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:

16 January 2024

RELEVANT ACTIVITY CARRIED OUT:

Corporate Service Provider

SUPERVISORY ACTION:

Onsite compliance review carried out in 2020

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of Euro 49,640

LEGAL PROVISIONS BREACHED:

- Regulation 5(1) of the PMLFTR and Section 8.1 of the Implementing Procedures (IPs)
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1 and 3.5.3 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- Regulation 5(1) of the PMLFTR and Section 8.1 of the IPs

The first written Business Risk Assessment (BRA) was dated April 2020, whereas the obligation to conduct a BRA came into force in January 2018. Committee members took into consideration the Company's representations, which acknowledged this shortcoming. The Company revealed how its previous MLRO did not instruct the Directors of the Company to complete this risk assessment. It was further elaborated that when the requirement of having a BRA in place was eventually brought to the attention of several Directors, it was undertaken in a proper and comprehensive manner.

The Committee noted that the delay of over a year in the Company's implementation of its first BRA left it vulnerable and unable to identify and assess the ML/FT threat it was being exposed to when servicing its clients. Reference was made to how the obligation came into force as per the amendments to the PMLFTR in January 2018 which were binding on all Subject Persons (SPs).

Another deficiency noted during the compliance review was that the Company failed to adequately factor in the risk posed by jurisdictional connections in the determination of the BRA's final risk scoring. The BRA did not allocate a risk score to jurisdictions which the Company's customers are linked to and did not assess whether the same jurisdictions were deemed to be non-reputable or otherwise. The Committee reviewed the BRA at examination stage and concluded that it was indeed generic as it did not mention the countries with which the Company is exposed to in terms of the different interactions

with jurisdictions that may exist. Jurisdictions were grouped by EU, EEA or high risk without providing a rationale as to why a country would be considered high risk. The Committee also noted within the SP's Customer Acceptance Policy (CAP) that countries that are EU/EEA are automatically classified as low risk without providing a rationale for doing so. Similarly, the CAP refers to a category which includes '*countries that are considered as high risk by the Company*', however, they are not established by the Company since the Subject Person failed to assign a risk score to each jurisdiction that concerned its customers.

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

In 80% of the files reviewed, officers noted that the Company failed to conduct an adequately documented CRA prior to the establishment of a business relationship. It was also established that although the Company had a risk scoring system in place, it did not have a formalised methodology and it was thus not able to properly assess the risk associated with the provision of directorship services, or to determine whether its customers fell within its risk appetite. Contrary to what the Company submitted in its representations, the Committee stated that the consideration of the 4 risk pillars within the CRA is indeed mandatory and that its methodology must be clearly documented whilst listing the categorisation, weighting and rating of risk factors.

Moreover, the Company failed to document the rationale as to why there were divergencies in the risk rating linked to the provision of directorship services within CRAs found in different files, and without providing a rationale for doing so. In its representations, the Company detailed that the structure of a client company and familiarity of the Company with the BO is taken into consideration when varying risk scores to a certain degree. While the risk exposure of providing directorship services may vary depending on the customer and the Company's involvement in the same, this must not be impacted by other risk factors which would be independently considered, so as not to shape the risk rating in a manner that would increase or decrease depending on the circumstance.

Aside from this, the Company was also found to have failed in factoring in all jurisdictional connections in the CRA for 20% of the files reviewed. In those instances, the Committee found that connections relating to a client's source of wealth and the place of residence of beneficiaries of a trust behind the client company.

Transaction Monitoring- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs

The compliance examination found that the Company had deficiencies in its transaction monitoring obligations with respect to 40% of the files reviewed, where it failed to thoroughly understand the activities or transactions of its customers together with their source of funds.

The Committee reiterated that for unusual transactions, a subject person may need to ask for further information and documentation to corroborate its source of funds and any other information necessary to confirm that the funds involved in the transaction are derived from legitimate sources. While the level of data requested should not be excessive or disproportionate, it should be sufficient for the SP to reasonably conclude whether the transaction is legitimate or otherwise. Moreover, the Committee stated that even in cases where SDD is merited, the Company still needs to monitor the relationship, firstly to ensure that SDD could still be applied, but also to monitor activities and capture any instances requiring further questioning or action.

In one of the files, the BO of the customer company channelled a number of transactions ranging from €300,000 to €4 million, into the customer company's bank account. The Company submitted that the BO of the Company is a well-known wealthy individual and that overall wealth and availability of funds was clearly shown in the Consolidated Wealth Report which was presented by the Company. The Committee acknowledged that this could be the case, but the mentioned document was too generic to be able to establish the wealth of the BO. In any case, even if it were enough to establish the BO's

source of wealth, the Company still needed to understand why such considerable amounts were needed by the customer company and how they were indeed utilised.

In another file which involved the transfer of funds between companies within a complex structure involving high risk jurisdictions, the Company was found to have failed to understand the source of such funds and the purpose and use behind the loans being granted. The Committee stated that it was indispensable for the Company to understand the purpose behind these multiple shareholder loan repayments and subsequent loan repayments, and the legitimacy of such transactions. The only supporting documentation for these transferred funds were documented minutes of the meetings held, which did not provide an adequate rationale behind these substantial loan amounts.

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

When deciding on the appropriate administrative measures to impose, in addition to the breaches outlined above, the Committee took into consideration the level of seriousness and at times the systematic nature of the breaches identified; the importance of the AML/CFT obligations that the Company has breached, together with the seriousness of the findings identified and their material impact. It considered the fact that the Company cooperated with the FIAU officials during the carrying out of the whole compliance review process. The Committee also took into consideration the nature and the size of the operations of the Company, and how the services it rendered and the AML/CFT controls in place, or lack thereof, may have impacted the local jurisdiction as a whole. It took note of the good levels of commitment by the Company and the enhancements in its level of regard toward the importance to understand and manage ML/FT risks. All such considerations had an impact on the final determination of the value of the administrative measure.

The Committee was particularly concerned regarding the degree and extent of non-adherence with certain crucial regulatory requirements as observed during the compliance examination. The extent to which the Company fell short of fulfilling these obligations raises doubts about the effectiveness of its AML/CFT measures and controls, at least, until the time when the compliance examination was taking place.

After taking into consideration all the above-mentioned information, the Committee decided to impose an administrative penalty of forty-nine thousand six hundred forty euro (€49,640) in terms of Regulation 21 of the PMLFTR with regards to breaches to:

- Regulation 5(1) of the PMLFTR and Section 8.1 of the Implementing Procedures (IPs)
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1 and 3.5.3 of the IPs
- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs

The Committee also took into consideration the fact that the Company is in the process of surrendering its license. Had the Company not began the procedure to surrender its license, apart from the administrative penalty indicated above, the Committee would have also served a Directive upon it, to follow up and carry out remedial actions in order to rectify the failures observed.

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

- SPs must ensure that they are aware of their obligations at law in order to ensure a robust AML/CFT framework to safeguard their operations from such threats. In this regard, it is of the utmost importance for SPs to stay updated to any changes to the same legislation to always ensure conformity with the same obligations while in operation.

- The BRA must include all the countries which the business is exposed to and understand the extent to which the exposure to same is material. In such circumstances, the Company should consult sources both to understand the country's reputability (which sources are dictated in the IPs) as well as the risks prevalent in a jurisdiction and then, according to such sources and determined exposure, the Company would need to determine the overall degree of risk each country presents to its operations. SPs should not rely on limited sources when it comes to risk rating jurisdictions, as multiple reliable sources should be consulted for the company to arrive to its own risk determination of each concerned jurisdiction.

- The CRA should be adequately documented for each client and conducted in a timely manner prior to the establishment of a business relationship with the same customer. The CRA should be based on the 4 risk pillars in line with Section 3.5 of the IPs in order to obtain a comprehensive framework and visibility of the risks associated with each of its customers. Among other things, SPs should consider all the material geographical connections that exist in relation to its customers.

- The application of SDD does not mean that no CDD is carried out, but rather that the extent and timing may vary. Even when SDD is applied, there should still be a level of monitoring undertaken, both to ensure that SDD is still merited, and to ensure that any circumstances requiring action are captured and addressed. The monitoring of customer behaviour and activities is indispensable in all circumstances.

- Transaction monitoring is essential to ascertain that the client's activity is in line with the customer profile, and in default, to make sure that information is obtained to verify the source of funds. In such instances, the subject person may be required to understand further and evidence the client's source of wealth through supporting documentation. Even though the IPs themselves state that the level of data to be obtained by the SP should not be excessive, disproportionate or irrelevant and that the requests should make sense in the context of the transaction and the customer in question, the level of data should be sufficient to allow the SP to be able to reasonably conclude whether the transaction is legitimate or otherwise.

16 January 2024