



## 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 measures established by the Board of Governors of the FIAU.

This Notice provides extracts 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:**

17 November 2023

### **RELEVANT FINANCIAL ACTIVITY CARRIED OUT:**

Fiduciary Service Providers (Trustees & Fiduciaries)

### **SUPERVISORY ACTION:**

Onsite compliance review carried out in 2020

### **DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:**

Remediation directive.

### **LEGAL PROVISION BREACHED:**

- Regulation 5(1) of the PMLFTR and Sections 3.3 of the Implementing Procedures (IPs) Part I
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1, 3.5.3 and 8.1.3 of the IPs Part I
- Regulation 5(5)(a) of the PMLFTR and Section 3.4 of the IPs Part I
- Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.2.1, 4.2.2 and 4.3 of the IPs Part I
- Section 4.3.1.1 of the IPs Part I
- Regulation 11(1) of the PMLFTR and Section 4.9 of the IPs Part I
- Regulation 7(1)(d) and 7(2)(b) of the PMLFTR and Section 4.5.3 of the IPs Part I
- Regulation 13 of the PMLFTR

### **REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURES:**

#### Business Risk Assessment (BRA)

The Compliance Monitoring Committee (Committee) observed that there were three versions of the BRA carried out by the Company – one prior to the examination (dated 2018), one provided by the Company at the time of the examination (dated 2020), and another one performed after the examination (dated 2021).

The Committee noted that the BRA provided by the Company for the purposes of the compliance examination carried out in 2020 contained several deficiencies in its methodology, including the following:

- Failure to outline the likelihood of money laundering and funding of terrorism (ML/FT) scenarios



- materialising and their possible impact;
- Failure to mention the Company's risk appetite;
- No number/percentage of customers falling under each risk category;
- Failure to outline the mitigating measures in place;
- Failure to consider the markets in which the Company operates;
- Failure to explain the rationale behind the assigned risk rating.

The Company in its representations also referred to an older version of the BRA, dated 2018, which it had submitted with its 2019 REQ. Nonetheless, the Committee noted that this document failed to explain the methodology for the assigned risk ratings. Additionally, there is no indication that the four risk categories, i.e., customer risk, product risk, interface risk and geographical risk, have been taken into consideration. This document merely provides a list of the Company's individual customers, the assigned risk rating to each of these and the Company's overall risk rating. The Committee held that it is clear that the requisites imposed by the PMLFTR, and which had been in place since January 2018, were not adhered to by the Company in the formulation of this BRA. The Committee also made reference to the 2018 Supervisory Guidance Paper on ML and FT Institutional/Business Risk Assessment, the updated IPs issued in 2019 and to the 2018 PMLFTR and stated that the Company had sufficient guidance for it to carry out an adequate BRA.

In determining the administrative measure to be imposed, the Committee took into consideration the BRA dated 2021 carried out by the Company following the compliance examination. Whilst the Committee acknowledged that the latter BRA had addressed the deficiencies existent in the previous BRA i.e. the one available at the time of the compliance examination, certain risk scenarios were still missing. Despite the fact that the Company did take certain measures to remedy its BRA, these could not be used as a justification to exonerate the Company from the shortcomings persisting at the time of the visit.

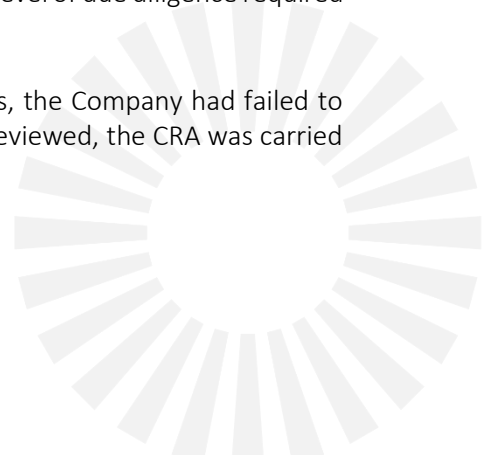
In view of the above, the Company was found in breach of Regulation 5(1) of the PMLFTR and Sections 3.3 of the Implementing Procedures (IPs) Part I.

#### Customer Risk Assessment (CRA)

The Committee noted that although the Company did have a document outlining the risk factors and their allocated risk weighting, there was no documented explanation on the calculation of the final risk score and the rationale behind a risk weighting being assigned to a particular risk factor. Moreover, the Committee also noted that the CRA matrix assesses whether its customers are linked to a low, medium and high jurisdiction by relying exclusively on the Transparency International Corruption Perception Index (CPI).

Additionally, with respect to two (2) corporate customers belonging to the same BO, the Company carried out solely one CRA. The Committee pointed out that even though the entities in question belonged to the same BO, two separate CRAs should have been carried out by the Company for each of the corporate companies at onboarding stage in order to assess the ML/FT risks posed by both entities to the Company. The Committee noted that even though both corporate customers were in the same industry, both entities should have been risked assessed separately in order to take adequate consideration of the actual risk factors pertaining to each entity and, consequently, to apply the appropriate level of due diligence required according to the risks identified.

Furthermore, the Committee noted that, with respect to two (2) customers, the Company had failed to carry out a CRA. Moreover, with respect to circa 67% of the customer files reviewed, the CRA was carried



out late.

In view of the above reasons, the Committee determined that the Company was in breach of its obligations under Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1, 3.5.3 and 8.1.3 of the IPs.

#### Policies and Procedures

The AML/CFT policies and procedures provided by the Company for the purposes of the 2020 compliance examination were vague and generic as they were not risk-based and did not include the steps which the Company had designed to counter the financial crime threat posed to it. The Committee noted that the Company did not provide representations in respect of this finding. Following a review of the Company's AML/CFT policy document, the Committee noted that a risk scoring grid was provided in the said document wherein the risks pertaining to the customer, product, interface and geographic risks are listed and assigned a risk scoring. However, as stated in the Findings Report, the document failed to provide information on the measures taken by the Company in respect of each risk respectively in order to mitigate the same. Moreover, it was noted that the mentioned risk scoring grid did not explain the rationale behind the assigned risk scores with respect to each risk factor.

Additionally, the ongoing monitoring procedures outlined in the AML/CFT policy and procedures did not outline, for instance, when periodic reviews should be carried out in a manner which is commensurate to the level of risk posed by the customers. Moreover, the Company's procedures did not provide that an unusual transaction or changes in the customer's activity should serve as a trigger event for the Company to request and obtain additional information/documentation to be able to establish whether the transaction is suspicious or otherwise legitimate. Furthermore, it was noted that there was no documented process in place setting out how customer risk drives the frequency, scope and nature of periodic reviews.

In view of the above, the Committee determined that the Company was in breach of its obligations under Regulation 5(5)(a) of the PMLFTR and Section 3.4 of the IPs.

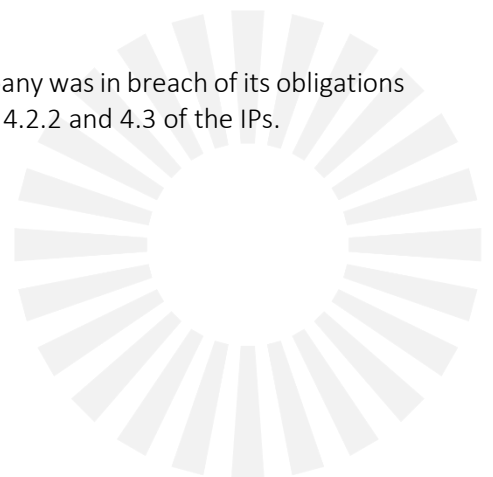
#### Customer Due Diligence

The Committee noted that with respect to 40% of the customer files reviewed, the Company did not take the steps necessary to meet its customer identification and verification obligations. For instance, with regards to one customer, the Company did not contain any corporate registry documents to identify and verify the corporate customer. Nor did the Company obtain an address verification document for the BO. Moreover, with respect to another customer, the identification document of one of the BOs was invalid since it had expired prior to the date of onboarding of the said customer.

When determining the administrative measure to be imposed in this regard the Committee did note that a number of years had passed since the onboarding of these customers. Nonetheless, the Committee held that the Company was still in breach of its CDD obligations since the PMLFTR was enacted in 2008 and the subject persons' obligation to carry out CDD upon onboarding new customers was already encompassed therein. The Company was expected to comply and implement the obligations set out in the PMLFTR upon its coming into force.

In view of the above reasons, the Committee determined that the Company was in breach of its obligations under Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.2.1, 4.2.2 and 4.3 of the IPs.

#### Certification of Documentation



The Committee noted that in 20% of the customer files reviewed, the Company failed to obtain the certification of the BOs' identification and verification documents upon onboarding.

In this regard, the Committee made reference to Section 4.3.1.1 which stipulates that a certified copy of a document must be signed and dated by the certifier and is to include the certifier's: name and surname; address; contact details; and profession, designation or capacity. Subject persons are also required to conduct independent checks to verify the existence of the certifier and document these checks (e.g., checks on open media sources or professional registers).

For these reasons, the Committee determined that the Company was in breach of its obligations under Section 4.3.1.1 of the IPs.

#### Enhanced Due Diligence

The Committee noted that the corporate customer in question was assigned a medium risk rating, despite the fact that the customer's BO was a high-net worth individual. This required the Company to carry out enhanced due diligence (EDD) measures on an ongoing basis.

In effect, the information obtained by the Company on the customer's source of wealth (SOW) and anticipated level of activity that was to be undertaken throughout the business relationship was insufficient as it merely consisted of the customer's self-declaration, Bank references, and information on banking transactions received by an entity belonging to corporate customer's BO. The Committee pointed out that the mentioned documents were not sufficient so as to ascertain that the corporate customer was deriving its funds from legitimate sources. Further documents should have been analysed by the Company including the financial statements of the corporate customer and the companies owned by the high-net worth individual (i.e. the customer's BO).

In view of the above, the Committee determined that the Company was in breach of its obligations under Regulation 11(1) of the PMLFTR and Section 4.9 of the IPs for this one file.

#### Ongoing Monitoring

The Committee noted that with respect to 20% of the customer files reviewed, the Company had delayed the carrying out of periodic reviews by a considerable amount of time. For instance, in one customer file the first periodic review carried out was eight years following customer onboarding. The Committee remarked that the obligation to carry out ongoing monitoring has been in place since the enactment of the PMLFTR in 2008. Therefore, the Company was expected to ensure effective ongoing monitoring of its business relationships upon the coming into force of the obligation.

In view of the above, the Committee determined that the Company was in breach of its obligations under Regulation 7(1)(d) and 7(2)(b) of the PMLFTR and Sections 4.5.3 of the IPs.

#### Record Keeping

The Committee noted that the Company had failed to correctly record the onboarding dates of its customers. In this regard, it was observed that there were mismatches in the onboarding dates of the customers as different dates appeared on different documents (including due diligence documents and CRAs) hence making it difficult for the relevant authorities to determine which date is the actual

onboarding date of the customers. The Committee held that that such failure is further concerning as the relevant authorities, whilst conducting a compliance examination, cannot ascertain whether customer due diligence and a CRA were conducted at onboarding stage or whether there was a delay in the carrying out of these obligations.

For this reason, the Committee determined that the Company was in breach of its obligations under Regulation 13 of the PMLFTR.

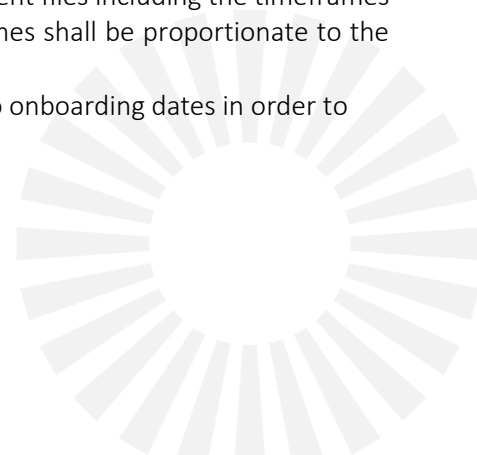
#### **ADMINISTRATIVE MEASURES TAKEN BY THE FIAU'S COMPLIANCE MONITORING COMMITTEE:**

After taking into consideration the above mentioned findings together with (i) the nature of the services and products offered by the Company; (ii) the size of the Company; (iii) the seriousness of the obligations breached and whether these were systematic in nature; and (iv) the impact that these breaches could potentially have on both the Company and the local financial system, the Committee, in terms of its powers under Regulation 21(4)(c) of the PMLFTR, decided to impose a Remediation Directive (Directive) with regards to the breaches identified in relation to:

- Regulation 5(1) of the PMLFTR and Sections 3.3 of the Implementing Procedures (IPs) Part I
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1, 3.5.3 and 8.1.3 of the IPs Part I
- Regulation 5(5)(a) of the PMLFTR and Section 3.4 of the IPs Part I
- Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.2.1, 4.2.2 and 4.3 of the IPs Part I
- Section 4.3.1.1 of the IPs Part I
- Regulation 11(1) of the PMLFTR and Section 4.9 of the IPs Part I
- Regulation 7(1)(d) and 7(2)(b) of the PMLFTR and Section 4.5.3 of the IPs Part I
- Regulation 13 of the PMLFTR

The aim of this Remediation Directive is to direct the subject person to take the necessary remedial actions to ensure that it understands the risks surrounding its operations and that it 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 this Directive, the Subject Person was requested to:

- Update the Company's BRA, clearly outlining how the Company has tackled the shortcomings identified by the Committee;
- Update and document its CRA measures that are to be based on the four risk pillars: customer risk, product/service risk, delivery/interface risk and geographical risks;
- Update its AML/CFT Manual and make sure that the Manual is implemented in practice;
- Update the CDD documentation in relation to the customer files in question in order to adequately identify and verify the corporate customers and their respective BOs;
- Obtain and hold on file the relative certifications with respect to the identification and verification documents of the corporate customers' BOs with respect to the customer files in question;
- Obtain and hold on file information and supporting documentation in relation to the Source of Wealth and Source of Funds of the high-risk corporate customer and its BO in order to evidence that EDD is being carried out;
- Document the procedure in relation to periodic reviews of its client files including the timeframes within which such reviews are to be conducted. These timeframes shall be proportionate to the level of risk posed by the customers;
- Ensure that it centralises its records, especially when it comes to onboarding dates in order to not have any discrepancies in the information in its files.



In the event that the Company falls short of its obligations in terms of this Directive, the Committee will be informed of this default. This could result in the possibility of action being taken, including the potential imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21 of the PMLFTR.

### Key Takeaways

- The carrying out of a comprehensive and approved BRA is essential for subject persons to combat ML/FT risks sufficiently. The BRA is expected to factor in the four (4) risk pillars, these being, customer risk, geographical risk, product/service/transactional risk, and interface risk. A BRA should also carry out a quantitative and qualitative risk assessment of the risk factors to which the Subject Person is exposed to. Subject persons are also expected to assess the inherent risk which depends on the identification of the existent threats and vulnerabilities, the likelihood of these threats and vulnerabilities to materialise and the impact they would have if they were to actually materialise.
- Subject persons should keep in mind that the CRA is one of the pillars of a sound AML/CFT compliance program. The CRA is necessary both for determining the level of due diligence required to build comprehensive customer profiles, as well as for ascertaining the degree of on-going monitoring necessary. Therefore, the failure to conduct an adequate CRA has serious and widespread repercussions. Furthermore, given that risk is dynamic, it is important that customer risk assessments are reviewed from time to time. The level of detail of a CRA is to reflect the complexity of the business relationship being engaged in. The more complex the customer and the relationship, the more thorough the details required to assess it need to be, in order to ensure a comprehensive risk understanding.
- Subject persons are required to identify the beneficial owner, where applicable, and to take reasonable measures to verify the identity of the same. In the case of a customer being a body corporate, subject persons are also required to take reasonable measures to understand their customer's ownership and control structure.
- High-net-worth individuals present elements of higher risk. Consequently, a subject person should consider whether it should implement EDD measures by obtaining supporting documentation on the customer's profile as well as conducting enhanced scrutiny to ensure that the business activity remains within the declared anticipated level and nature of the business relationship and that the customer/BO's funds are being generated from legitimate sources.
- The onboarding date of a customer is necessary for the FIAU to understand when a business relationship has commenced and thus, when AML/CFT obligations should have been conducted or started to be conducted. It is therefore vital for the subject person to retain on file the date when a customer has been onboarded and that there are no inconsistencies in between the dates it holds so that it can clearly demonstrate that it conducted a CRA and CDD obligations on time.

17 November 2023

