waystone | Compliance Solutions

Regulatory Update

Middle East, August 2025

Issued 9 September 2025

Table of Contents

1. DIFC AND DFSA LATEST DEVELOPMENTS

1.1 DFSA Holds an Outreach Session

On 14 August, the Dubai Financial Services Authority ('DFSA') hosted a webinar focused on the 2025 Annual Anti-Money Laundering Return ('AML Return'). This regulatory reporting requirement is designed to evaluate firms' adherence to anti-money laundering obligations and to collect data that supports the DFSA's risk-based supervisory approach.

The session was particularly relevant for all authorized firms responsible for the preparation and submission of the AML Return.

Key topics covered included:
- how the DFSA utilises the AML Return to inform its supervisory activities
- outcomes of the DFSA's AML Return assurance review
- practical guidance and considerations for completing the 2025 AML Return.

The DFSA has published a Frequently Asked Questions ('FAQ') document on the annual AML Return, which provides additional guidance on how to complete the Return.

You can find the FAQ document here.

1.2 DIFC Academy Hosts Cyber Compliance Training

The Dubai International Financial Centre ('DIFC') Academy launched its Cyber Forward Programme 2025 (the 'Programme') in July, with initial sessions providing a broad overview of the initiative. In August, the Academy conducted four focused training sessions as part of the Programme. This initiative is designed to equip firms operating within DIFC with the tools and knowledge needed to navigate the rapidly evolving cyber threat landscape.

The key learning points from the session held on 1 August were as follows:
- identity management, authentication and access control
  - definitions and distinctions between authentication vs. authorisation
  - importance of least privilege and separation of duties
  - role-based access control ('RBAC'), multi-factor authentication ('MFA'), and identity proofing
  - asset-linked identity and adaptive access control
- platform security
  - configuration and patch management
  - secure software development lifecycle
  - prevention of unauthorised software execution
- data security
  - protection of data at rest, in transit, and in use
  - encryption, backup, and digital rights management
  - data classification and handling policies
- advanced concepts
  - zero trust architecture ('ZTNA')
  - identity and context-based access boundaries
  - restriction of lateral movement
  - comparison with legacy network security models
- artificial intelligence ('AI') in cybersecurity
  - use of machine learning for adaptive threat detection
  - emphasis on explainability and integration with existing control
- secure system design cheat sheet

    - covers authentication, encryption, vulnerability management, API security, container security, and disaster recovery.

Two sessions were also held on 15 August. Key highlights from both sessions are summarized below:

- technology infrastructure resilience
    - logical access control: segmentation, firewalls, zero trust architecture
    - environmental threat protection: fire, flood, temperature, humidity
    - equipment security: UPS systems, offsite handling, secure disposal
    - resilience mechanisms: redundancy, load balancing, failover infrastructure
- data backup and recovery
    - real-time and scheduled backups
    - offline and offsite storage with geographic separation
    - annual restore testing and incident-proofing strategies
- malicious code protection
    - entity-wide antivirus and malware scanning
    - mobile code usage restrictions and monitoring
    - recovery planning and awareness campaigns
- information exchange management
    - secure internal and external data exchange policies
    - email security: disclaimers, encryption, retention, and access controls
    - alignment with information security regulation ('ISR') controls for confidentiality and integrity
- security testing and threat intelligence
    - regular vulnerability assessments and code reviews
    - cyber threat advisories and awareness of emerging attack vectors
- cyber awareness and human risk
    - rise in phishing, smishing, and social engineering attacks
    - UAE-specific scam examples (buy now pay later fraud, fake police notices)
    - emphasis on training, simulation, and behavioural change
- training and education
    - personalised learning paths and adaptive modules
    - gamification, multi-channel simulations, and compliance alignment (General Data Protection Regulation, ISO 27001)
    - real-time phishing detection using generative AI
- vulnerability and exposure management
    - use automated tools to identify and prioritise vulnerabilities
    - exposure management goes beyond patching, it's about understanding what is visible to attackers
    - regular updates, access controls, and employee awareness are foundational
    - protecting data requires layered defences: encryption, segmentation, and endpoint hardening
- detection lag is dangerous
    - average breach detection time is more than 200 days
    - early detection drastically reduces financial and reputational damage
- continuous monitoring
    - real-time analytics and anomaly detection are essential
    - use security information and event management ('SIEM') tools to correlate events across systems
- threat intelligence integration
    - external threat feeds help anticipate attacker behaviour
    - internal telemetry must be mapped to known attack patterns
- cyber kill chain
    - breaks down attacker steps from reconnaissance to data exfiltration
    - helps defenders disrupt attacks early in the chain
- MITRE ATT&CK framework

    - adversarial tactics, techniques, and common knowledge ('ATT&CK')
    - maps adversary tactics and techniques to real-world behaviours
    - enables defenders to align detection capabilities with attacker methods
- case studies
    - each breach revealed gaps in detection, segmentation, or response
    - mapping incidents to MITRE techniques showed where defences failed
    - key lesson: effective detection is not solely a technical challenge, it requires strong organisational coordination, clear roles, and streamlined communication across teams
- incident response maturity
    - preparation → detection → containment → recovery → lessons learned
    - regular tabletop exercises and red teaming improve readiness.

The Programme is open to all individuals seeking to deepen their understanding of cybersecurity and stay informed on the latest strategies for achieving compliance in an increasingly complex digital environment.

Interested participants may register directly through the DIFC Academy's official website here.

1.3 DFSA Issues Several Scam Alerts

In August, the DFSA issued multiple public warnings about scams involving fraudulent licenses, cloned versions of the DFSA register, fake DFSA email addresses and letters, impersonation of Authorised Firms, and false claims of DFSA authorisation.

Consumers are urged by the DFSA to check its Public Register to verify which Firms and Individuals are officially licensed.

The full list of DFSA alerts is available 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 Publishes Amendments to Its Prudential Framework

On 20 August, the Financial Services Regulatory Authority ('FSRA') finalised key amendments to its prudential framework for Authorised Persons classified under categories 3B, 3C, and 4, as outlined in the Prudential – Investment, Insurance Intermediation and Banking Rulebook ('PRU'). These changes follow extensive industry consultation and feedback received on Consultation Paper No. 2 of 2025.

The updated framework introduces:
- revised capital requirements for category 4 firms
- updated reporting obligations for category 3B and 3C firms
- enhanced professional indemnity insurance ('PII') standards applicable across all three categories.

The amendments are effective immediately, with the exception of the new minimum PII cover standards, which will come into force on 1 January 2026.

To support implementation, the FSRA will issue a Dear SEO letter detailing the changes and their implications for regulatory reporting.

You can read the FSRA announcement in full here.

2.2 ADGM Announces Abu Dhabi Finance Week

On 1 August, the Abu Dhabi Global Market ('ADGM') unveiled plans for the fourth edition of Abu Dhabi Finance Week ('ADFW'), scheduled to take place from 8 to 11 December 2025. This year's theme, "Engineering the Capital Network," will delve into the evolving dynamics of global financial markets, spotlighting the structural forces and emerging realities shaping the industry.

ADFW 2025 aims to reinforce Abu Dhabi's position as a rising nexus in the international financial ecosystem, bringing together thought leaders, policymakers, and market participants to explore strategic opportunities and foster cross-border collaboration.

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 SCA Issues Draft Regulation for Virtual Assets

On 5 August, the Securities and Commodities Authority ('SCA') issued draft regulations governing virtual asset ('VA') activities. These include provisions for VA service providers, outlined in the General Module and Business Regulation Module, as well as regulations pertaining to alternative trading systems ('ATS').

Interested parties were invited to review the proposed regulations and submit their feedback or comments via email to consultation@sca.ae by the end of 1 September 2025.

3.2 CBUAE and Bank of South Sudan Sign MoU

On 13 August, the Central Bank of the UAE ('CBUAE') and the Bank of South Sudan signed a Memorandum of Understanding ('MoU') establishing a strategic cooperation framework across key financial infrastructure domains. The agreement aims to enhance collaboration in security printing, payment systems development, and technical capacity-building.

The key agreements under the MoU include:

- Oumolat, a subsidiary of the CBUAE, will provide innovative solutions for the security printing of banknotes in South Sudan
- Al Etihad Payments, also a subsidiary of the CBUAE, will support the development of a national payment card system in South Sudan through a two-phase implementation

  - phase one will involve the delivery of advanced switching and processing solutions for payment card transactions, aligned with global standards for efficiency, security, and data confidentiality
  - phase two will focus on infrastructure development to enable local processing of payment card transactions.

Furthermore, the MoU facilitates the exchange of knowledge and expertise, including technical support and training for Bank of South Sudan personnel in banking supervision and monetary operations. These programmes will be delivered through the Emirates Institute of Finance, further reinforcing institutional capacity and regulatory alignment.

This partnership reflects the UAE's commitment to fostering regional financial development and cross-border regulatory cooperation. Further updates will be provided as implementation progresses.

You can read the full CBUAE announcement here.

3.3 EOCN Holds Webinar on TFS for FIs, DNFBPs & VASPs

On 21 August, the Executive Office for Control and Non-Proliferation ('EOCN') hosted an online webinar for Financial Institutions ('FIs'), Designated Non-Financial Businesses and Professions ('DNFBPs'), and Virtual Asset Service Providers ('VASPs'). The session provided a comprehensive overview of the newly updated Targeted Financial Sanctions ('TFS') guidelines, with particular emphasis on the definition and scope of TFS, implementation procedures, and reporting obligations via the goAML platform. The guidance also included practical case studies illustrating how to apply and report TFS measures across various scenarios, including complex ownership and control structures.

The key highlights are as follows:

- reporting entities must have procedures in place to screen against sanctions lists and prevent any access or use of funds or assets on weekends and public holidays
  - however, if no business is conducted during the weekends or public holidays and customers cannot access accounts during this closure, screening must start from the first minute of reopening, with any required freezing measures applied immediately
- the funds freeze report ('FFR') has been renamed to the confirmed name match report ('CNMR')
- additional clarification has been provided for partial name match reports ('PNMRs')
- for existing customers, if the reporting entity, using the customer's ID, cannot determine whether it is a false match or confirmed positive, then they must immediately do the following:
  - suspend all activity, cease providing funds, assets, or services
  - file a PNMR via goAML within five business days, and maintain the suspension until instructed by EOCN to either cancel it (in case of a false positive) or freeze and file a CNMR (if confirmed)
- for potential customers or counterparties, reporting entities must make reasonable efforts to obtain ID documents to reach a conclusion
  - if a false positive is confirmed, reporting entities may establish the business relationship without the need to report a PNMR, but internal records must be kept
  - if IDs are unavailable within ten business days, reporting entities must reject the service and file a PNMR within five days of rejection, specifying that the relationship has been rejected due to lack of ID documents
  - if IDs arrive post-rejection, the reporting entity should rescreen the customer and treat it as a new case (confirmed match, false positive, partial name match)
  - where verification still remains inconclusive even with IDs, the reporting entity should suspend and file a PNMR within five business days of suspension.

The EOCN reiterated that individuals who fail to comply with the stated obligations may be subject to imprisonment and/or fines, while reporting entities may face regulatory actions including warning letters or license termination. Furthermore, the EOCN affirmed that any individual who, in good faith, freezes funds or assets or withholds financial services in compliance with the applicable legal framework shall be shielded from liability or legal claims resulting from such actions.

The updated EOCN guidance can be found here.

3.4 AMLCFT Supervisory Subcommittee Holds Virtual Outreach Sessions

On 26 and 28 August, the AML/CFT Supervisory Subcommittee hosted two awareness sessions as part of its ongoing commitment to supporting compliance professionals across the UAE. These sessions form part of a broader initiative running through August and September, aimed at enhancing institutional resilience against financial crime, proliferation financing, and terrorism financing. These sessions were specifically designed for Fis, VASPs, and DNFBPs, with a particular emphasis on entities regulated by the CBUAE.

The AML/CFT Supervisory Subcommittee is one of several specialised bodies operating under the UAE National Anti-Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organisations Committee ('NAMLCFTC'). Its primary role is to coordinate and enhance the supervisory efforts of various UAE authorities in implementing effective AML and CFT measures.

The key takeaways from the first two workshops include:

- proliferation and terrorism financing
    - essential components of a robust sanctions compliance program
    - applicable legal frameworks and regulatory obligations relevant to FIs, VASPs, and DNFBPs
- role-based AML/CFT/CPF training for licensed financial institutions
    - detailed walkthrough of best practices for implementing targeted AML/CFT/CPF training tailored to specific roles within an institution.

The upcoming September workshops will address the following focus areas:

- risk-based approach and institutional risk assessments
- transaction monitoring ('TM')
- risks related to proliferation finance ('PF').

3.5 SCA Updates Governance Framework for Public Joint Stock Companies

On 25 August, the SCA published the amendments to the resolution no. (3/Chairman) of 2020, specifically addressing the combination of roles between chairman of the board of directors and company manager (CEO or equivalent). Firms under the supervision of the SCA may wish to proactively review and update their internal governance manuals, policies, and board procedures to ensure alignment with the newly introduced regulatory amendments.

The key changes include:

- an introduction of a new article (7/bis "Controls for Combining the Positions of Chairman of the Board of Directors and Company Manager") establishing strict conditions under which a company may combine the roles of chairman and company manager
    - articles of association ('AoA') must explicitly allow the combination
    - board composition must ensure that at least 75% of its members are independent, reinforcing governance integrity and minimizing potential conflicts of interest
    - all members of permanent board committees must be independent

    - general assembly ('GA') approval must be obtained through a special resolution, supported by a detailed study justifying the role combination and its impact on board independence and oversight
    - GA's approval is valid only for the duration of the board's term
- governance committee ('GC') duties expanded
    - if the roles of chairman and company manager are combined, the GC must objectively evaluate the company manager's performance, annually assess the impact of the role combination on board independence, and recommend whether to renew or terminate the arrangement based on these evaluations
- chairman's recusal requirement
    - the chairman is required to step down from chairing and abstain from voting in board meetings when matters within the GC's scope are discussed, with the vice chairman assuming leadership of those sessions
- mandatory governance committee formation
    - if the chairman also serves as company manager, forming a GC becomes mandatory.

The resolution takes effect the day after publication in the official gazette.

You can read the SCA resolution in full here.

3.6 SCA Issues Several Warnings

On 4 August, the SCA issued a public warning against dealings with Ajman Tadawul (ajmantadawul.com), an entity that is not licensed or authorised to conduct regulated financial activities or provide related services under the SCA's supervision. The SCA stated that it assumes no responsibility for any transactions or engagements involving this company.

On 6 August, the SCA issued a public advisory urging individuals to refrain from engaging with an unlicensed company, FX GLOBE Marketing Management, that is not authorised to conduct regulated financial activities or offer related services under its supervision.

On 20 August, the SCA issued a public caution advising investors not to engage with Mr. Thoufeek Raja Abdul Majeeth, who is neither licensed nor authorised to conduct any activities subject to the SCA's supervision. The SCA clarified that it does not assume responsibility for any transactions or dealings involving Mr. Majeeth.

SCA urged market participants to exercise heightened vigilance when engaging with individuals or entities operating outside the regulatory perimeter. Investors are strongly advised to verify the licensing and regulatory status of any entity before entering into agreements or transferring funds, as a safeguard against potential fraud.

These notices highlight the critical importance of conducting thorough due diligence when dealing with financial service providers in the UAE.

Additional details on all public warnings issued by SCA are available here.

Further information

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

4. INTERNATIONAL UPDATES

4.1 Wolfsberg Group Publishes Statement on Monitoring Suspicious Activity

On 27 August, the Wolfsberg Group ('WG') released an updated statement introducing a broader framework for Monitoring Suspicious Activity ('MSA'), expanding beyond traditional transaction monitoring approaches.

This update builds on the initial statement released by the WG in 2024, which outlined how financial institutions can apply Wolfsberg principles (such as compliance with AML and CFT regulations, providing actionable intelligence to government agencies, and implementing risk-based controls) to develop an effective monitoring for suspicious activity programmes.

The updated statement emphasises a risk-based, technology-driven approach to detecting financial crime, with three core pillars:

- transition to a new MSA and validation
  - the objective for FIs is to move beyond replicating past performance, aiming instead to enhance efficiency, uncover emerging risks, and produce higher-quality intelligence for law enforcement
  - promotes the adoption of AI-driven systems to strengthen monitoring capabilities
  - emphasises validating the effectiveness of the new approach rather than benchmarking against legacy models
- balancing model risk vs. financial crime risk
  - model risk refers to the potential for adverse outcomes when a quantitative model produces inaccurate results or is applied inappropriately, impacting a financial institution's decision-making
  - in contrast, financial crime risk involves the misuse of a financial institution's products or services to facilitate illicit activities
  - financial institutions are encouraged to prioritise tangible, observable threats over hypothetical or theoretical risks
  - the approach supports responsible innovation while maintaining control over operational complexity
- explainability and transparency
  - FIs must be able to explain their MSA approach through three core lenses: risk coverage, model design and calibration, and model usage
  - calls for models that are interpretable to regulators and internal teams
  - unlike traditional systems that trigger alerts based on predefined rule thresholds, advanced models require a more nuanced understanding of outputs to support informed automated decision-making and investigative follow-up.

The Wolfsberg Group is an association of 12 global banks committed to developing frameworks and guidance for managing financial crime risks, particularly in areas like AML, CTF, and KYC practices.

You can view the full MSA statement here.

4.2 FATF Publishes NRA Toolkit

On 28 August, the Financial Action Task Force ('FATF') published a Money Laundering National Risk Assessment ('ML NRA') toolkit intended to support countries in developing and enhancing their risk-based approach to combating financial crime. The toolkit consists of three annexes which are not mandatory and should not be interpreted as a checklist or requirement, as FATF Standards do not prescribe a specific format for national risk assessments. Instead, the annexes are designed to complement the ML NRA Guidance by

providing illustrative examples and optional tools that jurisdictions may adopt based on their individual risk profiles and contextual needs.

Countries are encouraged to:
- use only the annexes relevant to their needs
- consult specific quick guides (e.g. on corruption) when appropriate
- treat suggested data sources as supplementary, not definitive
- ensure the NRA process remains manageable and accessible to both public and private sectors.

You can read the FATF announcement here and access the NRA toolkit here.

4.3 FATF Publishes Several Guides on Assessing ML Risks

On 28 August, the FATF published a series of guidance documents focused on assessing money laundering risks related to the informal economy, legal persons and arrangements, and virtual assets and virtual asset service providers.

Each guide offers practical insights for conducting these assessments, along with illustrative case studies that enhance understanding and application.

You can access the FATF guides in full here.

4.4 FATF Publishes Guidance on Risks of Corruption

On 28 August, the FATF published a quick guidance on assessing the money laundering risks of corruption.

The guidance provides several case studies and outlines the following key considerations for assessing money laundering risks associated with corruption:
- risk of corruption
  - review country-specific legal and regulatory frameworks
  - assess international threats and United Nations Convention Against Corruption ('UNCAC') related vulnerabilities
  - consider governance risks tied to natural resource wealth extraction
  - account for the size and influence of the informal economy
  - identify how corruption acts as a predicate or enabling factor
  - evaluate digitisation in procurement and public transparency tools
  - examine corruption across both public and private sectors
  - analyse risks of state capture and its impact on AML institutions
- risk of dealing with politically exposed persons ('PEPs')
  - identify PEPs (foreign and domestic)
  - examine the effectiveness of oversight of PEPs
  - examine PEP use of legal persons and arrangements
  - high-value transactions and unexplained wealth
- process and types of corruption
  - identify corruption-linked predicate offences (e.g., embezzlement, extortion)
  - map enablers and financial flows post-offence
  - review laundering typologies, especially those involving abuse of power
  - watch for red flags like unexplained PEP transactions and use of complex legal structures
  - assess all forms of corruption across sectors and populations, including state capture risks
  - prioritise analysis of grand corruption in public procurement and infrastructure projects

- foreign corruption
    - assess corruption risks in the wider region and among similar-risk countries
    - examine links between domestic corruption and exposure to foreign illicit proceeds
    - recognise that low domestic risk doesn't eliminate vulnerability to foreign corruption
    - monitor financial flows to/from high-risk jurisdictions and foreign PEPs.

You can read the FATF guidance in full here.

4.5 UNSC Updates Sanctions List

The United Nations Security Council ('UNSC') has made amendments to its sanctions list. As a UN member, the UAE is committed to enforcing UNSC resolutions, and all firms are required to report their involvement with sanctioned entities or individuals.

On 5 and 22 August, the UNSC updated its Consolidated Sanctions List, which includes individuals and entities subject to sanctions. The updates comprised the addition of one individual related to Iraq and revised details for five individuals listed under the ISIL (Da'esh) and Al-Qaida sanctions regime.

Further information can be found here and here.

Further information

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

5. ENFORCEMENT ACTIONS

5.1 CBUAE Imposes a Financial Sanction on an Exchange House

On 1 August, the CBUAE imposed a financial sanction of AED 10.7M on an exchange house, in accordance with Article (14) of Federal Decree Law No. (20) of 2018 concerning Anti-Money Laundering ('AML') and Combating the Financing of Terrorism and Illegal Organisations, including its amendments.

The enforcement action follows a regulatory examination which identified the exchange house's failure to comply with AML/CFT policies and procedures, as well as breaches of its sanctions obligations. These findings reflect significant shortcomings in the firm's compliance framework and internal controls.

CBUAE reiterated its commitment to maintaining the transparency, integrity, and resilience of the exchange house sector. Through its supervisory mandate, the CBUAE continues to ensure that all exchange houses, their owners, and staff operate in full alignment with UAE laws, regulations, and standards – safeguarding the broader financial ecosystem.

You can read the CBUAE notice in full here.

5.2 CBUAE Imposes a Financial Sanction on a Finance Company

On 6 August, the CBUAE imposed a financial sanction of AED 600,000 on a finance company, pursuant to Article (137) of Decretal Federal Law No. (14) of 2018 concerning the Central Bank and Organisation of Financial Institutions and Activities, including its amendments.

The sanction follows findings from a regulatory examination which revealed that the Finance Company had failed to comply with market conduct and consumer protection regulations and standards. These breaches reflect deficiencies in the firm's adherence to regulatory expectations regarding fair treatment of consumers and responsible market behaviour.

You can read the CBUAE notice in full here.

5.3 CBUAE Suspends the Licence of YAS Takaful PJSC

On 18 August 2025, the CBUAE announced the suspension of YAS Takaful PJSC's licence, in accordance with Article 33(2)(K) of Federal Decree Law No. (48) of 2023 Regulating Insurance Activities.

The enforcement action follows YAS Takaful PJSC's failure to comply with the regulatory framework governing insurance companies in the UAE. Despite the suspension, the firm remains liable for all rights and obligations arising from insurance contracts concluded prior to the effective date of the suspension.

CBUAE reaffirmed its commitment to upholding the integrity and stability of the insurance sector, ensuring that all insurers, their owners, and staff operate in full compliance with UAE laws, regulations, and supervisory standards.

You can read the CBUAE notice in full here.

5.4 VARA Fines a Virtual Asset Service Provider

On 18 August 2025, the Virtual Assets Regulatory Authority ('VARA') issued a Notice of Fines following enforcement action against Morpheus Software Technology FZE ('Morpheus (Fuze)'), a licensed virtual asset service provider.

Morpheus (Fuze) was granted its licence on 19 October 2023, authorising virtual asset market operations subject to specific conditions. However, a regulatory investigation launched in April 2025 uncovered multiple breaches, including:

- deficiencies in the firm's AML programme, governance, compliance, and internal controls
- intentional engagement in unlicensed virtual asset activity, in violation of licence terms
- failure to disclose material facts to VARA during supervisory review.

The financial penalty is accompanied by the appointment of a skilled person to oversee the execution of a remediation plan. Morpheus (Fuze) has accepted the findings and committed to corrective measures. The firm will remain under enhanced supervisory oversight to ensure full compliance and protect market integrity.

You can read the VARA notice in full here.

5.5 CBUAE Revokes Licence of Malik Exchange and Imposes Financial Sanctions

On 20 August, the CBUAE announced the revocation of Malik Exchange's licence, removal of its name from the official register, and imposition of a financial sanction totalling AED 2M. This action was taken pursuant to Article (14) of Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations, and its amendments.

The enforcement measures follow the outcome of a regulatory examination which identified serious violations and failures by Malik Exchange to comply with the AML/CFT framework and associated regulatory obligations. These breaches reflect systemic deficiencies in governance, risk management, and compliance oversight.

You can read the CBUAE notice in full here.

5.6 ADGM RA Imposes Financial Penalties on Half Moon

On 26 August, the ADGM Registration Authority ('RA') imposed financial penalties totalling US$ 37,500 against Half Moon Investments Limited ('HMIL') and its three directors for failing to file accounts and reports within the statutory deadline for the financial year ending 31 December 2023.

The penalties were issued as follows:

- US$ 7,500 – HMIL
- US$ 10,000 – Mr. Shaukat Murad
- US$ 10,000 – Mr. Zia Murad
- US$ 10,000 – Mr. Manuel Mateos.

Under ADGM regulations, directors of licensed entities are required to ensure timely submission of annual accounts and reports to the RA. The RA reiterated its expectation that firms and their directors maintain high standards of compliance and contribute to a culture of regulatory accountability.

This enforcement action aligns with the RA's broader commitment to international standards, including those set by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes ('GFTEI').

Firms operating within the ADGM are reminded to review their internal governance and filing protocols to avoid similar contraventions.

You can read the RA notice in full here.

5.7 FSRA Imposes Financial Penalty on Auditor

On 26 August, the FSRA took enforcement action against UHY James Chartered Accountants (the 'Firm') for multiple failures to comply with anti-money laundering obligations during the period from 1 February 2022 to 14 February 2024.

The Firm was issued a financial penalty of US$ 20,000 and was found to have:

- lacked adequate AML policies and procedures in line with regulatory and federal requirements
  - UBOs not identified and verified within 20 days post effecting transactions
  - no consideration to FATF's list of jurisdictions under increased monitoring to identify high risk countries
- failed to implement effective systems to screen customers and detect/report suspicious activity
  - numerous unresolved matches
  - positive matches disregarded without providing adequate justifications to explain the decision
- neglected to conduct proper business risk assessments related to TFS

    - AML business risk assessment failed to identify and assess the risks to which the firm was exposed in relation to TFS, PF and TF
- did not perform sufficient customer risk assessments before and during client relationships
    - subjective scoring methodology
    - usage of repetitive wording to describe different types of risks associated with multiple customers
    - lack of identification of PEPs
- inadequately carried out customer due diligence and enhanced due diligence where required
    - lack of certified true copies of documents for some customers
    - failure to identify source for funds ('SOF') and source of wealth ('SOW')
    - in some cases, no EDD undertaken on PEPs or high-risk customers
    - failure to identify UBOs
    - failure to conduct periodic reviews of customer information.

These deficiencies reflect a broader failure to meet AML/CFT compliance standards and have prompted regulatory intervention.

You can read the FSRA notice in full 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 1, Gate Village Building 1,
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.