Administrative Measure Publication Notice

This Notice is being published by the Financial Intelligence Analysis Unit (FIAU) in terms of Article 13C of the Prevention of Money Laundering Act (PMLA) and in accordance with the policies and procedures on the publication of AML/CFT administrative measures established by the Board of Governors of the FIAU.

The Notice provides select information from the FIAU's decision imposing the respective administrative measure and is not a reproduction of the actual decision.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

25 July 2023

RELEVANT ACTIVITY CARRIED OUT:

Trustee Services

SUPERVISORY ACTION:

Off-site compliance examination carried out in 2020

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of €41,136, Reprimand and a Remediation Directive in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 5(1), 5(5)(a) of the PMLFTR and Section 3.3.1, 3.3.2 and 8.1 of the Implementing Procedures Part I (the IPs).
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1 and 3.5.3 of the IPs.
- Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Section 4.3.1 and 4.3.2 of the IPs.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment (the BRA) & Jurisdiction Risk Assessment (JRA) – Regulation 5(1), 5(5)(a) of the PMLFTR and Section 3.3.1, 3.3.2 and 8.1 of the IPs

During the examination the Company's representatives were to a certain extent able to articulate the risks surrounding its operations and to explain the degree of such risk exposure and the necessary level of control to mitigate the same. However, the first BRA was approved by the Board of Directors of the Company in December 2019. Hence the Company was found to have delayed its adherence to document a BRA for almost 2 years after the obligation became in force in January 2018.

In addition to the above, the Company's first BRA was not considered adequate due to the following reasons:

- Failed to include quantitative data in assessing the extent of its identified threats and vulnerabilities. This since, the Company neglected to consider the number of customers, their nationality[1] and especially their country of residence, hence failed to identify the extent of the Company's risk exposure by servicing such individuals or entities.
- The BRA failed to adequately cater for the rationale behind the control rating assigned. This since the mitigating measures within the BRA were either "Effective" or "Strong" however without including any rationale to support these assessments.

The Company also failed to conduct an evaluation of the ML/FT risks associated with the specific countries or jurisdictions that its client base had connections to. In terms of the assessment of foreign jurisdictions, assessments were required to be completed for at least 16 jurisdictions located in the African continent which its clients' business operations had links to, or where legal persons/UBOs with whom a business relationship was established were residing/situated or had connections to. It is pertinent to note that many of the aforementioned countries have been identified by the FATF as "Jurisdictions with strategic deficiencies" and are subject to increased monitoring.

Finally, due consideration was given to the fact that the Company had taken it upon itself to promptly start remediating its shortcomings by amending its policies and procedures i.e., Providing an amended BRA and new JRA.

Customer Risk Assessment (the "CRA") - Regulation 5(5)(a)(ii) of the PMLFTR, Sections 3.5.1 and 3.5.3 of the IPs

The Company's CRA Methodology in force at the time of the examination was inadequate given that there were shortcomings in 3 out of the 4 risk pillars identified in the IPs as being the basis to conduct a risk assessment (interface, product/services, Customer, Geography). Said inadequacies consisted of the following:

- The majority of the files reviewed had their 'Customer risk' pillar rated as 'low' given that the BOs were known by the Company's directors and given that none of the BOs are PEPs. Whilst it is good practice for the directors of the Company to personally meet the BO and determine their respective PEP status, other non-subjective factors should have been taken into consideration to assess the risk exposure emanating from its 'customer's (e.g., source of funds/ wealth, activity, adverse media, etc).
- For 'Geography Risk', it was noted that for 30% of the files reviewed, it could not be determined which jurisdictions were taken into account, i.e.: it could not be understood whether all the connections of the customer to jurisdictions including country of residence, country where the assets are held etc where at least taken into account. This is in addition to the lack of jurisdiction risk assessment failures identified and considered above in the BRA section. This since the Company was implementing a generic statement in the CRA to substantiate its conclusion, specifically that, "all the Company's business originated from 'Africa', this risk is considered High/Medium Risk". Hence, said generic and blanket statement does not suffice and does not identify the ML/FT exposure from where the trust is established and operated, from where funds originate or are to be remitted to, as well as an evaluation of the legal and regulatory

[1] While the mere fact that a beneficial owner was born in a high-risk jurisdiction should not itself mean that the business relationship is exposed to a heightened risk of ML/FT, however the subject person should assess whether there are any further links between that jurisdiction and the business relationship.

framework of that jurisdiction, including its AML/CFT laws, transparency requirements, and reputation in relation to financial crime risks.

- For 'Product Risk', it was noted that in 90% of the files reviewed, the Company instead of assessing the risk arising from the services offered to the customer (such as *inter alia* directorship, company secretary, trust, fiduciary services), the CRA focused on the industry the customer was involved in. This letter consideration is indeed an important one, but however it should have been linked with understanding the customer risk. The product risk consideration should have been focussed on the risks surrounding the product offered by the subject person.

In addition to the above, the Company was found to having failed to conduct a CRA for 1 file. This since, the Company had established a business relationship with the customer in July 2017 and despite being terminated in February 2019, a CRA for such customer was never carried out.

Finally, due consideration was given to the Company's proactive efforts to remediate its CRA methodology after the examination.

Customer Due Diligence (the "CDD") - Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.3, 4.3.1 and 4.3.2 of the IPs

In 1 file, the Company failed to identify the BO of the customer company, this since rather than collecting the BO's passport, the passport of his son was collected instead.

In another file, the Company failed to collect any documents to verify the addresses of 2 out of the 3 BOs of the customer company.

ADMINISTRATIVE MEASURES TAKEN BY THE FIAU'S COMPLIANCE MONITORING COMMITTEE:

When deciding on the appropriate administrative measures to impose, in addition to the specific breaches outlined above, the Committee took into consideration the importance of the obligations being breached, the level of seriousness, and at times systemic nature, of the findings identified, as well as the extent of ML/FT risk such failures could lead to. The Committee also considered the Company's size, that this is not a large institution, as well as the impact that the subject person's failures may have had on both its operations and on the local jurisdiction. The exposure to countries that were listed on the FATF list of jurisdictions with strategic deficiencies and the Company's lack of thorough and comprehensive understanding of the risks emanating from such exposures was highly considered by the Committee. The good level of cooperation portrayed by the Company throughout the supervisory process was also factored in, including the Company's commitment to remediate its failures, and its statements that it had already commenced working on some action points, even prior to the Directive imposed by the Committee. However, overall the Committee couldn't but note that, at least up until the compliance review, the failures observed confirm that the Company did not give the necessary attention to understanding the risks surrounding its operations and the customers serviced, which understanding is crucial for the implementation of effective controls. .

After taking into consideration the abovementioned breaches by the subject person, the Committee decided to impose an administrative penalty of €41,136 (forty-one thousand, one-hundred thirty-six Euro) for the breaches identified in relation to:

- Regulation 5(1), 5(5)(a) of the PMLFTR and Section 3.3.1, 3.3.2 and 8.1 of the IPs;
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1 and 3.5.3 of the IPs;
- Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Section 4.3.1 and 4.3.2 of the IPs.

In addition to the above, the Committee also issued a reprimand in relation to the below breaches:

- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1 and 3.5.3 of the IPs.

In terms of its powers under Regulation 21(4)(c) of the PMLFTR, the FIAU also served the Company with a Remediation Directive (Directive), to ascertain that the Company takes remedial actions to enhancing its risk understanding and control effectiveness in view of the breaches identified. The aim of the Directive is for the FIAU to ensure that the Company enhances its AML/CFT safeguards and that it becomes compliant with the obligations imposed in terms of the PMLFTR and the FIAU's IPs, which it has been found to be in breach of. The Company was directed to remediate the breaches identified and submit the necessary documentation to prove that remediation has indeed taken place, this including but not limited to:

- An updated BRA and JRA adopted by the Company including explanations of how risk scores are being assigned to the specific jurisdictions it has links to and evidence that the breaches identified have been remediated.

- A documented update on the CRA methodology including explanations of how risk scores are being assigned in view of the breaches identified under Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs.

- Declaration that all the UBOs' identity and place of residence of its client companies are being verified.

The Directive served on the Company shall ascertain that sufficient and tangible progress is achieved on the adoption and implementation of all the procedures and measures referred to above. Finally, the Company has also been duly informed that if it fails to provide the above-mentioned information and supporting documentation within the specified deadline, the Company's default will be communicated to the Committee for its eventual actions, including the possibility of the imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21 of the PMLFTR.

The administrative penalty imposed is not yet final and may be appealed before the Court of Appeal (Inferior Jurisdiction) within the period as prescribed by the applicable law. It shall become final upon the lapse of the appeal period or upon final determination by the Court.

Key Takeaways:

- To conduct an adequate JRA, it is essential to determine the specific jurisdictions with which the subject person has business relationships or connections with, this includes the jurisdictions where the clients, counterparties, or transactions are based or conducted. Only after having identified all the jurisdictions linked to the business operations, can the subject person start gathering the necessary information to analyse the ML/TF risk associated with each jurisdiction and to ultimately assign the risk ratings and respective mitigating measures.

- In assessing the risks posed by jurisdictions it is imperative for subject persons to not simply rely on their knowledge of a jurisdiction but to consider a wide range of reliable resources that assess both the reputability and the risks surrounding the jurisdictions. Consideration of the FATF and EU lists is imperative. But so are considerations of other risks such as the level of political instability, corruption, bribery, organised crime, human and drug trafficking and other risks.

- When considering the risk specifically posed by your customer when compiling the CRA, apart from simply determining whether a customer is a PEP, SPs should also take into consideration other non-subjective factors to adequately assess the ML/FT risk exposure. This including, the source of funds

and source of wealth, the activity the customer is involved in, the structure type and any adverse media, this amongst any other factors which the subject person deems appropriate.

- Whilst personally meeting with customers to get an understanding of the risk profile is in fact a good and effective control, this however is not considered as being a sufficient customer risk assessment in terms of law. Moreover, it is also too risky to simply rely on just this factor and disregard concrete objective considerations. Whilst the subjective element shall always be present, the risk-based approach cannot solely rely on subjective mitigating measures alone, hence subject persons are to ensure to incorporate a set of objective criteria as part of their risk assessment methodology to derive the final risk score of their customers.

25 July 2023