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 penalties and measures established by the Board of Governors of the FIAU.

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

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

22 August 2023

RELEVANT ACTIVITY CARRIED OUT:

Corporate Services Provider

SUPERVISORY ACTION:

Off-site Thematic Review carried out in 2021

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €7,258 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 5(1) of the PMLFTR and Sections 3.3 and 8.1 of the Implementing Procedures (IPs) Part I
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs
- Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs
- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment (BRA) - Regulation 5(1) of the PMLFTR and Sections 3.3 and 8.1 of the IPs:

The Committee noted that the BRA provided during the compliance examination was finalised by the subject person in July 2020, this notwithstanding the obligation having come into force in January 2018. Moreover, the Committee observed that the BRA in place (albeit carried out late) could not be considered as adequate for the subject person to be able to comprehensively assess its risks and to effectively implement adequate controls. Some of the deficiencies highlighted include:

- When assessing the customer risk, while the subject person considered the industry of customers, it failed to comprehensively understand the potential risks involved in those industries.

- Despite assigning an inherent risk rating for each of the risk scenarios related to the provision of directorship services, the subject person failed to assess the overall inherent risk emanating from the directorship services it offered.

- Failure to carry out an analysis of the jurisdictions to which the subject person's customer base was connected. This albeit having customers with connections to countries such as Ukraine.

In view of the shortcomings listed, the Committee determined that, the BRA did not enable the subject person to comprehensively determine its threats and vulnerabilities and exposure to ML/FT risks. Positively, the Committee did consider that the subject person had knowledge of, and was able to explain the actual and potential risks surrounding its operations, and how its services could expose them to ML/FT risks. Indeed the Committee while noting that the BRA carried out was late, and had a number of shortcomings as outlined above, it also acknowledged that it did consider a number of risk factors that are in line with the subject person's operations.

Customer Risk Assessment (CRA) – Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs:

1. Inadequate CRA Methodology

a. Former CRA Methodology

Prior to starting a business relationship, the subject person would meet with the introducer and then with the prospective customer, with the information obtained being recorded in a document which included some general information (i.e. prospective customer name, date of the meeting, name of the person met) together with a high-level description of proposed structure and operation. However, despite having a brief description of the customers, the subject person failed to categorize risk factors and assess the customers with respective risk ratings.

b. Newly Implemented CRA Methodology

While positive of the subject person's remediation in implementing CRAs with a risk scoring assessment which factored in each risk indicator, there still remained a number of considerations within the risk factors that were not included for the assessment. Additionally, the actual methodology explaining the criteria for assigning a low, medium and high score, was not provided nor at least explained. Indeed, following a thorough review, the Committee concluded that the risk assessment applied still needed a number of enhancements. For example:

- For all the revised CRAs carried out after 17 July 2019 (being the date when the IPs requiring consideration of reputational risk came into force), the subject person failed to consider the reputation risk of the customer companies and their respective BOs.

- While the subject person considered the geographical area of the BOs, the CRA failed to consider other jurisdictional connections that customers might have. For instance, the subsidiaries for one particular customer were registered in Curacao, which connection was deemed to be material due to the fact that the subsidiary sent substantial amounts to the customer's company.

2. The CRA did not always reflect changes in the business relationship

Business relationships are not static, and the circumstances surrounding them and the customers themselves are very likely to change over time. The CRA, must therefore remain relevant, accurate and sufficiently timely if the subject person is to have a clear understanding of the ML/FT risks it is exposed to and that the measures it has put in place are effective. Nevertheless, for two (2) of the files reviewed, it was noted that this was not adhered to.

By way of example, the CRA for one customer was performed in February 2016 (in relation to services not being directorship services), whereas the subject person started providing directorship services in November 2019. Here the subject person stated that prior to the changes in services offered, various discussions were held with the introducer to consider the implications and impact of such change on the risk. However, none of the discussions were documented. In fact, a CRA update was only carried out a year later, in November 2020.

Purpose and Intended Nature of the Business Relationship - Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs:

Shortcomings in relation to the obligation to obtain information on the purpose and intended nature of the business relationship were identified in two (2) of the files reviewed. The Committee noted how the customer in File A was a holding company holding shares in the customer of File B. Nevertheless, the only information found was that the Source of Wealth (SoW) is derived from business profits, whereas the Source of Funds (SoF) comes from business operations. Moreover, the subject person held (a) a written confirmation from the BO indicating that he had been self-employed within the computer consultancy sector and with his annual income amounting to circa €24,000 and (b) a CV which included brief information on the BO's ownership of 3 structures.

While the above information is good, with regards to the corporate customer, additional information on business operations and profits were necessary such as obtaining financial statements. Additionally, the SOW of the BO was important because the customer had a € 500,000 share capital.

On-going Monitoring – Scrutiny of Transactions - Regulation 7(2)(a) of the PMLTFR and Section 4.5.2 of the IPs:

Subject persons are expected to adequately scrutinise transactions to ensure that any unusual transactions or transactions inconsistent with the customer's profile are identified and subsequently probed. Nevertheless, in three (3) files reviewed the Committee considered that during the compliance examination minimal or no supporting documentation was held on file for a number of transactions reviewed which were either unusual or not in line with the information provided by the clients.

For instance, although the objectives for Customer C and Customer D were to hold shares in gaming companies, the transactions referred to activity not in any way related to gambling business. When specifically queried on how the transactions tally with the customers profiles, the subject person stated that the customers are the personal holding companies of the BOs and whilst their main activity is to hold shares in the gaming group, they also hold other personal investments. While this may be the case, the customer files did not contain any record of any determinations made by the subject person on the basis of which the transactions were deemed as acceptable. Neither was there any evidence that the

subject person queried the transactions taking place and that these were substantiated with documentary evidence.

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

After taking into consideration the abovementioned breaches by the subject person, the Committee decided to impose an administrative penalty of seven thousand two-hundred and fifty-eight Euro (€7,258) with regards to the breaches identified in relation to:

- Regulation 5(5)(a)(ii) of the PMLFTR and corresponding Section 3.5 of the IPs
- Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs
- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs

When deciding on the administrative measures to impose and on the amount of any administrative penalty, the Committee must ascertain that these are effective, dissuasive, and proportionate to the seriousness of the failures identified. In doing so, the Committee took into consideration the importance of the obligations breached, the level of seriousness of the findings identified, and the extent of potential ML risk such failures could lead to. The Committee also considered the Subject Person's relatively small size. The good level of cooperation portrayed by subject person throughout the supervisory process was also factored in. The Committee also considered the knowledge the subject person portrayed on the risks its operations could be exposed to and showed good knowledge of the operations of its customers.

Under normal circumstances, a Follow-Up Directive would be imposed for the breaches identified in terms of Regulation 21(4)(c) of the PMLFTR, however the Committee took into consideration that the subject person has surrendered its licence. Had the subject person not surrendered its licence, a process to follow up on the measures necessary to ensure compliance with the local AML/CFT legislative provisions, both in relation to the failures for which the subject person has been found in breach (as relayed above), as well as on the remedial actions that the subject would have initiated.

The administrative penalty hereby 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 Take aways:

- Subject persons need to have sound knowledge of the risks their operations are or could be exposed too. However, in addition to having such knowledge subject persons are also to assess the risks that they are exposed to because of the business relationships they engage in. This needs to be done by assessing the inherent risk which depends on the identification of the existent threats and vulnerabilities as specified by Regulation 5(1) of the PMLFTR.

- 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 apply the respective mitigating measures.

- The CRA is one of the pillars of a sound AML/CFT compliance program where all the risk criteria are exhaustively considered, and an understanding of risk is obtained. The rationale which led the customer to be rated in a particular manner is to be reflected in the CRA and in turn it is to be ensured that appropriate mitigating measures/controls are applied to minimize the specific increased ML/FT risk identified. Documenting this process is important to confirm the considerations taken to arrive at the final risk score. 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 and also additional controls would be necessary depending on the risk identified.

- Subject persons must establish how a body corporate intends to finance its commercial activities and how it has obtained its current resources. In situations where the body corporate is already, to an extent, financially self-sufficient at an early stage, the subject person would have to consider, on a risk-sensitive basis, how, and by which means whoever contributed funds or assets acquired them. If the beneficial owner (BO) contributes significant resources which go beyond what is considered a reasonable initial amount affordable by most people, the subject person is expected to obtain information on the SoW of the individuals involved and how fresh capital will be made available. Otherwise, ascertaining that the customer can sustain its operations though the profits generated by the business is essential. Obtaining the financial statements to understand the customer's sources is a good approach.

- When monitoring transactions, subject persons are to ensure that any additional documentation and/or explanations required to substantiate the rationale behind a particular transaction or set of transactions are adequately understood. This to ensure that the activity undertaken is indeed legitimate and in line with the expected activity of the particular customer. Should the additional documentation and or explanations provided by the customer further shed doubt on the rationale of the flagged transaction or set of transactions, subject persons are to ascertain the legitimacy of the transaction and activity undertaken, this either by requesting for additional documentation and/or explanations or through other means available to the subject person.

22 August 2023