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 penalties established by the Board of Governors of the FIAU.

This 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:

28 December 2022

RELEVANT ACTIVITY CARRIED OUT:

Credit Institution

SUPERVISORY ACTION:

Onsite Compliance Review carried out in 2019.

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €27,531, a Reprimand and a Follow up Directive in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 5(5)(a) of the PMLFTR and Sections 3.5 and 8.1.3 the Implementing Procedures (IPs)
- Regulation 7(1)(a) and Sections 4.3.1 and 4.3.2 of the IPs
- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs
- Regulation 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs
- Regulations 7(1)(d) and 7(2)(b) of the PMLFTR and Section 4.5.1 of the IPs

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Customer Risk Assessment (CRA) - Regulation 5(5)(a) of the PMLFTR and Sections 3.5 and 8.1.3 of the IPs

The compliance examination identified shortcomings in the Bank's CRA methodology, particularly in adequately documenting the rationale behind the final attributed customer risk rating. This since, among others, the Bank failed to distinguish between the different types of products/services offered and their respective ML/FT risks. Also, the CRA failed to take into consideration the origin of the customers exposure to a particular jurisdiction, e.g., whether the customer shall be receiving/sending funds from/to a particular jurisdiction, is a national/ resident of such jurisdiction or otherwise. Similarly, the Bank's CRA was expected to take into account other considerations, such as and not limited to: any adverse media, origin of customers funding, interaction with customer, transparency level demonstrated by the customer and where applicable the level of complexity behind a corporate customer.

Notwithstanding the above, to substantiate such deficiency, only a couple of examples were identified from the sample reviewed during the examination. Hence, despite the Bank's CRA methodology lacking rationale behind the attributed rating, it appears that the Bank still managed to understand the ML/FT risk exposure emanating from its customers. It was also noted that the Bank has since the examination revamped its CRA methodology and proceeded to update all its client files accordingly.

However, in view of the fact that the Bank failed to have in place an adequate CRA methodology for a substantial period of time, it was found in breach of Regulation 5(5)(a) of the PMLFTR and Sections 3.5 and 8.1.3 of the IPs.

Identification & Verification - Regulations 7(1)(a) of the PMLFTR and 4.3.1 and 4.3.2 of the IPs

In two files, the documents collected to identify and verify the customers were not properly certified in line with the AML obligations imposed at law. However, it was also acknowledged that the Bank has since commenced a review on both customers to ensure it duly remediates its position.

In another file, it was noted that the director of the Bank certified the documents required to verify this customer. Hence, the customer's details were not deemed as being independently verified as required in terms of its AML obligations. Here again, it was also acknowledged that the Bank has initiated a review to remediate its position on this file too.

In view of the above the Bank was found in breach of its obligations in terms of Regulations 7(1)(a) of the PMLFTR and 4.3.1 and 4.3.2 of the IPs.

Purpose and Intended Nature - Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs

During the compliance review, shortcomings were identified in the Bank's ability to establish the Source of Wealth (SoW) and Source of Funds (SoF) of some of its customers, this as required to ensure it maintains a comprehensive customer risk profile. In some files, the customers' SoW was either not collected or else the Bank relied on generic phrases which still failed to account for the origin of the accumulated wealth. Similarly, when collecting the SoF of some of its customers, either no information was provided, or such information was considered generic. As an example:

- In one file, the information collected by the Bank to explain the customer SoW was 'salary', this without the Bank providing any explanation of the customer's employment, approximate salary amount or any other information to substantiate the customers origin of wealth. Similarly in another file, the Bank merely accepted the customer's statement that wealth originated through 'income', this without obtaining any additional explanations/ documentation to substantiate such origin of wealth.

- The SoW & SoF of another customer, being a minor, was said to originate from the customer's parent. The Bank held at hand a bank statement from a local bank with whom investment was made illustrating a fixed term deposit maturity reminder addressed to the customer (minor) amounting to approximately £100K. Another document collected by the Bank stated that the customer's parent had obtained funds through investments, however no further information on the respective investments was provided. Hence, the said documents were deemed as not providing sufficient rationale behind the source of the customer's wealth and funding, rather than that it originates from her parent. Despite collecting the bank statement, the Bank held no knowledge on how the parent of the customer had acquired the respective wealth required to make such investment and was not able to have reasonable assurance that such wealth was accumulated through legitimate means. Also, given that the customer was a minor, he/she is fully reliant on the parent to fund the account, hence the Bank should have ensured to collect information/ documentation to account for the parent's SoW and SoF which are to be used in funding the child's account.

In view of the above-mentioned shortcomings, the Bank was found to have breached its legal obligations in terms of 7(1)(c) of the PMLFTR and Section 4.4 of the IPs.

Politically Exposed Persons (PEPs)- Regulation 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs

The enhanced due diligence (EDD) measure/s required to be taken by the Bank when dealing with PEPs where not always being adhered to. This since, from a sample of files reviewed during the examination, it became evident that the Bank, in some instances, failed to undertake EDD measures despite being aware of the PEP involvement associated with its customer. For example:

- Despite that the customer in one file had not been a PEP at the time of onboarding, it became evident to the Bank that such customer became a PEP 20 months after the relationship had been established. Hence, while acknowledging that EDD was not required at the time of onboarding, the Bank had an obligation to conduct EDD on the customer as soon as it became aware of the customer's PEP involvement. Instead, the Bank initiated a review of such customer over 2 years after being aware of the customer's PEP association. Hence, for a substantial period of time, the Bank failed to mitigate the ML/FT risk exposure from dealing with a PEP.

In view of the above-mentioned shortcomings, the Bank was found in breach of Regulation 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs.

Ongoing Monitoring - Regulations 7(1)(d) and 7(2)(b) of the PMLFTR and Section 4.5.1 of the IPs

As per the Bank's policies and in line with the AML/CFT obligation imposed at law, the Bank's customers are subject to a periodic review, this depending on the risk nature of their profile. However, the examination identified one file for which the customer had not been reviewed within the stipulated time period in line with the Bank's AML policy. It was also acknowledged that as part of the Bank's ongoing review process, this file would be reviewed and updated with the required documentation.

In view of the above, the Bank was found in breach of their obligations at law under Regulations 7(1)(d) and 7(2)(b) of the PMLFTR and Section 4.5.1 of the IPs.

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

After taking into consideration the abovementioned breaches by the Bank, the Committee decided to impose an administrative penalty of twenty-seven thousand five hundred thirty-one euro (€27,531) with regards to the breaches identified in relation to:

- Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs
- Regulation 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs

In addition to the above, the following breaches were considered to be minor in nature, therefore the Committee concluded that a reprimand shall be imposed in relation to:

- Regulation 7(1)(a) and Sections 4.3.1 and 4.3.2 of the IPs
- Regulations 7(1)(d) and 7(2)(b) of the PMLFTR and Section 4.5.1 of the IPs

The Committee positively acknowledged the actions already taken by the Bank and the actions planned to be taken in order to remediate the failures identified during the compliance review. Hence, to ensure that the Bank's remediation is adhered to, the Committee also served the Bank with a Follow-Up Directive in terms of its powers under Regulation 21(4)(c) of the PMLFTR, this in relation to the following breaches:

- Regulation 5(5)(a) of the PMLFTR and Sections 3.5 and 8.1.3 the IPs
- Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs
- Regulation 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs

The aim of the Follow-up Directive is for the FIAU to ensure that the Bank enhances its AML/CFT safeguards and that it becomes fully compliant with the obligations imposed in terms of the PMLFTR and the FIAU's IPs, as well as perform any required follow-up measures in relation to the Bank's adherence to its AML/CFT legal obligations. In virtue of this Directive, the Bank is required to make available an Action Plan indicating the remedial actions that it has carried out and implemented since the compliance examination, together with remedial actions which are expected to be carried out to ensure compliance following the identified breaches, this including but not limited to:

- Documented explanation of the remediation undertaken/ planned to be taken in relation to the Bank's CRA methodology, this mainly through the implementation of the new CRA methodology.
- Update on the Bank's measures in relation to obtaining information and documentation on the purpose and intended nature of the business relationship, including SoW and SoF of its customers.
- Update on the Bank's measures undertaken in relation to conducting EDD on PEPs.
- Where the specific customer relationships found in breach are still active, the Bank is also required to update the same to be in line with its legal obligation.

In determining the appropriate administrative measures to impose, the Committee took into consideration the representations submitted by the Subject Person, together with the remedial action that the Subject Person had already started to implement, the nature and size of the Subject Person's operations, the overall impact, actual and potential, of the AML/CFT shortcomings identified vis-à-vis the Subject Person's own operations and the local jurisdiction. The level of seriousness of the breaches identified, together with their occurrence were also taken into consideration by the Committee in determining the administrative measures imposed.

Finally, the Subject Person has also been duly informed that in the event that they fail to provide the above-mentioned action plan and available supporting documentation within the specified deadline, this 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 of the PMLFTR.

The administrative penalty hereby 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 Take aways:

- The carrying out of a comprehensive CRA is essential for the understanding of the risks posed by customers and the level of controls necessary to manage and mitigate the same. Equally important is the adequacy of the records in place to understand how the risk has been derived and how the risk factors identified are contributed to the residual risk and the extent to which the controls manage such risks. This will enable both the understanding of the risks in greater detail but also understand how changes in particular circumstances during the business relationship effect the overall risks and level of controls necessary. The consideration of all risk factors that are specific to a subject person's operations, business model, customer targets and geographical exposure will enable a true understanding of risks. If this is not the case, the risk assessment risks being distorted and incomplete, resulting in certain risk exposures not being identified and more worryingly not being managed.

- Identification of the customer, and the verification of the customer's identity on the basis of documents, data or information is to be obtained from a reliable and independent source. The term "independent" should be interpreted to mean a source that is independent of the customer (therefore, this would exclude a declaration made by a customer). A source is reliable if it is reputable and is trusted by the subject person to provide extensive and sufficiently accurate data or information to verify the customer's identity.

- When the identification documentation obtained is required to be certified, subject persons are reminded of their obligation to ensure that certified documents are to include a written statement to the effect that:
    - the document certified is a true copy of the original document;
    - the original document has been seen and verified by the certifier; and
    - the photo visible on the document (where applicable) is a true likeness of the customer.

  Also, the certified copy 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). Subject persons must exercise caution when accepting certified copy documents, especially when these documents originate from a country or territory perceived to represent a higher risk than usual.

- Where the customer is an individual and a third party pays off the customer's dues, subject persons may be required to collect the source of wealth of such third party[1] as well as the rationale for this. In such circumstance, the subject person must consider this factor within its customer risk assessment, to determine the level of ML/FT risk presented by the relationship or occasional transaction. It is also necessary to establish:

    - whether there is a reasonable explanation for the third party to be providing the funds; and
    - based on the possible risks presented, obtain information and documentation to clarify and verify the source of wealth of the third party. The weaker the connection between the customer and the third party, the more one needs to query the third party's source of wealth, especially if the amounts are quite substantial.

  It may very well be acceptable for a parent to set aside some funds for a child and have them placed in the child's name, but one must verify the parental source of wealth to ensure that the funds used are legitimate. When no tie can be established which would reasonably explain why the third party is willing to make funds available for the benefit of the customer, the ML/FT risk has to be considered as particularly high and therefore the level of information and documentation required needs to be increased and its verification more thorough.

28 December 2022

[1] https://fiaumalta.org/wp-content/uploads/2022/07/Guidance-Note-On-obtaining-Source-of-Wealth-Information-related-to-Parties-other-than-the-Customer.pdf