encourages clients to report any suspected phishing or fraudulent emails to info@difc.ae.

1.7 DFSA Issues Dear SEO Letter on Liquidity Risk Management

On 26 March, the DFSA issued a Dear SEO Letter titled "Collective Investment Funds: Liquidity Risk Management, Redemption Pressures and Reporting." In the letter, the DFSA reminded fund managers of their ongoing obligations relating to liquidity risk management, monitoring of redemption pressures, and regulatory reporting.

The DFSA highlighted several key requirements for fund managers:
- robust, forward-looking liquidity risk management frameworks are in place
- the liquidity profile of fund assets remains aligned with the fund's objectives, strategy, and redemption terms
- liquidity assessments use realistic, dynamic assumptions that reflect current market conditions and exposure to less liquid assets
- firms understand their investor base, including concentration risks, and monitor redemption pressures under normal and stressed conditions
- regular liquidity stress testing is conducted using severe but plausible scenarios, with outcomes feeding directly into risk management and decision-making, supported by strong governance and escalation processes
- liquidity management tools (e.g., redemption gates) are operationally ready, fully disclosed in fund documentation, deployable in a timely manner, and assessed with regard to investor fairness and broader legal or structural considerations.

The DFSA also stressed that fund managers must promptly notify the DFSA of any material liquidity concerns, including significant or unexpected redemption requests, deterioration in asset liquidity, activation of liquidity management tools, or any situation where a fund may struggle to meet redemption requests. Where asset management activities are delegated, the fund manager remains responsible for ensuring the delegate provides all necessary information and support to meet DFSA reporting obligations.

You can read the Dear SEO Letter in full here.

1.8 DFSA Publishes Consultation Paper 170

On 27 March, the DFSA published Consultation Paper No. 170 "Operational Resilience", proposing new Rulebook requirements designed to embed the core components of an effective operational resilience framework. Under the proposals, Authorised Persons would be required to:
- identify their critical business services
- for each critical business service:
    - set appropriate impact tolerances
    - map the resources necessary for its delivery
    - conduct scenario testing to assess the ability to remain within impact tolerances
    - notify the DFSA of any material disruptions.

These measures aim to strengthen firms' ability to withstand, respond to, and recover from operational disruptions in a manner that minimises harm to clients, markets, and the DIFC's financial system.

You can read the Consultation Paper in full here. Comments are welcome until 26 May 2026.

1.9 DFSA Publishes Consultation Paper 171

On 27 March, the DFSA issued Consultation Paper No.171 "Miscellaneous Changes" seeking feedback on proposed amendments to the PIB module and the Conduct of Business ('COB') module.

The consultation paper proposes amendments to PIB Rules 3.8C.4 and 3.8C.5 to specify that a firm should refer to monthly values rather than daily metrics when calculating average assets safeguarded and administered ('ASA') and average capital requirement for assets under management ('AUM') respectively.

The amendments also propose removing the requirement for client money reconciliations to be performed on a trade settlement date basis. The regulator clarified that this requirement was intended for client investments and crypto tokens, but not for client money, which should instead be reconciled upon receipt of funds. COB Rule A5.11.1(3) and the associated guidance are therefore proposed for deletion.

You can read the Consultation Paper in full here. Comments are welcome until 27 April 2026.

1.10 DFSA Issues Dear SEO Letter on Cyber Threats

On 27 March, the DFSA issued Dear SEO Letter "Elevated Cyber Threat levels". In the Letter, the DFSA observed a recent increase in cyber-attacks targeting critical infrastructure, as well as hybrid operations directed at technology service providers across the region, in particular:

- threat actors conducting low-impact but persistent cyber operations, including Distributed Denial-of-Service ('DDoS') activity, privileged-user credential harvesting, and website defacements directed at financial institutions
- opportunistic exploitation of unmitigated vulnerabilities in internet-facing assets
- a surge in financial fraud, particularly e-mail and QR-code-based impersonation attacks affecting both organisations and their clients
- hybrid operations targeting regional cloud services infrastructure.

The DFSA reminded all Authorised Firms, Registered Auditors, DNFBPs, and Representative Offices to:

- maintain vigilant monitoring and conduct impact assessments within their operational environments. Intelligence indicates that low-level cyber incidents are increasingly amplified to align with broader geopolitical narratives
- notify the DFSA without delay of any material security incident, and no later than 72 hours after becoming aware of the event, using the Cyber Incident Notification form
- register with the DFSA Cyber Threat Intelligence Platform ('TIP') to receive and share timely cyber threat intelligence within the DIFC and the wider financial services community
- review their cyber risk management frameworks to ensure operational effectiveness
- prioritise risk mitigation efforts related to identity and access management controls and the security of internet-facing assets
- validate incident response processes through scenario-based exercises to ensure readiness for emerging threats.

You can read the Dear SEO Letter in full here.

1.11 DFSA Issues Multiple Fraud Alerts

Throughout March, the DFSA issued multiple fraud alerts in response to a noticeable rise in scams involving the misuse of the DFSA's name, brand, regulatory status, and official communications. The scams shared several recurring characteristics:

- impersonation of DFSA-authorised firms through similar-sounding names, cloned websites, and fraudulent claims of authorisation (e.g., Qalynomics, Qanotarytx, and "Amanah Capital")
- cloning of DFSA resources, including fake versions of the DFSA Public Register, to create a false appearance of legitimacy
- direct impersonation of the DFSA, including fake emails purporting to be from the DFSA's Finance Department, using unauthorised email addresses, fabricated contact details, and references to irrelevant foreign laws
- advance-fee and payment-request scams, where victims are instructed to transfer funds to unauthorised bank accounts and provide proof of payment
- misuse of DFSA contact information, including the regulator's address and fax number, without permission.

Across all alerts, the DFSA reinforced the same core messages:

- the entities involved are not authorised and have no connection to the DFSA or any legitimate DFSA-regulated firm
- individuals should not engage, not respond, and never send money in relation to these scams
- verification should always be conducted through the DFSA's official Public Register, Alerts page, and published guidance on common scam typologies.

You can read the DFSA alerts in full here.

Further information

If you have any questions or concerns regarding these DIFC and DFSA developments and requirements, please contact Nigel Pasea.

2. ADGM AND FSRA LATEST DEVELOPMENTS

2.1 FSRA Issues Cyber Risk Notice

On 2 March, the Financial Services Regulatory Authority ('FSRA') issued via an email Notice No. FSRA/FCCP/38/2026 to Senior Executive Officers and Principal Representatives, highlighting a heightened risk of cyber-attacks against the financial sector amid escalating geopolitical tensions. The UAE Cyber Security Council has raised the national cyber-threat level for financial services and banking to "High."

The FSRA urged all Relevant Persons to elevate their cybersecurity readiness to the highest level, with expectations covering both employee vigilance and strengthened technical controls.

Key expectations for Firms included a series of mandatory steps:

- employee awareness measures, such as heightened vigilance against phishing, strict adherence to MFA, prompt installation of system updates, and caution when handling sensitive information
- enhanced technical and procedural controls, including activation and testing of incident-response plans, 24/7 SOC monitoring, proactive threat hunting, updated EDR/IDS/IPS/SIEM systems, strengthened network segmentation, validated backup and recovery procedures, and tightened remote-access pathways

- reinforced email and access-control safeguards, including least-privilege configurations and hardening of external-facing services.

The FSRA also reiterated that any material cyber incident must be reported within 24 hours through the established IT and Cyber Incident reporting channels.

2.2 FSRA Issues Dear SEO Letter

On 2 March, the FSRA issued a communication to Senior Executive Officers ('SEOs'), confirming that the regulator remains fully operational and contactable, notwithstanding that some staff may be working remotely. The FSRA emphasised that supervisory activities continue on a business-as-usual basis, and firms are expected to maintain normal engagement with their supervisory contacts.

The FSRA reminded firms of their obligation to promptly notify the regulator of any material developments affecting operations, financial position, systems and controls, client servicing, or the ability to meet regulatory obligations. This includes the activation of contingency measures, changes to operational arrangements, such as remote-working models, and any other adjustments implemented or under consideration.

Firms were encouraged to assess the impact of current circumstances on their operations and ensure that appropriate governance and oversight remain in place. Any material issues, or issues reasonably expected to arise, must be reported to the FSRA without delay.

On 13 March, the FSRA issued further notice to SEOs requesting that they submit updates on their operational measures by 23 March.

2.3 FSRA Publishes Findings from Thematic Review on AML/CTF

On 5 March, the FSRA published a thematic review on Anti-Money Laundering, Counter-Financing of Terrorism and Proliferation Financing ('AML/CFT/TFS/CPF'). The purpose of the review was to assess the effectiveness of the systems and controls implemented by Authorised Persons and Recognised Bodies to ensure compliance with applicable AML/CFT/TFS/CPF obligations.

The thematic review focused on the following areas:

- customer onboarding, customer risk assessments, and ongoing customer due diligence
- systems and controls relating to terrorist financing and proliferation financing, including business-wide risk assessments
- transaction monitoring and the effective implementation of related processes and procedures
- the adequacy of suspicious activity and suspicious transaction reporting
- onboarding and ongoing due diligence of business partners.

To support the FSRA's initial analytical assessment of AML/CFT/TFS/CPF risks, all Authorised Persons and Recognised Bodies were required to complete a survey and submit their responses by 1 April 2026.

2.4 FSRA Issues Notice

On 6 March, following recent updates to the Financial Action Task Force ('FATF') lists, the FSRA issued a notice informing Regulated Firms of the National Anti-Money Laundering and Combatting Financing of Terrorism and Illegal Organisations Committee's ('National Committee') decision to adopt the FATF's list of high-risk jurisdictions. This includes the Blacklist (jurisdictions subject to a Call for Action) and the application of the corresponding countermeasures set out in the interpretive note to Recommendation 19.

The Notice also communicated the National Committee's decision to adopt the Gray List (jurisdictions under increased monitoring) and to require the implementation of enhanced due diligence measures by financial institutions, DNFBPs, VASPs, and NPOs. These measures must align with the interpretive note to Recommendation 10 and Article 4 of the 2019 Cabinet Decision (as amended), and be applied proportionately to the level of risk associated with each jurisdiction.

You can read the FSRA notice in full here.

2.5 FSRA Issues Dear SEO Letter on Operations and Contingency Measures

On 11 March, the FSRA issued via an email a Dear SEO Letter "Operations & Contingency Measures", to acknowledge that many Authorised Persons have already submitted the requested information on their current operational status in light of the ongoing regional circumstances. The FSRA emphasised that Firms that have already responded are required to keep the FSRA informed of any material developments or changes and must provide an updated submission by 23 March 2026, or earlier if circumstances change.

Authorised Persons that have not yet responded are instructed to submit their information as soon as possible, and no later than 16 March 2026, and to continue notifying the FSRA of any material updates thereafter.

The key operational and contingency measures are as follows:

- Firms are required to report any operational impacts affecting their ability to conduct business as usual. This includes notifying the regulator of
    - disruptions to key business functions or services, including any reduction in operational capacity
    - dependencies on critical third-party providers that may affect operational resilience
    - any other operational constraints that could impair normal business activities
    - activation of business continuity or contingency arrangements, including remote-working measures
- Where remote-working arrangements are in place, firms must also clarify:
    - the expected duration
    - whether arrangements apply within the UAE or abroad
    - any temporary staff relocation or evacuation
    - any additional measures implemented to support continued operations.

2.6 ADGM RA Publishes Findings from Thematic Review on NPOs

On 24 March, the Abu Dhabi Global Market Registration Authority ('ADGM RA') published the findings of a thematic review of the Non-Profit Organisation ('NPO') sector, covering all 43 NPOs registered in ADGM. The review assessed the sector's exposure to terrorist financing ('TF') risks and evaluated NPOs' compliance with ADGM's AML and Beneficial Ownership requirements.

The key findings of the review include:

- the sector is composed predominantly of professional membership organisations, with no charitable NPOs operating in ADGM
- 12 of the 43 NPOs maintain an international presence, although none operate in or remit funds to high-risk jurisdictions
- funding sources are limited to member contributions, UAE government support, and event sponsorships, with no public fundraising or cash-based activities
- governance structures vary, with 26% of NPOs having only a single governing body member, raising concerns regarding governance robustness

- all NPOs maintain policies and procedures governing the receipt and disbursement of funds, and none exhibited complex ownership structures.

Overall, the sector's terrorist financing risk was assessed as medium-low.

You can read the ADGM RA report in full here.

2.7 ADGM Issues FAQs on Workplace Health, Safety and Welfare

On 27 March, the ADGM Employment Affairs Office issued a set of FAQs on workplace continuity and workforce management to support ADGM employers and employees in maintaining effective operational arrangements.

The FAQs address key areas including workplace health and safety obligations, temporary workplace arrangements, workforce management measures, and wage-related requirements.

You can read FAQs in full here.

2.8 ADGM Celebrates 10th Anniversary

On 30 March, the ADGM marked its 10th year of operations, reporting continued growth and several strategic developments that contributed to its expanding role within Abu Dhabi's financial sector.

The key highlights include:

- AUM within ADGM increased by 36% in 2025
- the number of asset and fund managers rose to 171, collectively overseeing 244 funds
- ADGM issued 3,769 new licences in 2025, bringing the total number of active licences to 12,671
- The workforce grew by over 50%, reaching 44,339 individuals working within the financial centre.

You can read the ADGM announcement in full here.

Further information

If you have any questions or concerns regarding these ADGM and FSRA developments and requirements, please contact Shadi Dajani.

3. MIDDLE EAST REGULATORY UPDATES

3.1 VARA Releases a Circular

On 4 March, the Virtual Assets Regulatory Authority ('VARA') circulated a notice to all firms regulated or licensed by VARA regarding the issuance of Cabinet Resolution No. (134) of 2025. The Resolution concerns the Executive Regulations of Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Combating the Financing of Terrorism, and Proliferation Financing (the 'Executive Regulations').

VASPs are expected to implement all necessary updates without delay, in a manner proportionate to the nature, scale, and risk profile of their virtual asset activities. Where material gaps, deficiencies, or implementation

challenges are identified, VASPs must take timely remedial action and, where appropriate, engage proactively with VARA.

You can read the VARA notice here.

3.2 VARA Issues Several Warnings

On 5 March, VARA issued two separate Investor and Marketplace Alerts concerning unlicensed virtual asset activities being offered to Dubai residents.

The first alert related to Phoenixfin Pte Ltd, MEK Global Limited, Peken Global Limited, and Kucoin Exchange EU GmbH (operating as "Kucoin"), which VARA identified as potentially providing Virtual Asset ('VA') services in Dubai without the required approvals and misrepresenting their licensing status. VARA instructed these entities to cease and desist all unlicensed VA activities within the Emirate.

A second alert was issued the same day regarding MEXC Estonia OÜ and MEXC Global LTD (operating as "MEXC"), which VARA confirmed holds no licence to provide VA services in or from Dubai. VARA warned that any VA-related activities promoted or conducted by MEXC are in breach of VARA Regulations.

You can read the VARA warnings here.

3.3 CMA Issues Notice

On 9 March, the Capital Markets Authority ('CMA') issued an email notice to all licensed entities advising them of the National Committee's decision to adopt the latest FATF updates concerning high-risk jurisdictions subject to a call for action, as well as jurisdictions under increased monitoring.

Licensed entities were advised to review the updated FATF lists and take the necessary measures within their respective mandates, including updating their internal risk assessments, implementing enhanced due diligence and counter-measures where applicable, and ensuring full compliance with the applicable AML and Combating the Financing of Terrorism ('CFT') regulatory requirements.

3.4 FIU Releases Feedback Report

On 26 March, the Financial Intelligence Unit ('FIU') issued the H2-2025 Feedback Report to strengthen the quality, accuracy, and operational value of suspicious reporting across FIs, DNFBPs, and VASPs. The report is available via goAML portal and provides sector-specific insights, statistical trends, case studies, and strategic analysis to support national AML/CFT priorities.

During the reporting period, 62 banks received IEMS training, while 33 engagement sessions were conducted with Reporting Entities and supervisory authorities to reinforce compliance expectations. Additionally, 11 awareness sessions focused on proliferation financing red flags, STR/SAR reporting standards, and the FIU's operational role. A comprehensive goAML data clean-up exercise further improved entity classification and enhanced the accuracy of reporting across sectors.

The key observational insights from the report included:

- strategic analysis of misuse of VAs shows that fraud remains the dominant VA-related risk (including Ponzi schemes, romance scams, and task scams) as criminals increasingly rely on forged or AI-generated IDs, stolen cards, and mule accounts, alongside a continued rise in unlicensed VASPs and P2P brokers, a strong shift toward Tether ('USDT') on the Tron network, and more than 4,000 VA-related suspicious reports submitted since the 2021 AML/CFT framework expansion

- IEMS responses were generally timely and compliant, though VASPs must enhance the structure of their submissions by including wallet details, transaction hashes, and AED-equivalent values, while strong maker-checker controls and accurate documentation remain essential
- sector-specific issues
    - DNFBPs continue to show frequent errors in threshold reports, with some Reporting Entities incorrectly waiting for FIU instructions before acting, and all rejected reports required to be resubmitted through goAML
    - VASPs continue to submit reports with missing KYC/UBO information, weak analytical narratives, and insufficient blockchain evidence, all of which significantly reduce the analytical value of their submissions.

3.5 ECON Launches E-Learning Platform

On 27 March, the EOCN officially launched its new online e-learning platform, designed to strengthen national understanding and implementation of TFS and CPF.

This dedicated platform was developed following the recent consultation and training-needs survey, in which many stakeholders and clients participated. It aims to support compliance professionals across both the public and private sectors who are looking to deepen their knowledge of TFS and CPF within the UAE context.

Learners will have access to structured modules, interactive exercises, knowledge checks, and a final assessment. Upon successful completion, participants will receive an official certificate.

3.6 VARA Updates Exchange Services Rulebook

On 31 March, VARA updated the Exchange Services Rulebook by introducing Part V on Exchange Traded Derivative Services Rules.

Key updates include:

- only VASPs licensed by VARA to conduct Exchange Services may provide Exchange-Traded Derivative ('ETD') Services, and they must obtain VARA's prior approval before offering such services
- VASPs authorised to provide ETD Services must comply with all applicable requirements under Part V of the Exchange Services Rulebook
- the prohibition on VASPs investing their own or their group's portfolio of virtual assets or other assets is explicitly extended to investments in ETDs
- suitability assessments must be conducted for all clients to whom ETD Services will be provided ('ETD Clients')
- ETD Services must be fully segregated so that only ETD Clients can access or use such services
- all communications and disclosures relating to ETD Services or ETDs must be fair, clear, and not misleading, and must comply with VARA's Marketing Regulations
- enhanced content requirements are prescribed for ETD Services agreements
- detailed margin and leverage requirements are introduced for VASPs offering ETD Services, including stricter rules on initial and maintenance margin, permitted margin assets, differentiated leverage limits for retail and institutional investors, enhanced monitoring obligations, and VARA-approved margin valuation procedures
- VASPs providing ETD Services must maintain a properly valued, VARA-approved Insurance Fund, funded proportionately by the VASP and/or its clients, to cover negative equity risks, with limited exemptions available at VARA's discretion.
-

You can read the updated VARA regulations in full here.

3.7 CMA Publishes New Regulations

In March, the CMA published three new regulations, both of which are currently undergoing translation into English before formal release.

The new regulations include:

- Decision No. (4/Chairman) of 2026 on the Regulation of Virtual Asset Service Providers and Alternative Trading System Operators, comprising:
  - General Module
  - Business Regulation Module
  - Alternative Trading System Module
- Decision No. (7/Chairman) of 2026 on the Regulation of Margin Trading financed by the Dubai Financial Market via iVestor.

The CMA confirmed that the full decisions and supporting documents will be made available once the English translations are finalised.

You can read the CMA announcement in full here.

3.8 CMA Issues Several Warnings

Across March, the CMA issued a series of alerts warning investors about unlicensed entities conducting financial activities without its approval.

These include:

- HRG Investments LLC
- Soland Finance Consultancy LLC
- Skyline Technologies Trade LLC & Skyline Trading LLC and the website https://skylinetrading.com
- an unknown party that is falsely impersonating Soland Finance Consultancy LLC
- Hashim Al Fahmawi via the social media platform X (@hashim_fahmawi)
- Hypertech, represented by Sam Lee
- Rihani Crown Group, Winston Prime Limited and any associated platforms.

You can read the CMA warnings here.

Further information

For any questions or concerns regarding these updates, please contact Mohsin Ismail.

4. INTERNATIONAL UPDATES

4.1 FATF Publishes Report on Stablecoins and Unhosted Wallets

On 3 March, the FATF released a report outlining significant illicit finance risks arising from the criminal misuse of stablecoins, particularly through peer-to-peer ('P2P') transactions conducted via unhosted wallets. The report sets out recommended actions for both governments and the private sector to strengthen controls and safeguard the integrity of the financial system.

FATF notes that stablecoins have grown rapidly, with more than 250 in circulation by mid-2025 and a market capitalisation exceeding US$ 300Bn. According to market intelligence providers, stablecoins accounted for 84% of illicit virtual asset transaction volume in 2025, often involving unhosted wallets and sophisticated laundering techniques designed to obscure the origin of funds.

While stablecoins' liquidity, price stability, and interoperability support legitimate use, these same features make them attractive to money launderers, terrorist financiers, and state-linked cybercriminal groups. The report highlights misuse by DPRK-affiliated actors for laundering ransomware and phishing proceeds, and by Iranian networks for proliferation financing.

Key vulnerabilities include the ability to conduct P2P transfers via unhosted wallets without the involvement of a regulated intermediary, as well as challenges faced by stablecoin issuers in monitoring or controlling cross-chain activity, which may fall outside counter-illicit finance frameworks.

You can read the FATF report in full here.

4.2 Disarmament and Non-Proliferation Awareness Day

On 5 March, the international community marks the International Day for Disarmament and Non-Proliferation Awareness, an initiative aimed at strengthening public understanding, particularly among youth, of global disarmament priorities and the risks posed by weapons proliferation.

This day was established following the adoption of resolution A/RES/77/51 by the United Nations General Assembly ('UN'), with the date chosen to coincide with the entry into force of the Treaty on the Non-Proliferation of nuclear weapons.

You can read the UN article in full here.

4.3 UNSC Updates Sanctions List

In March, the UN Security Council ('UNSC') issued several updates to its sanction lists on 10, 26 and 30 March.

On 10 March, the UN Security Council Committee established under resolution 1988 (2011) approved amendments to entries on its 1988 Sanctions List. The updated listings apply to several individuals and entities subject to the assets freeze, travel ban, and arms embargo mandated under resolution 2816 (2026). The changes were made under the Council's Chapter VII authority.

On 26 March, the UN Security Council's ISIL (Da'esh) and Al-Qaida Sanctions Committee added one individual, Abd El Hamid Salim Ibrahim Brukan Al-Khatouni, to its sanctions list. The designation places him under an assets freeze, travel ban, and arms embargo under resolution 2734 (2024). According to the listing, he previously served as a senior financial management officer within ISIL. Updated narrative summaries and consolidated sanctions lists are available on the UN Security Council website.

On 30 March, the UN Security Council's ISIL (Da'esh) and Al-Qaida Sanctions Committee added one individual, Hamidah Nabagala, to its sanctions list. The designation subjects her to an assets freeze, travel ban, and arms embargo under resolution 2734 (2024). According to the listing, she is associated with ISIL financing activities in Central Africa and has been linked to a 2021 bombing in Kampala. Updated narrative summaries and consolidated sanctions lists are available on the UN Security Council website.

Further information can be found directly on the UNSC's website here, here, and here.

4.4 FATF Publishes Report on offshore VASPs

On 11 March, the FATF released a report highlighting significant risks arising from gaps in the oversight of offshore Virtual Asset Service Providers ('oVASPs'). FATF noted that these regulatory blind spots are being exploited to facilitate large-scale fraud, money laundering, and terrorism financing. The report outlines good practices for detecting, licensing or registering, supervising, and sanctioning non-compliant oVASPs.

The report explains how oVASPs, entities established in one jurisdiction but serving clients in another, structure their operations to avoid regulatory obligations, creating vulnerabilities that illicit actors exploit. FATF found that only 46% of jurisdictions apply an activity-based regulatory approach that captures offshore providers offering services into their markets.

Differences in national regulatory frameworks create opportunities for criminals to obscure illicit fund flows, including through dispersing victim funds across multiple wallets, layering transactions, and using multiple blockchains or bridges. The report also highlights cases where oVASPs have been used to launder proceeds from scam compounds, support terrorist financing, and misuse nested relationships to access licensed VASP services while unlicensed.

You can read the FATF report in full here.

4.5 MENAFATF Issues Statement

On 5 March, the Middle East and North Africa Financial Action Task Force ('MENAFATF') reaffirmed its commitment to working with member states and international partners to strengthen regional AML/CFT and counter-proliferation financing frameworks. The group highlighted ongoing efforts to enhance member countries' readiness for the next round of mutual evaluations and to support the effective implementation of international standards.

MENAFATF also emphasised the importance of international cooperation and coordinated regional action to address illicit financial flows, sanctions evasion, terrorist financing, and other financial crimes, noting that collective efforts are essential to improving financial transparency and supporting economic and security stability across the region.

You can read the MENAFATF statement in full here.

4.6 FATF Attends INTERPOL Global Fraud Summit

On 18 March, the FATF participated in the Global Fraud Summit hosted by INTERPOL and the UN Office on Drugs and Crime ('UNODC'). The discussions focused on the rapidly evolving global threat of fraud and collaborative strategies to strengthen international efforts to combat it.

You can read the FATF announcement here.

4.7 FATF Updates Consolidated Ratings

On 23 March, the FATF published an updated consolidated ratings table. The table summarises jurisdictions' progress against the 40 FATF recommendations. The recommendations assess the jurisdiction's maturity against money laundering, counter terrorist financing and proliferation financing measures.

You can read the consolidated FATF ratings here.

Further information

For any questions or concerns regarding these updates, please contact Mohsin Ismail.

ABOUT WAYSTONE COMPLIANCE SOLUTIONS

Waystone Compliance Solutions offers a new and unique approach to compliance services at a corporate level.

As a truly global partner, we have the capabilities to help you manage regulatory risk right across your organisation.

We can provide key services from initial registration and licensing to compliance programme integration. Our compliance solutions span business strategies, market activities, and operational and technology infrastructure, not to mention sales and marketing procedures. And we can do so anywhere in the world.

Our aim at Waystone is simple: to enable our clients to navigate the complex regulatory environment with confidence.

At Waystone, we have brought together the experience, the expertise, and the global reach to give you the certainty you need to address the ever-changing regulatory world. And by doing so, provide you with a secure route on the road to success.

https://compliance.waystone.com/

Consultancy Services & Support

- Compliance Advisory
  - The Virtual Compliance Clinic
  - Assurance Reviews
  - Compliance Remediation
  - Data Protection
  - Financial Crime Prevention

    - Corporate Governance
    - Risk Management
    - Prudential Rules & Regulatory Reporting
- Authorisation
- Outsourcing (Compliance Officer, MLRO, Finance Officer and Data Protection Officer)
- Documentation
- Training

If you wish to discuss how Waystone can assist you with any of the issues raised in this regulatory update, please contact us using the details below:

Email: compliancesolutions@waystone.com
Website: https://compliance.waystone.com/
Tel: Dubai +971 4 323 0800 | Abu Dhabi +971 2 440 2146
or write to us at:
Waystone Compliance Solutions
Level 2, Gate Village Building 7,
Dubai International Financial Centre (DIFC),
Dubai, PO Box 506733,
United Arab Emirates

This regulatory update provides information about the consultative documents and publications issued by various regulators which are still current, proposed changes to the Rules and Guidance set out in Handbooks, actual changes to Rules and Guidance that have occurred in the months leading up to the update and other matters of relevance to regulated firms. This regulatory update is intended to provide general summarised guidance only, and no action should be taken in reliance on it without specific reference to the regulators' document referred to therein.