By email

10 October 2025

To Senior Executive Officer (SEO) of FSRA Authorised Persons
Cc: Approved Persons

Dear SEO,

Thematic Review on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Overall Observations

Background

As part of its supervisory mandate to safeguard the integrity of the Abu Dhabi Global Market ("**ADGM**"), the Financial Services Regulatory Authority ("**FSRA**") continues to prioritise the enhancement of compliance with the Anti-Money Laundering ("**AML**"), Counter Financing of Terrorism ("**CFT**"), and Targeted Financial Sanctions ("**TFS**") frameworks across all financial services sectors.

To support this objective, the FSRA has undertaken a thematic review with a particular focus on Licensed Virtual Asset Service Providers (VASPs). The FSRA has identified this segment as an emerging area of risk due to the rapid pace of innovation in virtual asset activities, the evolving nature of related technologies and the heightened potential for misuse by illicit actors. The UAE National Risk Assessment together with international standard setting bodies, such as the Financial Action Task Force, has outlined the inherent risks in the virtual asset sector, highlighting the importance of effective regulatory oversight and robust risk mitigation measures.

The thematic review forms part of the FSRA's broader supervisory strategy to ensure that ADGM licensed entities are equipped to manage emerging financial crime risks. In particular, it reflects the FSRA's commitment to maintaining a well-regulated, transparent, and trusted environment for the conduct of virtual asset activities.

This letter presents the key findings, sector-wide themes, and regulatory expectations arising from the review. The findings are intended to guide VASPs in strengthening their AML/CFT frameworks, addressing identified gaps, and enhancing alignment with both regulatory standards and global good practices

Scope

The thematic review was designed to provide a comprehensive assessment of Licensed VASPs operating within ADGM with a focus on assessing the adequacy and effectiveness of their AML, CFT, and TFS frameworks. In order to form a clear understanding of how firms are applying regulatory requirements in practice, the FSRA considered the range of activity types, operational models, and risk exposures represented across the sector. This approach allowed the FSRA to gain a holistic understanding of the maturity of compliance frameworks within the VASP sector and assess its readiness to address evolving financial crime risks within different business models.

The review focused on four key areas of compliance:

- **Customer Onboarding and Due Diligence (CDD):** Evaluation of the adequacy of firms' onboarding processes, including client identification and verification, risk profiling, and the

application of enhanced due diligence measures for higher-risk relationships. The review also considered the role of governance, documentation, and technology in supporting CDD practices.

- **Transaction Monitoring**: Assessment of monitoring frameworks to determine whether firms are equipped to identify and escalate suspicious or unusual transactions in a timely and effective manner. This included consideration of the use of automated monitoring systems, calibration of thresholds, quality of generated alerts and investigation processes.
- **Targeted Financial Sanctions**: Review of controls designed to ensure compliance with UAE sanctions obligations. The assessment focused on the adequacy of screening tools, frequency of sanctions list updates, governance around managing potential matches, and the oversight provided by senior management.
- **Wire Transfers and Travel Rule Compliance:** Examination of measures implemented to ensure adherence to the Travel Rule and mitigate risks associated with cross-border transfers. This included assessing VASPs' ability to capture, transmit, and verify the required information, as well as their controls for identifying and addressing potential compliance gaps.

Approach adopted:

The thematic review was conducted using a structured risk-based methodology to assess the implementation and effectiveness of AML, CFT, and TFS frameworks across Licensed VASPs. The methodology was designed to ensure a comprehensive assessment while allowing supervisory attention to be directed toward areas of higher potential risk.

The approach is comprised of three main stages:

1. **Data Collection:**

All VASPs were requested to complete a detailed survey capturing information on their business models, governance arrangements, client base, and transaction activity. The survey included both quantitative and qualitative questions to provide FSRA with the necessary data to assess the maturity of internal controls and identify potential areas requiring further examination. This stage provided a foundation for analysing practices across the sector and informed subsequent risk-based decisions.

2. **Risk Analysis and VASP Selection:**

Data collected from the surveys was systematically analysed to identify VASPs that might have higher exposure to AML, CFT, or TFS risks depending on their business model. The analysis considered multiple factors, including operational complexity, product and service offerings, transaction volumes, and the geographic footprint of business activities. VASPs demonstrating potential operational vulnerabilities were selected for focused on-site assessment, ensuring that supervisory efforts were proportionately allocated to areas of greatest significance.

3. **On-Site Assessment:**

Selected VASPs were assessed on-site to examine the design, implementation, and effectiveness of their AML, CFT, and TFS frameworks. These assessments involved:

- Framework Evaluation: The adequacy of policies and procedures, including governance structures and management oversight.
- Operational Implementation: How policies and procedures were applied in practice, including resource allocation, staff awareness, and monitoring of compliance with internal controls.
- Systems and Controls: The effectiveness of technological solutions, reporting mechanisms, and internal controls in detecting, assessing, and mitigating risks.

Key Findings

The FSRA's thematic review of VASPs found that while firms generally demonstrate awareness of their AML/CFT obligations, there remain some weaknesses in the way these obligations are executed in practice. In particular, deficiencies were observed in the consistency and depth of customer due diligence, the strength of transaction monitoring systems, alignment with the Travel Rule and the overall application of risk-based frameworks. These gaps limit the sector's ability to identify, assess, and mitigate financial crime risks in line with regulatory expectations.

The review also noted insufficient independent assurance with some firms failing to subject their controls to internal or external review. In parallel, weaknesses were observed in counterparty due diligence and limited tailoring of training programs to staff roles and risk exposure.

Overall, the findings underline the importance of VASPs moving beyond high-level awareness and written procedures to demonstrate that AML/CFT frameworks are being applied in a consistent, well-documented, and risk-sensitive manner. By doing so, VASPs will be better placed to maintain regulatory compliance, safeguard market integrity, and respond effectively to the evolving financial crime risk environment. Addressing these gaps will be important for ensuring that AML/CFT frameworks are applied consistently, tested effectively, and capable of keeping pace with the risks inherent in virtual asset activities.

A detailed breakdown of the thematic findings along with corresponding regulatory expectations is provided in the Appendix to support firms in addressing these gaps and strengthening their AML/CFT frameworks.

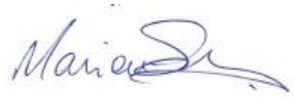
Next Steps

The FSRA expects VASPs to assess their current frameworks against the review findings and implement enhancements to meet the respective compliance expectations. Consistent and effective financial crime

controls are essential for sustaining a secure business environment and senior management is expected to play an active role in driving these improvements across all levels of the firm. Where concerns in relation to specific VASPs have been identified, these will be addressed directly with the firm concerned.

In case of any queries, please do not hesitate to contact the FSRA Supervision team.

Yours Sincerely,



Mary Anne Scicluna
Senior Executive Director - Supervision
Financial Services Regulatory Authority

Appendix 1

Overall observations and Themes	
Client onboarding and Customer Due Diligence (CDD)	**Observations:** The review identified specific deficiencies in how VASPs applied customer due diligence requirements, particularly in relation to enhanced due diligence ("**EDD**"). Few VASPs demonstrated weaknesses in verifying source of funds ("**SoF**") and source of wealth ("**SoW**"). In some cases, the necessary documentation was not collected at the time of onboarding. In other cases, firms relied primarily on client self-declarations without obtaining independent or reliable corroborating evidence, reducing the credibility of the information collected. These shortcomings are particularly concerning in higher-risk relationships, where a more robust standard of evidence is required. Further gaps were identified in the application of EDD for high-risk clients. In some instances, EDD measures were applied in a limited manner without the level of enquiry needed to mitigate the increased risks. In other cases, VASPs did not document the steps undertaken or the rationale behind their decisions and obtain senior management approval before onboarding high-risk client relationships. This lack of traceability and oversight weakens the effectiveness of AML/CFT frameworks.

	In very limited cases, VASPs did not obtain residential address verification documents during the onboarding process. Although not widespread, this gap highlight weaknesses in internal controls and creates the risk of incomplete client records which may impair VASPs' ability to monitor and manage client risks effectively on an ongoing basis. **Regulatory Expectations:** FSRA expects firms to ensure that CDD and EDD frameworks are comprehensive, consistently applied and fully documented. This includes: • Assessing SoF using reliable and independent sources of evidence to confirm the origin of the specific funds used in a transaction or business relationship, rather than relying only on self-declarations. • verifying SoW using reliable and independent sources of evidence to understand the customer's overall financial background and how their wealth was accumulated, rather than relying only on self-declarations. • applying EDD measures in all high-risk cases, including documenting the steps taken. • treating residential address verification as a mandatory component of the onboarding process. • ensuring senior management approval is obtained and recorded before onboarding high-risk clients. • periodically reviewing CDD policies and practices to ensure they remain effective and aligned with evolving risks and regulatory requirements.
Transaction Monitoring	**Observations:** The review identified few deficiencies in the design and operation of transaction monitoring systems used by VASPs. In few cases, scenarios and thresholds were simplistic or not aligned with typologies specific to virtual assets. Furthermore, transaction monitoring programs were often focused primarily on on-chain transactions with limited or no functionality to capture broader client behaviour, such as unusual activity patterns, complex or large transactions, and transactions not consistent with the client profile. These weaknesses increase the risk that unusual or suspicious activity may not be detected, escalated, or reported in a timely manner. **Regulatory Expectations:** FSRA expects firms to design and maintain transaction monitoring frameworks that are proportionate to the scale, complexity, and risk profile of their operations. At a minimum, firms must: • Implement on-chain and behavioral transaction monitoring scenarios that are calibrated to risks relevant to virtual assets. These scenarios should be designed to detect activity inconsistent with the firm's knowledge of the client, their business, and risk rating. Firms should periodically test and optimise thresholds to ensure effectiveness of these controls.

	• integrate behavioural monitoring alongside on-chain analysis to capture unusually large, or atypical patterns of client activity across products, services, and jurisdictions that may lack an apparent economic or legitimate purpose • ensure that Transaction Monitoring scenarios integrate risk sensitive thresholds allowing to capture key characteristics of clients in terms of wealth, expected transaction volumes and patterns, residence and business location, etc. • establish clear, documented protocols for escalation, investigation, closure, and reporting of suspicious activity. • subject transaction monitoring frameworks to regular governance oversight and independent assurance to ensure ongoing effectiveness and alignment with risks.
Risk-Based Approach	**Observations:** We noted shortcomings in how some VASPs designed and applied their risk-based frameworks. For example, a small number of Business Risk Assessments (BRAs) were generic with limited analysis specific to the risks associated with virtual asset activities. In certain instances, BRAs did not address important risk factors and lacked a clear methodology or meaningful link to the firm's AML/CFT controls. Without a detailed assessment, BRAs cannot effectively guide the allocation of resources, the prioritisation of controls, or the overall design of the compliance program. Customer Risk Assessments (CRAs) showed similar weaknesses. During our review, we have noted that some methodologies were not adequately documented, leading to inconsistent application across the client base. In addition, limited number of CRAs did not include key factors such as the customer's business purpose or the type of products and services being used. These gaps reduce the accuracy of customer risk ratings and increase the likelihood that higher-risk clients are classified as low risk, which undermines the effectiveness of AML/CFT controls. **Regulatory Expectations**: FSRA expects VASPs to strengthen their risk-based frameworks to ensure that both BRAs and CRAs are reliable, comprehensive, and capable of supporting proportionate AML/CFT measures. Specifically, VASPs are Should: • developing robust, well-documented BRAs that capture all relevant financial crime risks outlined in the AML Rulebook, including those unique to virtual asset activities, products, services, and jurisdictions. • implementing structured CRAs based on documented methodology and consistently applied criteria that accurately reflect the customer's overall risk profile. • Review and update BRAs and CRAs regularly and whenever material changes occur.

Travel Rule Compliance	**Observations:** While there is general awareness of the Travel Rule's requirements, practical implementation remains a challenge, specifically in scenarios where FSRA VASPs act as a beneficiary VASP. A number of firms highlighted operational and technical barriers to compliance, including the "sunrise issue" where counterparties in other jurisdictions have not yet implemented the Travel Rule in full. In addition, all VASPs had established internal policies and procedures to support compliance. However, these frameworks were often limited in scope and lacked sufficient detail to ensure effective application. In particular, a number of VASPs did not have adequate processes in place to manage instances where counterparties are unable to comply with the Travel Rule. This included an absence of defined protocols for identifying, reviewing, and taking appropriate action on non-compliant transactions. The review also noted that few VASPs had not conducted any internal audit or independent assessment to evaluate the effectiveness of their Travel Rule compliance frameworks. Without such independent assurance, weaknesses in internal controls may go undetected and increase the risk of non-compliance with regulatory requirements. Finally, few examples were observed where firms applied de minimis thresholds to cross-border virtual asset transfers which are not in compliance with the FSRA AML Rulebook requirements. **FSRA Expectations** We understand that the sunrise issue might cause difficulties in complying with Travel Rule requirements, specifically for cross-border virtual assets transfers. Nevertheless, FSRA licensed VASPs are expected to fully comply with the AML Rulebook requirements. In practice, this means: • Apply Travel Rule obligations to all qualifying transfers with no de minimis thresholds permitted in line with FSRA AML Rules. • For Virtual Assets transfers, ensure that all required originator and beneficiary data is obtained and transmitted as outlined in AML Rule 10.3.2 This includes collecting, verifying, and retaining the required data elements prior to initiating or accepting a transfer, and ensuring that such information remains with the transfer throughout the payment chain. Firms must also monitor for incomplete transfers and take appropriate measures to address any associated ML/TF risks • Where required information is missing or non-compliant, establish clear protocols to review the completeness of information received, and define when to process, suspend, or reject transactions. The protocols could consider risk-based approach to assess whether

	to proceed with the transaction taken into account relevant risk factors such as jurisdictional status and risk exposure. • Conduct due diligence on counterparty VASPs' ability to comply with the Travel Rule, including documented escalation policies when compliance is not possible. • Retain a full record of data collection, transfer decisions, and escalation actions for at least five years. • Regularly test Travel Rule systems and processes to ensure results and exceptions are reported to senior management or Board for oversight. • Conduct periodic independent reviews to assess the effectiveness of their Travel Rule compliance framework.
Counterparty VASPs	**Observations:** The review identified weaknesses in the approach some VASPs taken when engaging with counterparty VASPs. The main concern was that several VASPs entered into business relationships or executed transactions without carrying out any form of risk assessment or due diligence on their counterparties. In these situations, VASPs did not evaluate whether the counterparty had appropriate AML/CFT systems and controls in place, nor did they assess jurisdictional or operational risks associated with the relationship. This lack of structured assessment exposes firms to financial crime risks, particularly where counterparties operate in higher-risk jurisdictions or have weaker AML,CFT and TFS frameworks. **Regulatory Expectations:** VASPs are expected to develop and implement comprehensive frameworks for counterparty due diligence and monitoring. This includes: • risk assessments prior to establishing relationships. • documented criteria for ongoing monitoring. • escalation procedures for dealing with non-compliant counterparties. • clear refusal or termination policy. • maintaining evidence of all assessments and decisions for supervisory review.
Treatment of unhosted Wallets	**Observations:** During our review, we have noted that almost all VASPs operating in the ADGM accepted transactions from unhosted wallets (self-hosted). By their nature, unhosted wallets make it difficult to obtain reliable originator and beneficiary information, creating gaps in transparency and limiting VASPs' ability to identify and assess financial crime risks. While several VASPs have documented approaches for managing these transactions, the measures observed were generally insufficient to address the inherent risks or to ensure alignment with FATF guidance and international best practices. This creates increased exposure to misuse of virtual assets through anonymous transactions.

	Regulatory Expectations: Although there are currently no specific obligations relating to unhosted wallets, VASPs are expected to adopt a documented, risk-based approach to their treatment. At a minimum, this should include: • Establishing clear policies and risk appetite thresholds that define when and under what conditions unhosted-wallet transfers will be permitted. • Collecting and retaining sufficient originator and beneficiary information to ensure traceability. This should include obtaining the necessary details directly from the customer before processing a transfer supplemented by verification methods such as the Satoshi Test. • Applying enhanced monitoring and due diligence measures to unhosted-wallet activity when necessary, including the use of blockchain analytics to identify unusual or high-risk patterns. • Documenting procedures for suspending, rejecting, or escalating transactions where information cannot be obtained or verified. • Maintaining strong governance and oversight, including regular reporting to senior management and periodic testing of controls to confirm their effectiveness.
Training and Awareness	**Observations:** The review found that AML/CFT training programs across VASPs were often generic and not tailored to staff roles and responsibilities. In many cases, refresher training was rarely conducted and there was limited evidence of effectiveness testing to confirm whether employees had properly understood the training provided. As a result, knowledge of VASPs specific risks and regulatory requirements varied widely among staff, reducing the consistency and reliability of AML/CFT controls. **Regulatory Expectations:** FSRA expects VASPs to establish structured AML/CFT training programs that are role-specific, risk-based, and designed to promote compliance awareness across the organisation. VASPs should develop training programs and include the following: • tailor training content to reflect staff responsibilities, including front-line, operations, compliance, and senior management. • provide training on a regular basis with mandatory refresher sessions. • include effectiveness testing such as assessments, scenario-based exercises, or knowledge checks to confirm understanding • ensure coverage of regulatory requirements, internal policies, procedures, and sector specific risks relevant to virtual assets • maintain comprehensive training records, including attendance, completion and test results.