

By email

26 August 2022

To Senior Executive Officers (**SEO**) of FSRA Authorised Firms

Cc: Recognised Functions

Dear SEO,

FSRA's Thematic Review on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT), and Targeted Financial Sanctions (TFS) ("Review") – Findings and Outcomes

Background

Following FSRA's letter sent to all Authorised Persons on 26 April 2022 the FSRA has completed its Review and herein this letter sets out the Findings and Outcomes. The purpose of the review was to evaluate the effectiveness of the firms' AML/CFT and TFS policies, procedures, systems and controls to ensure compliance with ADGM Regulations and Rules, along with the relevant UAE Federal Legislations.

Scope

The Review included over 145 Authorised Persons (AP's) across a broad spectrum of financial services activities and business models. The scope intended to cover the following key areas:

- a) Governance and oversight over AML/CFT and TFS risks.
- b) Internal controls put in place by Authorised Persons to ensure compliance with the requirements in FSRA's AML Rulebook, Cabinet Resolution No.10 of 2019, Cabinet Resolution No.24 of 2022 and Cabinet Resolution No. 74 of 2020.
- c) Policies and procedures governing AML transaction monitoring and TFS.
- d) Policies and procedures in place for the purposes of compiling and reporting on suspicious activities and suspicious transactions; and
- e) The practical execution of a robust risk-based framework of the Authorised Firms in this regard.



Approach adopted

The Review was conducted in the following manner:

1. The first stage included an industry wide survey, circulated to all AP's, focused on the quantitative assessment of the authorised population in terms of client numbers, client profile, nature of client risk exposure, volumes of business and geographic coverage.
2. A second survey was issued in line with the National Action Plan focused on obtaining details relating to Transaction Monitoring and related systems and controls.
3. The third survey was issued in line with the National Action Plan focused on Terrorist and Financing sanctions and related systems and controls.
4. The fourth stage of the Review included a selection of a sample of firms to conduct an onsite focused thematic review covering the practical execution of the systems and controls surrounding the areas covered above. This included interviews with management, a walkthrough of key systems and process, and a sample review of relevant files.

The responses to the surveys were assessed by the FSRA to identify any outlying trends or patterns that might suggest good and bad practices across the APs. As part of the fourth stage a more detailed review was conducted to assess practical execution of the AML and TFS frameworks across a selection of firms. This letter sets out the high-level observations and findings identified as a result of the thematic review.

Key Findings

Financial Crime compliance is a critical element of the FSRA and the wider UAE supervisory mandate. We appreciate that the size, scale, and complexity of APs differs from firm to firm, however we expect the highest of standards to be maintained when considering appropriate policies, procedures, systems, or controls in place to fully demonstrate compliance with FSRA's, and UAE, relevant requirements.

Overall, the thematic review has identified that most AP's have in place elements to broadly comply with the FSRA framework requirements. However, there are several areas where firms did not have sufficient depth, governance and adequate policies, procedures, systems, or controls in place to fully demonstrate compliance with FSRA's relevant requirements. What was particularly evident was that while many firms have systems and controls in place, they have not developed in terms of depth and coverage as the AP's business increased in volume and complexity.

As a result, several findings were identified during the review for further improvement. The FSRA would also like to reiterate the obligations on the Boards and senior management to dedicate sufficient resources and oversight of these areas.

Specifically, we have noted observations in the following areas:

- 1) Policies and Procedures
- 2) Risk Based Approach
- 3) Internal Controls
- 4) Suspicious activity reporting
- 5) Training and awareness
- 6) Record keeping



Next steps

APs are expected to carefully review the findings and recommendations outlined in this letter to enhance their practices and align them with FSRA's requirements. FSRA will continue to monitor firms' practices in this area and as part of its supervisory cycle will review the steps taken by selected firms to review and address any identified areas for improvement. When conducting their AML and TFS gap analysis APs are expected to take the observations of this letter into account and document their findings.

Where specific concerns have been identified for specific AP's, these will be addressed directly with the appropriate findings.

To assist you we have attached Appendix A which provides a list of good practices and areas for improvement noted during the review.

Yours Sincerely,

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



Appendix A

1) Policies and Procedures

Findings

Good practices

- Comprehensive AML/CFT and TFS policies and procedures based on a gap assessment conducted against FSRA AML/TFS requirements and Federal legislation.
- Adequate policies and procedures that cover the relevant topic related to AML/CFT and TFS, such as governance oversight, risk-based approach, customer on-boarding, ongoing due diligence, transaction monitoring and sanctions screening controls, training and awareness and recording keeping.
- With respect to branches, policies and procedures addendums have been developed to reflect FSRA AML/TFS requirements and Federal legislation.

Areas for improvement

- High level policies and procedures that outline FSRA AML/TFS requirements and Federal legislation rather than describing internal practices and procedures in detail.
- Lack of defined approach in relation to terminating an existing client relationship. There is a lack of governance and processes relating to reviewing the overall customer relationship and notifying law enforcement and/or other group affiliates.
- Policies and procedures are not reviewed and updated on a periodic basis.
- The absence of independent review by either internal audit or external auditors to assess the effectiveness of policies and procedures.

2) Risk Based Approach

Findings

Good practices

- Comprehensive AML and sanctions risk assessment methodology defining the factors considered in risk assessment as well as the processes involved in evaluating these factors.
- Majority of the APs have documented the factors considered during the AML/CFT risk assessment as in line with FSRA AM
- L/TFS requirements and Federal legislation.
- Most of the APs have identified at a high level their TFS risks depending on the nature and size of business.

Areas for improvement



- In one instance, an AP had not conducted the annual AML and sanctions risk assessment to identify key AML and TFS risks.
- Inadequate and high-level AML and TFS risk assessment.
- Lack of consideration of the findings of the National Risk Assessments when conducting the AML and TFS risk assessment.
- Unclear customer risk rating methodology that lacks consideration of certain key factors, such as product being used and customer information.
- No separate Terrorist Financing and Proliferation Financing risk assessments conducted by majority of APs. These risks are covered at a high level in the AP's AML Business Risk Assessment.

3) Internal Controls

Findings (Transaction Monitoring)

Good practices

- All firms have successfully registered in the goAML system.
- Application of risk-based approach to transaction monitoring by assignment of a risk rating to each alert generated by the transaction monitoring system.
- Transaction monitoring scenarios are clearly documented, reviewed and updated regularly.
- IP login address is considered as part of the transaction monitoring system to identify customers logging in from high-risk jurisdictions.

Areas for improvement

- Standard scenarios and standard thresholds are applied across the entire client portfolio, without having specific thresholds (lower/higher limits) or specific scenarios to demonstrate enhanced monitoring of high-risk clients.
- Limited ability to identify related parties or customers connected to one another.
- Limited number of firms in the asset management and custodian sectors have the view that some obligations related to the attainment of further information on high-risk customers do not apply to them since these activities are being conducted via the fund or executed by the Clients' Bank. All firms in the regulated community have a responsibility to investigate and report on any suspicious activities related to their activity, regardless of the legal entities involved.
- Inadequate assessment and tuning of Transaction Monitoring system parameters.
- Over-reliance on manual reviews of all transactions, which raises a risk of ensuring consistency and scalability as payment volumes increase

Findings (Sanctions Screening)



Good practices

- Firms have registered on the Executive Office of Control and Non-Proliferation website.
- Sanctions screening systems and controls are reviewed periodically by the compliance function.
- All the APs do sanctions screening prior to onboarding a client and while doing the KYC reviews or effecting changes to customer's information.

Areas for improvement

- Inadequate assessment and tuning of sanctions screening system.
- High level sanction screening procedures which do not take into account the process of screening after receiving a new designation from Executive Office of Control and Non-proliferation.
- Insufficient understanding of the capabilities and configurations of off-the-shelf sanctions screening systems.

4) Suspicious activity reporting

Findings

Good practices

- Generally, records of internal SAR/STR are appropriate and provide sufficient details in relation to the customer and underlying suspicions.
- External SAR/STRs are complete, sufficient, and timely filed in the goAML system.
- APs have adopted a maker and checker process/concept to verify the adequacy of the internal suspicion raised.

Areas for improvement

- Senior management should not influence any decisions made by the MLRO regarding SAR/STR.
- Approach to Suspicious Activity reporting is too high-level and is not adequately articulated in the AML Policy/manual and does not cover the roles and responsibilities of the individuals involved in the SAR process, description of the internal SAR process and description of the SAR investigation process and reports.
- Insufficient guidance and consideration of red flags to raise in an internal SAR/STR report.

5) Training and Awareness



Findings

Good practices

- Training covers the core risk elements and guidance to staff on identifying suspicious activity considering the means of delivery, the customer risks, geographical risk, and any risk derived from the change of circumstances.
- Training programs delivered across a variety of training methods, including induction training courses for new joiners, mandatory classroom courses, role specific training courses and e-Learning for all employees, including AML staff.

Areas for improvement

- Training material is too high-level and does not sufficiently focus on the relevant activities of the firm, including relevant FSRA and cabinet resolution AML requirements specific to the firms' business operations.
- Training material does not take into consideration regulatory developments and changes in relation to AML & CFT landscape.
- Competence and training needs are not regularly reviewed to ensure staff are kept abreast with changes in the regulatory AML/CFT obligations.
- Some APs do not provide internal training and awareness on AML/CFT, TFS obligations, and sanctions evasion typologies to its senior management and Board members.
- Training programs are generic and do not consider specific role-based requirements.

6) Record keeping

Findings

Good practices

- Most APs have systems and controls to obtain additional information in relation to obtaining further information for high-risk customers and suspicious transactions.
- All records and documents pertaining to SAR/STRs, and the results of all investigations performed is maintained for at least six years from the date on which the report was made.

Areas for improvement

- Following receipt of an Internal SAR/STR, which was not filed to the FIU, insufficient documentation is maintained to support and evidence why no such report was made.
- Insufficient records maintained against false positive matches during the screening process on the UAE Local Terrorist List or UN Consolidated List.



- Detailed reports generated from the sanctions screening system used by APs as evidence for closing the alerts are not always obtained or maintained as part of the alert closure process.