Administrative Measure Publication Notice

This Notice is being published by the Financial Intelligence Analysis Unit (the 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 measure and is not a reproduction of the actual decision.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

28 November 2022

SUBJECT PERSON:

HSBC Bank Malta plc

RELEVANT ACTIVITY CARRIED OUT:

Credit Institution

SUPERVISORY ACTION:

Offsite compliance review carried out between 3 July 2020 and 24 August 2020.

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of €82,966, a Follow-Up Directive and a Reprimand.

LEGAL PROVISIONS BREACHED:

- Regulations 7(1)(b) and 7(3) of the PMLFTR and Section 4.3 of the IPs
- Regulations 7(5) and 8(1) of the PMLFTR and Section 4.6.1 of the IPs
- Regulations 11(1)(b) and 11(5) of the PMLFTR and Section 4.9 of the IPs
- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

<u>Identification and Verification – Breach of Regulations 7(1)(b) and 7(3) of the PMLFTR and Section 4.3 of the IPs:</u>

For three (3) customer files, it was observed that at the time of onboarding, the Bank had failed to collect the necessary documents to verify the identity or address of the beneficial owners (BOs)/senior managing officials. Similarly, for four (4) customer files, the Bank had failed at the onboarding stage to carry out the verification of the agents/authorised signatories involved. Therefore, the Bank was found to be in breach of Regulations 7(1)(b) and 7(3) of the PMLFTR and Section 4.3 of the IPs. However, given that the Bank had already remediated these shortcomings prior to the compliance examination, and taking into consideration the fact that such inadequacies were identified in a relatively low number of files, the Committee deemed this breach to be minor in nature, and proceeded to impose a Reprimand and Follow-Up Directive on the Bank.

Timing of Customer Due Diligence (CDD) – Breach of Regulations 7(5) and 8(1) of the PMLFTR and Section 4.6.1 of the IPs:

The compliance examination report revealed that in certain instances, the verification of the identity of the agents involved in the business relationship was carried out late. This observation was noted for two (2) customer files.

Since the Bank failed to carry out such verification prior to the establishment of the business relationship, the Committee found the Bank to be in beach of Regulations 7(5) and 8(1) of the PMLFTR and Section 4.6.1 of the IPs. Whilst acknowledging that this finding is minor in nature and that the Bank took the necessary remedial actions to rectify the shortcomings identified, the Committee reiterated the importance of carrying out the necessary CDD measures when establishing a business relationship or prior to carrying out an occasional transaction. Furthermore, the Committee emphasised that going forward, the Bank should ensure that it always adheres to the obligations emanating from the PMLFTR and the IPs, which includes ascertaining that the timing of the CDD process is in line with the stipulated requirements.

Enhanced Due Diligence (EDD) – Breach of Regulations 11(1)(b) and 11(5) of the PMLFTR and Section 4.9 of the IPs:

For one corporate customer, the Committee noted that although information on the source of wealth (SOW) was collected, this was not sufficiently verified. It was noted that the BOs of the customer in question were Politically Exposed Persons (PEPs). The customer also had a complex ownership structure, including trusts and foundations. In addition, over a period of less than two years, the customer affected numerous transactions running into the millions. However, despite the high-risk elements present, the Bank solely relied on reliable public sources as a confirmation and source of information of the BOs' SOW.

In its representations, the Bank argued that information on the SOW of the customer's BOs had been obtained and included in the onboarding Know Your Customer (KYC) forms. The main SOW of the BOs was attributed to the sale of an international company for an amount in the range of tens of billions of dollars. Validation of the SOW information was obtained from a prominent and reliable public source, which was deemed by the Bank as being sufficient given that this source is publicly known, and that the BOs are officially listed on the same source due to their wealth generation. Moreover, the Bank indicated that additional checks and controls were also performed, which included conducting an onsite client visitation.

After taking into consideration the above finding together with the representations submitted by the Bank, the Committee emphasised that since this business relationship represents a higher level of ML/FT risk, and there are PEPs involved, the Bank should have undertaken more rigorous Enhanced Due Diligence (EDD) measures pertaining to SOW verification, and not simply relied on information obtained from public sources. While it is possible to rely on credible and reliable public sources, this must always be considered within the context of the risks presented (actual or potential) by the business relationship being established. In the case of this customer, the Committee stated that to sufficiently verify the information on the BOs' SOW provided in the onboarding KYC forms, the Bank should have, in addition to obtaining information from public sources, also collected additional information such as the financial statements of the company cited as being the main source of the BOs' SOW or an independent valuation of the same. Given the BOs' PEP status, the collection of such documentation becomes even more important.

In view of the Bank's failure to carry out adequate EDD measures that would address the higher ML/FT risk the customer was exposing the Bank to, the Committee found the Bank to be in breach of its obligations in terms of Regulations 11(1)(b) and 11(5) of the PMLFTR and Section 4.9 of the IPs.

Ongoing Monitoring – Breach of Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs:

Finding 1: Failure to monitor whether transaction patterns are in line with the customer's profile

Based on the review of the customers' transactional activity, it was noted that for some business relationships, there were certain discrepancies between the transactional activity and the information held by the Bank vis-à-vis such customers' risk profiles. Indeed, the Bank's transaction monitoring system does not adequately monitor transactions based on expected customer activity declared at onboarding, but rather, only takes into consideration recent activity. This means that the system does not comprehensively trigger alerts when there are mismatches between the transactions processed and the customer's business and risk profile, including information gathered about the purpose and intended nature of the business relationship. On this point, the Committee highlighted the importance of monitoring the transactional activity of individual customer segments which make economic sense. Such customer segments should comprise of a cluster of customer profiles which are relatively similar in nature in terms of characteristics and risk rating. While the Committee acknowledged that the Bank has in place transaction monitoring rules and thresholds which vary depending on the customer segment involved, the adequacy of the same was at times questioned.

By way of example, in the case of one specific customer file, it was observed that although the expected monthly turnover was approximately €15,000, the total amount credited to the customer's account during a particular month was more than ten times the expected monthly turnover, with over €100,000 being credited in just one day. When requested to provide an explanation regarding this inconsistency, the Bank stated that the thresholds in place were not violated, and therefore, no alert had been generated for this transaction. The Bank also submitted that as per revised KYC information obtained, the customer's projected annual turnover was substantially increased to circa €700,000. Consequently, the customer's actual annual turnover of roughly €500,000 was in line with this projected figure. The Committee obtained a copy of the customer's financial statements and, from its review thereof, noted that that the increase in projected annual turnover was indeed justified; however, no documentary evidence was held on file to support this increase.

Regarding the aforesaid mismatch between the transactions processed and the customer's profile, the Committee highlighted that this should have been flagged by the Bank's transaction monitoring system, and the sudden deposit spikes should have been reviewed further if necessary. In this regard, the Committee held that the Bank's transaction monitoring system does not completely and effectively capture sudden deposit spikes or deviations from the information provided by the customer on the expected level and nature of activity.

Furthermore, the Committee reiterated that certain thresholds set at the time when the transactions were affected were deemed to be too wide. However, the Committee also acknowledged that thresholds were subsequently revised, and through the Follow-Up Directive imposed on the Bank, the FIAU shall ensure that such revised thresholds are indeed adequate.

The Committee commended the various systems and controls that the Bank has in place to monitor the transactional activity of its customers. However, it stressed the importance of ensuring that transactions undertaken throughout the course of the business relationship are consistent with the subject person's knowledge of the customer, as well as its business and risk profile. Through the monitoring of customer transactions, subject persons should be in a better position to identify unusual behaviour or transactions that diverge from the customer's expected or known transactional pattern.

Based on these considerations, the Committee concluded that the Bank failed to ensure that the transactions undertaken are consistent with its knowledge of the customer and its business and risk profile, and thus found the Bank to be in breach of Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs.

Finding 2: High monetary thresholds applied

During the compliance examination, it was noted that the monetary thresholds for large value transactions were too high to allow the Bank to effectively monitor the same. The compliance examination report referred to various high value transactions pertaining to one customer file at times reaching €800,000 which were not alerted by the Bank's transaction monitoring system.

By means of its representations, the Bank explained that although the rule in place at the time did not trigger any alerts relative to the transactions pertaining to this customer, following the performance of its tuning exercise and introduction of its revised thresholds, an alert would have now been triggered by the same rule. The Bank also stated that other controls in place did lead the Bank to scrutinise the transactions involved. As part of its representations, the Bank provided a risk management review report which provided information regarding the financial crime risk considerations considered when assessing the customer. However, the Committee noted that the document did not make specific reference to the transactions in question, and failed to provide evidence that such transactions were indeed scrutinised by the Bank.

The Committee emphasised that the previously established monetary thresholds to monitor large transactions passing through the accounts within a specific time period were too high, thus increasing the risk that certain large and anomalous transactions were not being captured and adequately scrutinised by the Bank. This risk would have been further exacerbated should there have been instances where such transactions were not alerted by other rules. However, the Committee acknowledged the remedial action undertaken by the Bank, whereby a tuning exercise was conducted to revise the thresholds utilised. Additionally, the Committee commended the fact that such tuning was not performed as a one-off event, but is carried out on a periodic basis.

Taking all facts into consideration, the Committee found the Bank to be in breach of Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs.

Finding 3: No or insufficient information/documentation provided by the Bank on some selected transactions

During the compliance examination, the FIAU Officials reviewed numerous transactions pertaining to several customer files. Subsequently, the Bank was requested to provide further information and/or documentation on a selected number of such transactions. However, for one customer file, the Committee noted that the Bank failed to provide a copy of the invoices pertaining to a payment exceeding €2 million. Through its representations, the Bank provided more detailed information regarding the business operations of the customer in question, noting that since the particular transaction was deemed to be in line with the customer's business and KYC, no further action was taken by the Bank.

In taking the decision for this file, the Committee noted that although the Bank's representations provided more context regarding the transaction in question, neither the invoices referred to in the compliance examination report nor any other supporting documentation were included as part of the representations. For this reason, the rationale for the payment received could not be further substantiated. In addition, based on the review of the customer's transactions list, the Committee observed that the value of the transaction in question is significantly larger when compared to the value of the other transactions that were passing through the accounts.

In view of the above, the Committee found the Bank to be in breach of Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs.

Finding 4: No link between the alerted transaction and the documentation obtained in support of the transaction

The compliance examination report revealed that the supporting documentation obtained in relation to two alerted transactions was not specifically related to these transactions. In connection with both alerts (amounts: approximately €50,000 and €700,000), the Bank submitted that the requested information pertaining to the respective transactions was made available during the compliance examination. However, it was noted that the documentation provided for the alerted transactions did not make specific reference to the transactions in question. Based on these considerations, the Committee found the Bank to be in breach of Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs.

Finding 5: No pre-transaction monitoring carried out

The Committee noted that the Bank's pre-transaction monitoring is in relation to sanctions screening, and no further pre-transaction alerts are used, not even as an EDD measure for high-risk customers. Not conducting out pre-transaction monitoring may hinder the Bank's ability to effectively fulfil its obligations under Regulation 15(4) of the PMLFTR, which states that in situations where a subject person knows or suspects that a transaction is or may be related to proceeds of criminal activity or the funding of terrorism, the subject person will not carry out the transaction until it has informed the FIAU.

In its representations, the Bank stated that although its transaction monitoring system is based on post-transaction monitoring, it still carries out pre-transaction monitoring through various systems, procedures and controls, which include: (a.) its core banking system functionality, which allows for debit and credit transactions to be referred to the commercial manager before being executed; (b.) global trade and receivables finance business controls (e.g. checking of invoices, bills of lading and other documents, sanctions screening and KYC checks); and (c.) its credit applications process.

The Committee emphasised that although post-transaction monitoring is a very important and indispensable measure that is to be employed for transaction scrutiny purposes, the Bank should have also remained vigilant to monitor transactions in real time, especially when considering the high value and heightened risks associated with certain transactions the Bank was/is or may be involved in. The Committee positively acknowledged the above-mentioned core banking system functionality used by the Bank's commercial managers in high-risk scenarios, which allows for payments to be reviewed, and for further documentary evidence to be requested, prior to such payments being released. However, this process is not comprehensive and rather subjective because pre-transaction monitoring is only carried out if the commercial managers deem it necessary. Therefore, there is a risk that not all unusual or anomalous transactions are captured through this system, especially when considering the Bank's large customer base and the voluminous number of transactions that are affected daily. Likewise, high value transactions affected by non-high-risk customers may end up not being flagged.

The Committee stressed that it was not expecting the Bank to review all transactions in real time, but to have the measures in place to be able to better and more consistently flag high-risk transactions based on scenarios determined in line with the Bank's business model and customer base, as well as to capture high value transactions before these are allowed to pass.

In view of the above, the Committee held that the Bank had failed to have in place comprehensive measures for the carrying out of pre-transaction monitoring, and consequently found the Bank to be in breach of Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs.

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

After taking into consideration the aforementioned findings, the Committee decided to impose an administrative penalty of €82,966 regarding the breaches identified in relation to:

- Regulations 11(1)(b) and 11(5) of the PMLFTR and Section 4.9 of the IPs; and
- Regulation 7(2)(a) of the PMLFTR and Section 4.5.2 of the IPs.

The Committee also imposed a Reprimand with regard to the breaches identified in relation to Regulations 7(1)(b) and 7(3) of the PMLFTR and Section 4.3 of the IPs.

In addition to the above, in terms of its powers under Regulation 21(4)(c) of the PMLFTR, the FIAU also served the Bank with a Follow-up Directive. 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:

- Ascertaining that going forward, the timing of CDD measures is in line with the stipulated requirements, meaning that the identity of the customer, and where applicable, the beneficial owner, is always verified prior to the establishment of a business relationship.
- Obtaining an independent verification of the SOW of the BOs pertaining to the customer file found to be in breach of Regulations 11(1)(b) and 11(5) of the PMLFTR and Section 4.9 of the IPs.
- Providing a documented explanation of the remediation undertaken/planned to be undertaken to ensure that the deficiencies noted with the Bank's transaction monitoring system and related processes are rectified. The following should be provided:
    - More detailed information/documentation regarding the transaction monitoring tuning exercise that was carried out by the Bank, together with a list of the revised rules/thresholds per customer segment that were implemented and are currently in place, including effectiveness testing.
    - Information/documentation regarding the process the Bank has in place vis-à-vis the investigation and review of alerted transactions, including the types of checks carried out, the rationale for discounting and any escalation procedures.
    - Information/documentation regarding the pre-transaction monitoring procedures and measures currently applied by the Bank, as well as an explanation of any updates or enhancements that the Bank has made to its pre-transaction monitoring system following the completion of the compliance examination.

The Bank was informed that in the eventuality that the requested information and/or documentation would not be made available within the stipulated timeframes, the Bank's default will be communicated to the Committee for the possibility to take eventual action, including the potential imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21 of the PMLFTR.

When deciding on the administrative measure to impose and on the amount of any administrative penalty, the Committee has to ascertain itself that these are effective, dissuasive and proportionate to the seriousness of the failures identified.

In doing so, the Committee took into consideration the importance of the obligations that the Bank breached, together with the seriousness of the findings identified and their material impact. The Committee also considered whether the breaches identified could have led to the unintentional facilitation of ML/FT. It also considered the impact that the Bank's failures may have had on both its operations, as well as on the local jurisdiction and its financial system. The size and operations of the Bank, and it being a core banking institution in Malta, were also taken into account.

In its deliberations, the Committee also factored in the good level of cooperation exhibited by the Bank throughout the whole process as well as the constructive and positive dialogue had throughout the years, together with the regard that the Bank has shown towards its AML/CFT obligations. Furthermore, the Committee took into consideration the Bank's long-standing commitment towards enhancing and updating its AML/CFT processes to ensure compliance with its legal obligations, and the remedial actions that the Bank indicated it has already started to implement. The Committee also considered the Bank's continuous investment in its technical and human resources tasked with preventing/combating ML/FT.

Key take-aways

- If a business relationship represents a greater level of ML/FT risk, subject persons are expected to undertake EDD measures. Therefore, in high-risk scenarios such as those involving PEPs with exceptional wealth, subject persons should not solely rely on information obtained from public sources to verify the SOW/SOF, and should obtain independent verification of the information. Furthermore, such verification is also required in cases where the PEPs involved are well-known public figures who are officially listed on public sources due to their wealth generation.
- Through the monitoring of the business relationship, subject persons should be able to identify transactions or behaviours which are not consistent with the customer's business and risk profile. Carrying out effective scrutiny of transactions also facilitates the identification of any sudden deposit spikes or deviations from the information provided by the customer on the expected level and nature of activity. Hence, the presence of any unusual transactions should serve as a red flag or trigger event for the subject person to assess the situation and request additional information or documentation if required. The use of adequate customer segments is crucial to enable effective monitoring.
- To ensure that transactions are effectively scrutinised, subject persons are to have effective transaction scrutiny measures in place. Depending on the size and nature of the business, these may necessitate the implementation of a transaction monitoring system. Such system is to enable the generation of alerts based on scenarios which are established based on the subject person's business model, transactional history, and customer base. The introduction of such a transaction monitoring system should enable subject persons to identify any unusual or suspicious transactions. Depending on the robustness of the system adopted, subject persons can be in a better position to effectively monitor transactions both prior to their execution, as well as after they have taken place.
- Effective monitoring of transactional activity can be carried out through the analysis of transactions undertaken by different types of customer segments (e.g., cash intensive sectors, student accounts, unemployed individuals, etc.). Each customer segment should comprise of a cluster of customer profiles which are similar in nature in terms of characteristics and risk rating, and together make economic sense.
- If the subject person opts to utilise thresholds/parameters, these will be different for, and dependent on, each scenario and customer segment. If the monetary values of the thresholds set for specific scenarios and customer segments are too high, this may result in large and anomalous transactions not being captured.

- When a particular transaction is flagged, the subject person should ascertain that the transaction is reviewed, and if discounted, ensure that the rationale for closing the alert is duly documented. It is also essential that the reviewed is concluded within a reasonable timeframe.
- While greater emphasis is naturally placed on the monitoring of credit transactions (incoming funds) to obtain a more comprehensive understanding of where the funds are coming from, subject persons still need to ensure that debit transactions (outgoing funds) are also reviewed in cases where the payments being made are unusual, exceptionally high, or significantly diverge from the customer's typical transactional pattern as they may still be indicative of a change in the customer's known business and risk profile.
- Pre-transaction monitoring is indispensable to effectively monitor high-risk situations, particularly where there are large value or anomalous transactions, or transactions that significantly diverge from the expected level of activity. While it is not expected that all transactions are monitored a priori, high-risk transactions should be alerted and assessed before being processed.

5 December 2022