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.

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

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

12 July 2022

RELEVANT ACTIVITY CARRIED OUT:

Accounting and Auditing Services

SUPERVISORY ACTION:

Compliance review carried out in 2020

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €22,107 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 3.3.1 of the Implementing Procedures (IPs)
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5, 3.5.1, 3.5.2, 3.5.3 and 8.1 of the IPs, and Section 4.1 of the 2015 and 2017 IPs

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment

The review carried out on the Subject Person's Business Risk Assessment (BRA) revealed various shortcomings which convey that this assessment was not truly reflecting the threats and vulnerabilities of the Subject Person's business.

Moreover, the BRA fell short in properly documenting the methodology used for the assessment of the services offered by the Subject Person and the latter where not properly assessed in the BRA. Additionally, the Subject Person assigned a low-risk score to the services offered by the Subject Person without providing an adequate justification for this. The Compliance Monitoring Committee (Committee) noted that this low-risk score assigned by the Subject Person contrasted sharply with the level of risk assigned to CSPs by the National Risk Assessment (NRA) and the Supranational Risk Assessment (SNRA) issued by the European Union in 2019, and there was no justification for the divergence.

The section within the BRA dealing with the risk posed by the Subject Person's customers was too brief and generic in nature as it failed to properly assess the qualitative and quantitative aspect of the risk area. Furthermore, an assignment of a low overall residual customer risk score was not appropriate due to the nature of the customers it services. The Subject Person deals with customers which, inter alia, trade in sectors such as the gaming and transportation sectors, are structured as holding companies, contain complex/multi-tier structures, and have connections with high-risk jurisdictions. Although the gaming and transportation sectors on their own do not automatically pose a high risk of ML/FT, when considering these together with the other element, a low-risk situation becomes highly doubtful.

The BRA rated the interface/delivery risk of the business as posing a low residual risk of ML/FT without any reasoning or methodology to support that low-risk rating.

In relation to geographical risk, the BRA assigned a low overall residual risk score to the ML/FT risk posed by the geographical areas with which the Subject Person has links and/or deals with. The Committee determined that this overall risk score is unfounded and inappropriate since during the compliance review, it was evident that the Subject Person has/had dealings with various foreign jurisdictions. Some of these jurisdictions were also considered to be high-risk at the time of undertaking the occasional transaction or during the business relationship.

In addition, the BRA failed to take a quantitative approach both when compiling it and computing the risk scores. The Subject Person was simply listing, but not identifying, the extent of the threats and vulnerabilities that it was exposed to since it was not considering the risk factors from a quantitative point of view.

Consequently, in view of the above shortcomings, the Committee decided that the Subject Person was in serious breach of Regulation 5(1) of the PMLFTR and Sections 3.3 and 3.3.1 of the IPs.

Customer Risk Assessment and Policies and Procedures

The Committee noted that in its policies and procedures, the Subject Person was using the term 'non-reputable' to indicate that jurisdictions are to be considered as having high risk of ML/FT. This means that the Subject Person failed to draw a distinction between a non-reputable jurisdiction and a high-risk jurisdiction. Additionally, the Subject Person, in its representations, acknowledged that its policies and procedures had shortcomings when it comes to documenting whether certain jurisdictions are reputable or non-reputable.

In respect of 3 occasional transactions, a Customer Risk Assessment (CRA) was not found on file. This means that the Subject Person had failed to identify and assess the ML/FT risks emerging from having carried out these transactions. This increased the risk that due diligence measures could not be commensurate to the level of the risk that the customers were posing to the Subject Person. Thus, the Subject Person was neither able to mitigate the inherent risk, nor to determine whether these specific occasional transactions fell within the Subject Person's risk appetite. In its representations, the Subject Person held that these occasional transactions were carried out in 2015, 2017 and 2018 respectively and that at the time the old version of the IPs was in place, and these were not as detailed as those set out in the subsequent versions. However, the Committee highlighted that the subject persons' obligation to carry out a CRA in respect of their customers was detailed in the very first IPs in 2011, and simply evolved in detail over time. Moreover, while the IPs do refer to the possibility to carry out a more comprehensive CRA following onboarding, they

also clearly state that a CRA must be carried out as part of the onboarding process. Due to this, the Committee determined, that the Subject Person was expected to identify and assess the ML/FT risks posed by the customer as early as onboarding stage.

Although the Subject Person had assigned a score to risk rate customers, no documented rationale was provided to justify the score given to the different risk factors in any of the seventeen (17) transactions reviewed in which a CRA was drawn up. Consequently, it remained unclear how these risk factors were weighted to arrive at the score assigned. Occasionally, the Subject Person assigned the lowest score within the range risk scores without due explanation of how and why the score was determined. The methodology and weighting being applied by the Subject Person led to a situation where it was impossible for any business relationship or occasional transaction to be classified as posing a high risk of ML/FT.

The Committee noted that when assessing customer risk, rather than evaluating the factors which assess the risk brought about by the customer, the Subject Person only considered the jurisdiction of the customer and the nationality and/or residence of the BO, even though the jurisdictional risk was already being assessed in the jurisdictional aspect of the CRA. Consequently, this could not be classified as an assessment of the customer risk.

Despite the connections which the Subject Person's customers had with several jurisdictions, the Subject Person failed to assess the ML/FT risks emanating from these connections as part of the CRA. It became apparent that, with regards to 6 customer files, the Subject Person did not consider all the geographical links that the customers and their respective beneficial owners had. The shortcomings included failure to carry out a jurisdictional risk assessment: on the place of residence of the customer's BO; on the jurisdictions where two trusts within the legal arrangement were settled; and on the jurisdictions from where the customer's BO was generating his wealth.

As part of its policies and procedures, the Subject Person created a jurisdiction risk list which it updated on a yearly basis. However, discrepancies were noted between this list and the final jurisdiction risk rating documented in the updated CRAs. The Subject Person should have therefore ensured uniformity in the approach to jurisdiction risk considerations, ensuring that the risks of a jurisdiction are clearly and unequivocally determined and then applied to each customer depending on the perceived exposure to any jurisdiction.

For all the occasional transactions carried out since 17 July 2019 (being the date when the IPs requiring consideration of reputational risk came into force), the Subject Person had failed to consider the reputation risk of the customer company and its BOs in the CRA. In fact, the Subject Person did not perform further checks, neither on the customer nor on its BO that covered the reputational risk.

In view of the above, the Committee determined that the Subject Person was in serious and systemic breach of Regulation 5(5)(a) and 5(5)(a)(ii) of the PMLFTR and Sections 3.5, 3.5.1, 3.5.2, 3.5.3 and 8.1 of the IPs, and Section 4.1 of the 2015 and 2017 IPs.

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 twenty-two thousand, one hundred and seven euro (€22,107) with regards to the breaches identified in relation to:

- Regulation 5(1) of the PMLFTR and Sections 3.3 and 3.3.1 of the IPs for the Subject Person's serious failure to have an adequate BRA in line with the requirements imposed by the PMLFTR and the IPs
- Regulation 5(5)(a) and 5(5)(a)(ii) of the PMLFTR and Sections 3.5, 3.5.1, 3.5.2, 3.5.3 and 8.1 of the IPs, and Section 4.1 of the 2015 and 2017 IPs

When deciding on the final amount of the administrative penalty to be imposed, in addition to the specific considerations outlined above, the Committee took into consideration the importance of the obligation, the seriousness of the findings identified, and the risk of possible ML/FT caused by the breach identified. The Committee also considered the impact that the Subject Person's failure may have had on both its operations and on the local jurisdiction, the size of the Subject Person, as well as the fact that the officials of the Subject Person were generally cooperative during the examinations. The Committee also took into consideration that the breaches identified were a result of the Company's lack of adherence to AML/CFT obligations imposed by the PMLFTR and the IPs. Furthermore, the Committee ensured that the penalty being imposed is effective, dissuasive, and proportionate to the failures identified.

In reaching its conclusions, the Committee also took into consideration that the Company has ceased to carry out any relevant activities as outlined in the PMLFTR. In ordinary circumstances and had the Company still been operating, in addition to the administrative penalty, a Remediation Directive would have been imposed to address the Company's failures to adhere to its AML/CFT obligations. Through such a Directive the FIAU's Enforcement Section would be monitoring the actions taken by the Company to remedy the shortcomings, as well as guiding the Company to implement the additional measures necessary to be compliant with its legal obligations, as well as to have effective and robust controls to combat ML/FT. However, due to the termination of any relevant activity by the Company the Directive could not be applied.

Key Takeaways

- Subject Persons are required to take appropriate steps, proportionate to the nature and size of their business, to identify and assess the risks of ML/FT arising from their activities. This risk assessment should consider the customers, countries or geographical areas, products, services, transactions, and delivery channels, as well as any national or supra national risk assessments relating to the risks of ML/FT.

- The identification of the threats and vulnerabilities a subject person is exposed to requires consideration of the risk areas and risk factors both from a qualitative and a quantitative point of view. Thus, for the purposes of the BRA, it is not sufficient for the subject person to merely draw up an inventory of the threats or vulnerabilities, but the subject person must also consider how numerous these threats or vulnerabilities are. The use of past experience for subject persons that have been in operation is highly recommended.

- The Subject Persons' BRA must assess whether the jurisdictions they are dealing with are non-reputable jurisdictions or are otherwise to be regarded as high-risk jurisdictions. While a non-reputable jurisdiction is always to be regarded as a high-risk jurisdiction, a high-risk jurisdiction may not necessarily always be regarded as a non-reputable jurisdiction. A non-reputable jurisdiction is one that has deficiencies in its national AML/CFT regime or has inappropriate and ineffective measures for the prevention of ML/FT. When assessing whether a jurisdiction is to be considered as high-risk, subject

persons are required to conduct a wider assessment than merely assessing the jurisdictions' AML/CFT issues and shortcomings, and hence should also include other factors when conducting their assessment such as prevalent crime risks, application of the rule of law, risks of corruption and bribery and other factors.

- To understand the jurisdiction risk exposure, Subject Persons should be aware of the jurisdictions the customer is exposed to. This can take many forms. In case of a corporate customer, Subject Persons must consider both the place of incorporation and where business is being carried out to/from, taking into consideration the materiality of the exposed jurisdiction where business dealings are taking place. Subject persons must also consider both the place of residence of the BO and where the wealth of the BO has been generated, especially where the BO is funding the corporate entity.

- Apart from understanding risk at a business-wide level, Subject Persons must have this understanding to also assess risks at a customer level. This is done by carrying out a CRA for each business relationship formed or occasional transaction carried out. Amongst the risk factors to consider for the CRA, the subject person must consider, customer risk, geographical risk, product, service and transaction risk and delivery channel risk. The CRA must factor in the reputational risk a customer or its beneficial owner may pose by considering any links they have to adverse reports linking to crime and/or terrorism.

- Subject Persons must consider all risk factors that are known, including those referred to under Section 3.2 of the IPs and ensure that all these factors are included in the customer's risk profile. The information collected to draw up the CRA formulates the customer's risk profile, which subsequently determine the adequate level of Customer Due Diligence (CDD) measures to be applied to mitigate the ML/FT risk posed by the customer.

- Customer risk is the risk of ML/FT that arises from entertaining relations with a given person or entity. This may be due to the business or professional activity carried out by the customer or the beneficial owner. Some business or professional activities, from which the customer or the beneficial owners are deriving their wealth or the funds to be used during a business relationship or an occasional transaction are to be considered as presenting a high risk of ML/FT. Furthermore, the assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. With respect to legal entities, subject persons must assess the risk posed by the industry. Furthermore, they must be conscious that corporate structures, trusts, foundations, associations, and commercial partnerships may be used as a vehicle to obscure the link between a criminal activity and the persons benefitting from the proceeds of such criminal activity.

18 July 2022

APPEAL – On the 2nd August 2022, the FIAU was served with a copy of the appeal application filed by the Subject Person before the Court of Appeal (Inferior Jurisdiction) from the decision of the FIAU as detailed above. The grievances brought forward by the Subject Person include, inter alia, that the FIAU based its decision on incorrect factual considerations; that the FIAU based its decision on a wrong application of the law; that the process leading to said decision breaches the Subject Person's right to a fair hearing; that the law on the basis of which the administrative sanction is imposed and

the manner in which the Subject Person was treated are unconstitutional. It thus requests the Court to uphold its appeal and cancel the administrative penalty imposed by the FIAU.

Pending the outcome of the appeal, the decision of the FIAU is not to be considered final and the resulting administrative penalty cannot be considered as due, given that the Court may confirm, vary or reject, in part, the decision of the FIAU. As a result, the FIAU may not take any action to enforce the administrative penalty pending judgement by the Court.

This publication notice shall be updated once the appeal is decided by the Court so as to reflect the outcome of the same.

8 August 2022