ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

ADGM-DNFBP-21-0011L-CEO

By Email

15th June 2021

FSRA NOTICE NO (15) of 2021

To: All DNFBPs

Dear All,

BACKGROUND

The Financial Crime Prevention Unit ("FCPU") of the Financial Services Regulatory Authority ("FSRA") conducted an AML/CFT Thematic Review (the "Review") of Designated Non-Financial Businesses and Professionals ("DNFBP's") with a focus on law firms and corporate services providers ("CSPs") in the Abu Dhabi Global Market ("ADGM"). Both sectors were rated as 'medium-high' risk in the UAE's National Risk Assessment ("NRA") and experienced significant growth over the past two years (2018* and 2019**).

In particular, the Review sets out to achieve a better understanding of the said sectors' practices in relation to preventing and detecting acts of money laundering and terrorist financing under the obligations imposed on them by the ADGM AML Rulebook and UAE Federal AML/CFT Legislation.

THE REVIEW

The Review draws on the examination of the findings generated from a desk-based analysis of 25 Annual AML Returns submitted by 13 law firms and 12 CSPs in 2020. It is important to note that the Annual AML Return is a regulatory reporting tool that poses various specific and focused questions that the FSRA expects Relevant Persons ("RPs") to complete in a comprehensive manner. Accordingly, the FSRA deemed it important to share the findings from such a review and set out FSRA's expectations in relation to the 5 key AML / CFT compliance topics, namely:

1. Customer on-boarding;
2. Applying a risk-based approach (RBA);

---

* The number of legal consultancies increased by 6% in 2018 and by 42% in 2019
** The number of CSPs increased by 38% in 2018 and by 50% in 2019

3. Sanctions monitoring and management;
4. Suspicious Activity Reports (SARs); and
5. AML training and awareness.

For a detailed summary of the Findings and Recommendations please see Annexure A.

The institutionalization of a robust AML/CFT regime is a key priority and central to our regulatory efforts, both in the FSRA and in line with the broader UAE national efforts to combat financial crime.

The FCPU will continue to monitor industry practices in relation to AML/CFT in order to ensure that robust and effective control standards are maintained by RPs. As a means of assisting RPs in achieving the same, the FCPU will continue to conduct outreach sessions and issue specific guidance to raise the level of awareness and compliance jurisdiction-wide.

Sincerely**,**

Emmanuel Givanakis
Chief Executive Officer
Financial Services Regulatory Authority

Annexure A

Findings and Recommendations

The findings indicate that although RPs had taken some effective measures to implement the systems and controls that are prescribed in our AML Rulebook, the FCPU observed that the majority of the responses received were indicative of RPs potential shortcomings on adopting a robust risk-based approach to their AML/CFT control measures. In various instances, the implementation of systems and controls by RPs appeared partial to the extent that we concluded that many RPs may have not fully complied with the expected AML/CFT practices. As such, RPs are required to pay close attention to the below highlighted findings and recommendations with the view of improving their practices and enhancing the effectiveness of the identified risk areas.

<table>
<tr><td colspan="2">1. Customer Due Diligence (CDD)</td></tr>
<tr><td>Findings</td><td>Recommendations</td></tr>
<tr><td>The FCPU noted that even though the majority (80%) of RPs in their responses indicated that they conducted CDD and customer risk assessments as part of their on-boarding process, they did not provide any detail on the approach they adopted; neither did they specify the factors taken into consideration to determine the customer's risk rating methodology.

Although most RPs used common databases for screening their customers, just over half (58%) of RPs appear to maintain documentary evidence of the searches they performed as part of their customer on-boarding process.

Despite demonstrating the importance of conducting CDD and customer risk assessments, a significant amount (48%) of RPs appear to have failed to conduct enhanced CDD on their customers or their customers' beneficial owners classified as</td><td>The FSRA requires RPs to have in place formal internal policies and procedures to determine their approach relative to their CDD and customer risk assessments practices.

1. In order to comply with the regulatory requirements in relation to CDD practice, the adoption of structured and thought-through CDD processes and procedures through the allocation of appropriate resources, the establishment of clear roles and responsibilities, and the adoption of risk-based controls that are commensurate with their customers' ML/TF risk profile. In order to demonstrate that effective controls are in place for customer on-boarding, these processes and procedures should be formally documented, approved by senior management and reviewed on a periodic basis.</td></tr>
</table>

PEPs or assessed to be high risk. Moreover, our analysis revealed that a notable portion (48%) of RPs had not specified the frequency of conducting ongoing CDD for customers commensurate with their respective customer risk ratings (i.e. based on the categorization of 'High', 'Medium' or 'Low' risk).	2. As part of the CDD process, entities must maintain records of all documentation and information obtained in undertaking initial and ongoing CDD and hold them for the prescribed period determined by their Regulator (AML Rule 4.5 Record Keeping). 3. It is recommended that all entities must carry out enhanced CDD measures on all customers and their Beneficial Owners who are PEPs or considered to be a high ML/TF risk. Enhanced CDD measures must include, where applicable, the identification and verification of the source of funds and source of wealth as prescribed by AML 8.4.1 (c) (i) and (ii), and the outcome of which should be incorporated as an integral part of the customer risk assessment. 4. The frequency of ongoing CDD for different types of customer risk ratings (high, medium or low) should be clearly defined and documented based on a risk-based approach. To this effect, RPs should adhere, as far as possible, to the ongoing due diligence timelines assigned to a customer after completing the on-boarding process or the previous KYC periodic reviews. By way of example, it would reasonably expected that RPs should apply an intensified and on-going monitoring program with respect to higher risk transactions and customers. 5. RPs should establish and maintain effective screening software scrubs against batch lists of key names and Beneficial Owners on an on-going basis that generates real time alerts. This essentially entails a process of identifying anomalies, inaccuracies, duplicates or incomplete data and then 'scrubbing' it clean to ensure a

	standardised format is in place. Such systems may rely on new technological solutions, including monitoring algorithms or Artificial Intelligence ('AI') and must be subject to extensive due diligence and testing to ensure that RPs are able to comply with their regulatory requirements.
2. Risk-Based Approach (RBA)	
Findings	Recommendations
The Review assessed the application of a RBA by reflecting on the extent to which RPs were able to devise and appropriately utilize two key AML/CFT compliance tools, namely: their Business Risk Assessments ("BRA") and Customer Risk Assessments ("CRA"). The FCPU noted that while more than two-thirds (80%) of RPs have a formal approval process for their BRA's, more than half (68%) of RPs failed to assess their AML/CFT frameworks against the vulnerabilities identified in the UAE's NRA, and a notable amount (32%) of RPs did not possess a formal risk methodology for their BRAs. With regard to CRAs, the FCPU noted that a significant amount (28%) of RPs were unable to demonstrate the kind of procedures they used for assessing customers from high-risk jurisdictions and for those classified as PEPs.	1. As a means of considering and addressing results and risk factors identified in the UAE NRA, all RPs are required to incorporate the findings of the UAE NRA into their BRA methodology with immediate effect to avoid further regulatory scrutiny. 2. All RPs are required to incorporate BRAs as an integral part of their general compliance requirements on at least an annual basis and tailor their assessments in line with the size, nature, and complexity of their business operations. 3. RPs are required to monitor the developments of Federal AML/CFT and Sanctions laws together with the AML Rules (collectively, "AML regulations") and take into account how the aforementioned may impact the RPs daily operations. RPs are therefore required to reflect and incorporate the changes in the AML regulations as part of their BRA methodology on a timely basis. By way of example, material changes in AML regulations at any given time must be appropriately incorporated

	into both new and pre-existing products and service considerations. 4. All RPs should ensure that the BRA risk methodology is formally incorporated as part of their general compliance requirements by ensuring that it is clearly defined and documented, and reviewed on a periodic basis. 5. RPs need to analyze and comprehend the risk factors that they have included in their CRA methodologies and ensure that the calibration of the risk scores are commensurate with the degree of the ML/TF risks. 6. RPs should have documented guidance for employees who conduct CRA's to ensure a consistent standard is adhered to. 7. An RPs customer risk-based approach should be clearly documented in their policies and procedures and should differentiate in greater detail the distinct methods/approaches used to on-board customers with different risk ratings, such as simplified, standard due diligence and enhanced CDD. 8. A risk rating register should be maintained comprising a list of all of its entire customer-base that should be reviewed and updated periodically.
3. <u>Sanctions Monitoring and Management</u>	
<u>Findings</u>	<u>Recommendations</u>
The FCPU noted various shortcomings in the performance of sanctions monitoring and	1. On 18 June 2020, the FCPU issued Notice No.: FSRA/FCPU/07/2020, which

screening. The majority (76%) of RPs, failed to activate a subscription with the Executive Office of the Committee for Goods and Material subject to Import and Export Control to receive alerts on designated individuals and entities. While some RPs conducted screening on an intermittent basis, more than half (60%) of RPs who utilized technology service providers to conduct sanction screening failed to indicate the frequency that their customer database was screened against the relevant resolutions or Sanctions lists. Contrary to RPs recognizing the importance of a robust AML/CFT framework, more than one-third (38%) of RPs did not have established procedures which define their response to a 'positive' Sanctions match.	notified all RPs of the subscription feature accessible by the Executive Office for the Committee for Goods and Material subjected to Import and Export Control. The subscription disseminates updates on changes to the UNSCR's Consolidated List and the UAE National List. In order to effectively comply with requirements of AML 11.1 and Article 21 of Cabinet Resolution No. (74) of 2020, RPs are required to ensure that they have activated a subscription to receive updates from the Executive Office which should be used as part of their periodic Sanctions screening programs. Note: Entities can activate their subscription by accessing the link provided **here** 2. RPs are required to establish effective frameworks to comply with the relevant resolutions and Sanctions requirements under the AML regulations. This could include the use of technology applications to ensure accurate alert creation that stemming from the screening of their customer-base against the designated Sanctions lists on a daily basis. It is recommended that RPs consider devising a programmatic approach towards Sanctions monitoring and management which may comprise of specific enabling functions that work in conjunction to reduce Sanctions risks. These measures could include, but are not limited to: (i) Specific policies and procedures: defining the requirements of *what* needs to be screened, in what context and at which frequency; (ii) Responsible person: the appointment of a designated person with appropriate skills and experience in understanding the nuances as they relate to Sanctions

	risk; (iii) Risk assessment: applying a risk-based approach to resolve alerts, how to calibrate the screening filter to accommodate for 'false positives' and "fuzzy" logic; (iv) Internal controls: documenting the methodologies and technologies used to comply with Sanctions monitoring and management, as well as their operational risk areas (e.g. residual risks); and (v) Testing: regular assurance testing of the system and/or methodology supported by metrics, analysis and reporting. Note: RPs who do not possess an automated Sanctions screening solution, need to ensure that their employees are trained and kept abreast with best practices in relation Sanctions risk management, (e.g. the importance of varying the sequence and combination of the names that need to be screened). RPs are also required to establish effective freezing procedures. In the event where a positive match is identified, RPs are required to immediately freeze any funds without delay and without prior notice to the listed party**.** This may include funds or other assets the designated person(s) and entities may have control over.
4. Suspicious Activity Reports (SARs)	
Findings	Recommendations
The Review revealed that the majority (76%) of the RPs have successfully connected to the FIU's mandatory electronic system to	1. The provisions of AML Rule 14 stipulate that RPs must establish and maintain robust policies, procedures, systems and

report suspicious activities or transactions, (i.e. goAML); of these one RP has submitted an external SAR to the FIU via goAML.	controls in order to monitor and detect suspicious activity or Transactions in relation to potential ML/TF as prescribed by the Federal AML legislation. In order to effectively comply with the these provisions, RPs are required to register on the FIU's goAML portal as there is no longer any other acceptable means of referring STRs to the FIU. Entities are cautioned that a failure to comply with this requirement timeously will constitute a breach of the Federal AML legislation as well as the AML Rules. 2. Pursuant to AML Rules 14.2 and 14.3, RPs must retain records of all relevant details of every SAR for a period of at least six years from the date on which the report was made. These records must include all cases where alerts were internally escalated to the MLRO but decisions were taken not to report them via goAML.
5. AML Training and awareness	
Findings	Recommendations
RPs are generally familiar with the requirement to conduct AML training at least annually and at appropriate intervals based on the roles and responsibilities of their employees. However, nearly half (48%) of RPs did not provide AML training on an annual basis, and 40% of them had not tailored their training to cover their business activities including their products, services, customers, distribution channels, business partners and the level and complexity of their transactions.	1. In accordance with the provisions of AML 13.1 and 13.2, RPs must carry out annual AML training to each relevant employee on an annual basis, during on-boarding and as required on an ad hoc basis in response to specific trigger events. The content of the training should be tailored and include education on the Federal AML legislation, risks that employees may encounter during their daily activities and/or emerging risks and trends that may be applicable to RPs particular business activities. Pursuant to the requirements of AML 13.3.1, RPs are required to maintain up to date records of the:

	(a) dates when the training was given, (b) nature of the training; and (c) names of the employees who received the training. 2. RPs should regularly review, develop and communicate clear internal guidance tailored for their business which may need to include but is not limited to, the nature of ML/TF risks that arises from the RPs business, raising red flags based on customer behaviors and account activities, appropriate escalation and risk mitigation measures. 3. RPs should periodically assess and enhance their training programs to include new relevant informationto ensure that specialized training is provided for each relevant employee and a framework for continuous learning is developed within their business. To this effect, RPs may also consider devising separate role-based training or tailored training targeted at specific groups with heightened exposure, (i.e. high-risk roles such as members of the payment processing team).