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 (the 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 measures and is not a reproduction of the actual decision.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

5 June 2025

RELEVANT ACTIVITY CARRIED OUT:

Collective Investment Scheme

SUPERVISORY ACTION:

Off-site compliance examination carried out in January 2022

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Remediation Directive in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (the PMLFTR)

LEGAL PROVISIONS BREACHED:

- Regulation 5(5)(a)(i) of the PMLFTR and Section 3.5 of the FIAU Implementing Procedures – Part I (the IPs)
- Section 6 of the IPs
- Regulation 7(1)(a) of the PMLFTR and Section 4.3 of the IPs
- Regulation 10(1) of the PMLFTR and Section 4.8.1 of the IPs

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

<u>Customer Risk Assessment (CRA) – breach of Regulation 5(5)(a)(i) of the PMLFTR and Section 3.5 of the IPs</u>

During the compliance examination, various deficiencies were identified in relation to the CRA methodology adopted by the Company. Notably, the risk options set out within the CRA were found to be overly generic, failing to take into account factors such as client type, size, sector, and expected investment size. Lastly, it transpired that the CRA primarily focused on customer and geographical risks, while neglecting other important risk factors, these including product, service and transaction risk, as well as delivery channel risk. However, even in the case of geographical risk, the risk assessment was deemed to be insufficient, as the analysis for natural persons only factored in their country of residence and jurisdictional connections, not their nationality and country of birth.

It was further revealed that, for over 30% of the customer files reviewed comprising of regulated entities, the Company automatically assigned a low risk rating and applied simplified due diligence (SDD) measures without first carrying out a formal CRA to determine whether such an approach was indeed warranted.

Notwithstanding the above, the Committee positively acknowledged that, following the compliance examination, the Company started making certain enhancements to its CRA methodology, with a particular focus on refining the risk options included within the CRA.

Outsourcing – breach of Section 6 of the IPs

According to the compliance examination report, although the Company has an outsourcing agreement with its Fund Administrator, it does not adequately monitor the outsourced AML/CFT measures and procedures. Furthermore, it was noted that the Company did not provide evidence of a risk assessment being conducted before this outsourcing arrangement was entered into, with the Committee confirming that the ML/FT risks associated with the proposed outsourcing were indeed not appropriately evaluated. Lastly, deficiencies were also identified in the quarterly reporting made by the Company's Money Laundering Reporting Officer (MLRO) to the Board of Directors, as the reports submitted did not include any information or evidence regarding the monitoring or testing of the outsourced activities.

Despite these failings, positive consideration was given by the Committee to the fact that, post-compliance examination, the Company sought to address the gap in relation to the monitoring of the outsourced AML/CFT measures and procedures by introducing compliance monitoring plan reporting as part of future Board meetings.

Customer Due Dilligence (CDD) – breach of Regulation 7(1)(a) of the PMLFTR and Section 4.3 of the IPs

The compliance examination report highlighted that the Company failed to correctly identify and verify the actual end client with which the business relationship was ultimately being established in almost 10% of the customer files reviewed, erroneously considering other related third parties, such as the custodian or parent company, as the customer instead.

Simplified Due Dilligence (SDD) – breach of Regulation 10(1) of the PMLFTR and Section 4.8.1 of the IPs

During the compliance examination, it emerged that the Company neglected to perform the necessary checks on customers consisting of regulated or listed entities carrying out relevant financial business, as required under Section 4.8.1 of the IPs, to determine whether the application of SDD was permissible. These checks should have included conducting background checks on the customer entity, reviewing publicly available adverse regulatory or supervisory information, obtaining evidence of the customer's authorisation to conduct financial or banking business, and understanding the activities undertaken by the client. In total, this shortcoming was identified in almost 40% of the customer files reviewed.

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

In view of the breaches identified, the Committee proceeded to serve the Company with a Remediation Directive in terms of Regulation 21(4)(c) of the PMLFTR. The aim of this administrative measure is to direct the Company to take the required remedial actions to ensure that it has a sound understanding of the risks surrounding its operations and has implemented sufficient controls to mitigate such identified risks.

In reaching its decision regarding the administrative measures to impose, the Committee took into consideration all the information made available by the Company, both during the compliance examination, as well as through its representations. The Committee also considered the importance of the AML/CFT obligations that the Company has breached, together with the seriousness of the findings and their material impact. Furthermore, the Committee took into account the nature, size and operations of the Company, and how the services it rendered and the AML/CFT controls in place may have impacted

the local jurisdiction as a whole. In addition, the Committee factored in the level of cooperation exhibited by the Company throughout the whole process, and the overall regard that the Company has towards its obligations. The Committee also took note of the Company's commitment towards updating and enhancing specific AML/CFT processes, as well as the remedial actions that it has indicated are either underway or already implemented. Lastly, the Committee ensured that the administrative measure imposed is effective, dissuasive, and proportionate to the identified failures and the perceived ML/FT risks.

The main purpose of the aforementioned Directive is for the FIAU to ascertain that the Company enhances its AML/CFT safeguards and undertakes the requisite remedial actions to attain full compliance with its AML/CFT legal obligations emanating from the PMLFTR and the IPs issued thereunder. The Company is being directed to remediate the identified breaches by implementing a number of remedial actions, including but not limited to the following:

- Implement a robust CRA methodology that adequately addresses all four risk pillars, i.e. customer risk, geographical risk, product, service and transaction risk, as well as delivery channels/interface risk, incorporating sufficient considerations and relevant risk indicators to satisfy regulatory requirements and rectify the shortcomings identified in relation to such methodology. The Company is also to ensure that customers comprising of regulated or listed entities are still subjected to a standard and complete CRA process.

- Ensure that the outsourcing arrangement with the Fund Administrator is effectively monitored and tested, this to that the outsourced AML/CFT measures and procedures are carried out as required by law and in accordance with the Company's own policies and procedures.

- Ascertain that, in all instances, the Company identifies and verifies the actual end customer with which the business relationship is ultimately being established. The Company is also required to remediate all customer files in which CDD shortcomings were identified during the compliance examination.

- In the case of customers carrying out relevant financial business, to make sure that SDD measures are only applied after conducting the necessary background checks, as stipulated in Section 4.8.1 of the IPs. The Company is also expected to remediate all customer files in which SDD shortcomings were identified during the compliance examination.

The Directive served on the Company shall ascertain that sufficient and tangible progress is achieved on the adoption and implementation of all the procedures and measures referred to above. In the event that the requested information and/or supporting documentation are not made available within the stipulated timeframes, or the Company falls short of its obligations in terms of this Directive, the Company's default will be communicated to the Committee for its eventual actions, including the possibility of the imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21(1) of the PMLFTR.

Key Takeaways

- An integral component of any robust CRA methodology is the comprehensive assessment each of the four risk pillars. Indeed, the CRA should clearly reflect all relevant factors and considerations that had an impact on a customer's risk score and corresponding risk rating. It is essential that each and every client undergoes a formal risk assessment prior to the establishment of the business relationship or the execution of an occasional transaction. This requirement applies equally to all customer types, including those that are generally perceived to carry a lower inherent risk level, such as regulated or listed entities.

- In cases involving customers with which contact has been lost, i.e., dormant clients, the associated risk is usually negligible, provided such clients remain inactive and no further transactions are undertaken, or services are offered. However, should a customer become active again, subject persons must ensure that appropriate controls and measures are in place to promptly re-assess the client, which includes the immediate completion of a refreshed CRA and the assignment of an updated risk rating.

- AML controls are only as strong as their weakest link, including those relating to outsourced activities. As stipulated in Section 6.2 of the IPs, subject persons are obligated to effectively monitor the outsourced AML/CFT measures and procedures, this to ensure that these are being carried out as required by law and in accordance with the respective subject person's own policies and procedures. This can be achieved through the submission of periodical reports by the outsourced third party, spot checks, and requests for CDD information on specific customers.

- In all instances, the subject person must ensure that the individual or entity identified as the customer is the actual end client with which the business relationship is ultimately being established, and not any other related parties, such as a parent company or other entities within the group. Therefore, it is crucial that all relevant AML/CFT requirements, including the collection of CDD documentation, are fulfilled in relation to such end customer.

- With specific reference to customers carrying out relevant financial business, in determining whether SDD measures should be applied, the subject person should carry out a number of background checks. Such checks are outlined in Section 4.8.1 of the IPs and entail the following:
  - Checking for any publicly available adverse regulatory or supervisory information;
  - Obtaining evidence that the customer institution is licensed or authorised to conduct financial and/or banking business;
  - Gaining an understanding of the activities that customer is undertaking, including the products and services offered, as well as its client base; and
  - Determining whether the customer applies robust and risk-sensitive CDD measures to its own clients and, where applicable, to their beneficial owners.

5 June 2025