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:

Corporate Service Provider

SUPERVISORY ACTION:

Targeted compliance review carried out in 2020 and targeted compliance review carried out in 2022 in relation to five corporate customers

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €25,822 and 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) of the PMLFTR and Section 3.3 and 3.3.1 of the Implementing Procedures (IPs).
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.5, 3.5.1, 3.5.2, 3.5.3 and 8.1 of the IPs, and Section 4.1 of the 2015 IPs.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Targeted compliance review carried out in 2020

Business Risk Assessment

The review carried out on the subject person's Business Risk Assessment (BRA) revealed various shortcomings, which conveyed that this assessment was not reflecting neither the threats and vulnerabilities of the subject person's business nor the extent. .

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 were not properly assessed in the BRA. Additionally, the subject person assigned a low-risk score to the services it offered without providing an adequate justification for this. The Committee noted that this low-risk score being 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 this divergence.

The section within the BRA dealing with the risk posed by the subject person's customers was too brief and generic in nature since 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 since, during the compliance review, it emerged that the subject person deals with customers which, inter alia, trade in sectors which deal in high value or high frequency transactions, are structured as holding companies or contain complex/multi-tier structures and have connections with high-risk jurisdictions.

The BRA rated the interface/delivery risk of the business as posing a low residual risk of ML/FT without any reasoning or methodology behind 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 emerged that the subject person has/had dealings with various foreign jurisdictions. Some of these jurisdictions were also considered to be high-risk or non-reputable at the time of undertaking the occasional transaction or during the business relationship.

The Committee further 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. In its representations the subject person, acknowledged that its policies and procedures had shortcomings when it comes to documenting whether certain jurisdictions are reputable or non-reputable.

In addition to this, the BRA failed to take a quantitative approach in the computation of the risk scores and in its overall compilation.. 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 findings constituted a serious breach of Regulation 5(1) of the PMLFTR and Sections 3.3 and 3.3.1 of the IPs.

Customer Risk Assessment

During the compliance review it became apparent that for one of the customer files taken into consideration for the purposes of the review, no Customer Risk Assessment (CRA) was held on file in respect of a particular occasional transaction. Thus, the risks for this relationship were unknown, rendering the correct application of due diligence measures more challenging. In its representations, the subject person held that the mentioned occasional transaction was carried out in 2015 and that at the time the old version of the IPs was in place, which procedures 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 has been in force since the introduction of the IPs in 2011. 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.

In the thirty-six (36) transactions/business relationships reviewed wherein a CRA was carried out, the subject person had assigned a score to risk rate the customers. However, the subject person failed to document the rationale justifying the score assigned to the different risk factors. Consequently, it remained unclear how these risk factors were weighted to arrive to the score assigned. Moreover, the CRA was carried out and drafted in a very brief manner in respect of sixteen (16) of these customer files. These CRAs were insufficient as the customer risk, product/service risk, delivery channels/interface risk and geographical risk were not considered when assessing the ML/FT risk posed by the customer. Furthermore in 3 out of the above-mentioned sixteen (16) files, the overall risk score was not included. In addition, the CRA was carried out one year late in respect of four customer files, and four years late in respect of another customer file.

The below considerations were taken by the Committee in respect of each specific risk factor:

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.

Furthermore, in situations where the subject person offered incorporation and registered office services consecutively, only the BOs were assessed without any assessment being carried out in respect of the corporate customers. The Committee remarked that although at the stage of incorporation, it is not possible to carry out a detailed CRA on the corporate customer itself, the subject person was still expected to assess the customer's prospective organisational structure and its potential business markets. This is even more so since the subject person offered the provision of a registered office to the corporate customers in question. A detailed CRA, assessing the corporate customers, should have then followed in due course during the business relationship.

The product/service being offered by the subject person was not factored in the CRA for 4 customer files. The Committee also noted that in some of the files reviewed, the subject person assigned a low-medium risk score and medium risk score to the CSP services being offered by the subject person. The Committee reiterated that the NRA rates the CSP sector as posing a high risk of ML/FT both from an inherent and residual risk perspective. In addition to this, the Committee observed that no documented justification as to why these services were given a lower risk score was found on file.

In 5 customer files, the delivery channels/interface risk were not factored in the CRAs. Moreover, although, the delivery channels/interface risk were being factored in the updated CRAs, it resulted that there were 5 files wherein this was not done prior to the establishment of the business relationship or the carrying out of the occasional transaction. Additionally, in the case of a particular customer file, the individual customer was being represented by an agent. However, the subject person failed to factor this situation in the CRA.

Despite the connections the subject person's customers had with several jurisdictions, the subject person failed to assess the ML/FT risks emanating from such connections as part of the CRA. In the case of 5 customer files, the subject person did not consider all the geographical links that the customers and their respective BOs had. Such shortcomings included: failure to carry out a jurisdictional risk assessment on the place of residence of the customer's BO; and, where the service offered to the customer was the provision of a registered office, failure to take into consideration the jurisdictions where shareholding companies of the corporate customer were incorporated. In its representations, the subject person indicated that the focus was made on the nationality of the BO. However, the Committee emphasised that while nationality of the BO should be factored in, one has to remain cautious as to its actual impact and understand what the real ties with the jurisdiction are. Nationality does not define an individual since they could since have distanced himself both physically and financially from the respective country of nationality. On the other hand, the BO's place of residence is an essential element that must be considered when conducting the jurisdiction risk assessment as this could be linked to the place of his/her own business and from where his/her wealth is being generated. Apart from the BO, as already relayed previously, understanding the jurisdiction risk posed by other entities which are also part of the group is equally important.

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 the particular jurisdiction(s) the customer had connections to.

The Committee noted that at times the subject person assigned the lowest score within the range of the risk score without due explanation of how and why this rating was assigned. This approach leads 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. This further reaffirms the serious failures with the methodology implemented by the subject person.

In view of the above, the Committee determined that the subject person was in serious and systemic breach of Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.5, 3.5.1, 3.5.2, 3.5.3 and 8.1 of the IPs, and Section 4.1 of the 2015 IPs.

Targeted compliance review carried out in 2022 in relation to five corporate customers

The Report noted that the five corporate files examined during the compliance review related to companies incorporated on behalf of the same individual. The companies were incorporated over a period of 17 months creating an element of duration sufficient to establish a business relationship with the beneficial owner.

In its representations the Company submitted that at the time when the customers were onboarded, the distinction found within the Report between a business relationship and an occasional transaction had not yet been included in the IPs and thus, the Company had considered such incorporations as a single one-off service. The Committee rebutted the Company's arguments and stated that the distinction between a business relationship and an occasional transaction has been in force since the introduction of the IPs and the implementation of the PMLFTR. The text found within the IPs as amended in 2019 was intended to serve as a further explanation of the distinction between a business relationship and an occasional transaction, which has always been characterised by the same three elements:

- The relationship must be of a business, professional or commercial nature
- The relationship must subsist for a period
- One of the persons involved in the relationship must be a subject person

The Committee observed that although a business relationship existed with the beneficial owner for the purpose of incorporating the 5 companies, the Company still failed to obtain information on the purpose and intended nature of the business relationship on these companies. The Company did not gather information on the reason why the individual had to create 5 separate companies with related purposes within just 17 months. This fact, in and of itself, should have prompted the Company to obtain further details as to why the beneficial owner required these 5 companies to conduct his business and what each customer would be doing. This would have allowed for the understanding whether it made sense to create all these companies in a very relatively short period of time. Furthermore, to garner further information on the risk profile of the customer (i.e., the BO of all these 5 companies).

In view of the Company's failure to obtain information on the purpose and intended nature of the business relationship, the Committee concluded that the Company was in breach of its obligations under Regulation 7(1)(c) of the PMLFTR. Nonetheless, the Committee noted that no funds had been processed through these five customers and that the subject person had general knowledge on the operations of each individual company that was being formed as well as on the BO. Additionally, it was noted that the BO had experience in the sector within which the companies were operating. Since the ML/FT risks associated with these relationships were minor in nature (since no funds were processed and the beneficial owner had experience in the industry of the companies), the Committee agreed to serve a Remediation Directive.

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-five thousand, eight hundred and twenty-two euro **(€25,822)** 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)(ii) of the PMLFTR and Sections 3 .2, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.5, 3.5.1, 3.5.2, 3.5.3 and 8.1 of the IPs, and Section 4.1 of the 2015 IPs for the subject person's serious and systematic failures in its CRA methodology.

In addition to the above, the Committee also served the subject person with a Remediation Directive due to the stated breaches of the PMLFTR and IPs, as well as about the breach of Regulation 7(1)(c) of the PMLFTR. The aim of this Remediation Directive is to direct the subject person to take the necessary remedial action to ensure that it understands the risks surrounding its operations and that the subject person has implemented sufficient controls to mitigate the identified risks. Furthermore, it aims to ensure that the subject person is effectively addressing the breaches set out above. In virtue of the Directive, the Company was requested to make available:

- An updated BRA which incorporates a revision of the Company's ML/FT risks and of the mitigating measures in place, consider risk factors from a qualitative and quantitative perspective, consider details as found in the NRA and SNRA for the specific sector of the subject person and determine whether the remaining residual risk falls within its risk appetite.
- An updated and documented CRA, based on the four risk pillars, explaining how each risk factor is assessed and scored, and the way the final risk rating is obtained.
- Policies and procedures which clearly delineate the information and documentation, which needs to be collected where applicable, from the Company's customers to establish their purpose and intended nature. This must include the collection of information on the business/activity of the customer, its source of wealth and source of funds, and the anticipated level and nature of activity. The Company's policies and procedures should also clearly establish the distinction between a business relationship and an occasional transaction.

Moreover, the Company must carry out a review of all its active clients to make sure that the risk assessments maintained by the Company are accurate, adequate and in accordance with the updated CRA methodology of the Company.

The subject person was informed that in the eventuality that the requested information and/or documentation is not made available within the stipulated timeframes, the Committee will be informed of this default for its consideration and possible eventual action.

When determining the appropriate administrative measures to impose, 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 overall cooperative during the examinations. The Committee also took into consideration that the breaches identified were a result of the subject person'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.

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 must 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. The subject person should 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 shortcoming, and hence should also include other factors when conducing their assessment such as prevalent crime risks, application of the rule of law, risks of corruption and bribery and other factors.
- In addition to understanding business-wide risks, subject persons are also required to carry out a customer specific risk assessment i.e., a CRA, that is, an assessment of the specific risks they will be exposed to in providing their services or products, either during a business relationship or in the event of an occasional transaction. Amongst the risk factors to consider for the CRA, the subject person needs to consider, customer risk, geographical risk, product, service and transaction risk and delivery channel risk. One must have due regard to the operations or business endeavours of the customer; the source of wealth funding the operations; any risks presented by who is in control (where applicable); the jurisdiction of incorporation or residence, the place of operations, target markets or the place where the source of funds would be emanating from; the risk of PEPs being involved as well as consideration of the delivery channel.
- 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 determines the adequate level of CDD measures to be applied to mitigate the ML/FT risk posed by the customer.
- Subject persons are required to carry out the CRA prior to entering into a business relationship or carrying out an occasional transaction. Furthermore, the assessment should be reviewed from time to time in accordance with the risk presented by the business relationship and when there is an event marking a material departure from the risk profile of the customer. Any decisions relative to the CRA and changes to it must be duly documented to evidence that an appropriate assessment has taken place.
- 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 should assess the risk posed by the industry and to 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.

- In situations where the services being offered by subject persons involve the incorporation of a new company and provision of a registered office, although at the stage of incorporation, it is not possible to carry out a detailed CRA on the entity itself, subject persons are still expected to assess the entity's prospective organisational structure and its potential business markets. This should be done as a consideration of the service being offered to the customer (in this case being the beneficial owner). A detailed CRA, assessing the corporate customer, must then follow during the business relationship, in circumstances where a service would then be offered to the corporate customer.
- The scores assigned to the individual risk factors should then allow the subject person to generate an overall risk score and lead to an understanding of whether the business relationship or occasional transaction falls within its risk appetite. Where this is the case, the subject person is then to categorise the business relationship or occasional transaction accordingly.
- With respect to interface risk, communication with an agent on behalf of the customer must be factored in as one of the considerations to be considered when risk assessing customers (even when the customer was met by the subject person face-to-face).
- When it comes to the jurisdiction risk assessment carried out for the purposes of the CRA, subject persons must keep in mind that nationality does not define an individual since they could since have distanced themselves both physically and financially from the country of nationality. On the other hand, the BO's place of residence is an essential element that must be considered when conducting the jurisdiction risk assessment as this could be linked to the place of their own business and from where the wealth is being generated. This is particularly important when the BO would be funding or financially aiding the company's operations. Apart from the BO, as already relayed previously, understanding the jurisdiction risk from other entities which are also part of the group is equally important.

19 July 2022