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.

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:

08 August 2022

SUBJECT PERSON:

Ferratum Bank P.L.C

RELEVANT ACTIVITY CARRIED OUT:

Credit Institution

SUPERVISORY ACTION:

On-site compliance review carried out between 2018 and 2019

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of €653,637

LEGAL PROVISIONS BREACHED:

- Regulation 5(1) of the PMLFTR.
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 4.1 of the IPs applicable at the time of the review.
- Regulation 7(1)(a) of the PMLFTR and Section 3.1.1.2 of the IPs applicable at the time of the review.
- Regulation 7(1)(c) of the PMLFTR and Section 3.1.4 of the IPs applicable at the time of the review.
- Regulations 11(5) and 11(8) of the PMLFTR and Section 3.5.3.1 of the IPs applicable at the time of the review.
- Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 3.1.5 of the IPs applicable at the time of the review.
- Regulation 15(3) of the PMLFTR.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

<u>Regulation 5(1) of the PMLFTR – The Business Risk Assessment (BRA):</u>

The compliance review revealed that the Bank's BRA had various shortcomings that were of high concern for two reasons:

1. The inherent risk was being assessed inadequately. For example, a particular product; low value loans, was risk assessed as 'low', despite the elevated financing of terrorism (FT) risks associated with this product. The Bank only took into consideration that this product involved low value funds

and that it had a low risk of money laundering (ML). The Bank also failed to consider other important areas such as the urgency to open a bank account and the risk of customers involved in sanctions or linked to adverse information. The geographical connection emanating from the place of remittance/receipt of funds was also not considered.

2. The controls in place were not being adequately assessed. A generic statement rather than a comprehensive assessment of controls was noted in the BRA. At times it was not even confirmed whether the mentioned controls were being implemented or otherwise.

The Bank's BRA was not comprehensive – the Bank had multiple assessments in place on the different products it was offering, which focused on the jurisdiction the product was being offered in. These assessments were not merged in one global assessment providing details of the inherent and residual risks and therefore could not be considered as a comprehensive BRA. Consequently, the assessment was not reflecting a clear picture of the threats and vulnerabilities of the Bank's business.

The Bank stated that its BRA was holistic and comprehensive and that the arguments put forward during the supervisory review were unpublished expectations by the MFSA and FIAU. The Committee rebutted this statement by underlining that the requirement to carry out a BRA has been in place since January 2018 when the PMLFTR was revised (vide Regulation 5(1)), furthermore a guidance paper was issued by the FIAU and MFSA in February 2018, providing more insight into this obligation.

Moreover, the assessments did not show the implementation and the effectiveness of the controls in place but included generic descriptions of measures to be implemented. The Bank tried to dismiss this requirement by referring to the abovementioned paper issued by the FIAU and MFSA, and it argued that this paper did not indicate that the BRA should contain a detailed list of such control measures. However, the Committee dismissed this statement noting the paper clearly indicated that control measures need to be evaluated for their effectiveness[1].

In view of this, the Members of the Committee determined that at the time of the compliance examination the Bank's shortcomings with regards to the BRA were serious and systematic, and concluded that the Bank was in breach of its obligations as envisaged under Regulation 5(1) of the PMLFTR.

<u>Regulation 5(5)(a)(ii) of the PMLFTR and Section 4.1 of the IPs applicable at the time of the review – The Customer Risk Assessment (CRA):</u>

<u>Finding 1: No CRA procedures prior to November 2018</u>

The compliance review revealed that the Bank did not have CRA procedures in place prior to November 2018. A broad review of all the Bank's customers was eventually carried out within a 24-hour period at the time when the Bank received notification of the compliance review. Yet, the CRA for all the mobile banking customers reviewed and the CRAs of almost all the EFDIS (savings and fixed deposits accounts) customers reviewed were not provided. The Bank explained that at the time when the mobile banking and EFDIS customers reviewed were onboarded, the obligation to have a documented CRA in place was not in force. However, the Committee could not agree with this statement, reminding the Bank that the obligation to carry out a CRA has been in place since 2008, by virtue of the PMLFTR, and that more detail as to the implementation of such risk assessments were explained in the FIAU's IPs which were first issued in 2011. The recording of the CRA in writing, has also been in place since August 2011.

The Committee also referred to the Annual Compliance Reports (ACRs) that the Bank had submitted from 2013 until 2017 where it indicated that CRAs which included the 4 main risk pillars were being conducted,

[1] Supervisory Guidance Paper on ML and TF Institutional/Business Risk Assessment, issued on 2 February 2018 - link to guidance paper

however, during the compliance review, it became evident that the Bank had made a false declaration to the FIAU.

Members of the Committee declared that having no CRA for approximately 6 years (from the time it was licensed until 2018) had serious and widespread repercussions, over understanding the customers' risks and applying effective controls to manage and mitigate the same.

Finding 2: Inadequate CRA methodology

The methodology of the CRA subsequently adopted by the Bank was not robust enough, and it led to an incorrect assessment of the Bank's customer risk. The compliance review revealed that the Bank applied a blanket solution to customers making use of loan products, whereby it assessed all these customers as 'low risk' on the basis that the product and the jurisdictions of the customers (EU countries) were considered as low risk. While it is possible to consider groups of customers or business relationships that share similar characteristics as presenting the same level of risk, if this grouping is logical and specific enough, it still requires a proper risk understanding and assessment of the different risk factors involved. In this case, the Bank did not factor in the risks that this product normally carries, such as the ease with which the loan is granted, which makes it more susceptible to FT risk. The Bank also did not factor in the rationale why a customer requested the loan, nor that the small value transactions involved fall below monitoring thresholds.

The officials performing the review also carried out a test on the Bank's CRA system and noted that with regards to the geographical risk, if one had to tick high-risk countries, the system did not rate their risk as high. Although the Bank indicated that transactions would be automatically blocked if these had to pass to or from these countries, this could not be confirmed at the time of the visit since the Officials identified transactions which had passed to/from jurisdictions that were included in the Bank's own jurisdiction 'blacklist'. Therefore, there was not a good level of controls implemented when it came to high-risk jurisdictions.

Another shortcoming noted during the compliance review was that none of the Bank's customers was rated as 'high-risk'. Although the Bank informed the Committee that high-risk customers fall outside of the risk appetite of the Bank and are not accepted, it only referred to PEPs and sanctioned individuals as carrying a high risk. The Committee stated that it is not only PEPs and sanctioned individuals that carry a high risk, but other factors can also elevate the risk to high, either at the start of the relationship or throughout. These would include, significant and unexplained movement of funds, high net worth individuals, material links to high-risk jurisdictions amongst others. The Committee reiterated that without an adequate CRA system in place, the Bank was not able to understand and determine the risk emanating from the business relationship.

In view of this, members of the Committee determined that the Bank had systematically breached its obligations as stipulated under Regulation 5(5)(a)(ii) of the PMLFTR and Section 4.1 of the IPs applicable at the time of the review[2].

Regulation 7(1)(a) of the PMLFTR and Section 3.1.1.2 of the IPs applicable at the time of the review – Customer Due Diligence

In one file, the copy of the identification document collected by the Bank had adhesive tape attached to the part where the residential address could be found. In other instances, the Committee noted how the documentation which could verify the identification details of the customers was not provided to the Officials during the compliance examination but was only submitted with the representations without evidence that this was obtained at onboarding. In view of this, it could not be confirmed whether the

[2] Currently Section 3.5 of the IPs

documentation was collected during the time of on-boarding or otherwise. Additionally, in another instance, basic identification details such as the date of birth of the customer, were only obtained after the customer was provided with the services (in this case, a loan).

However, the Committee noted that it was only in a limited number of cases where shortcomings in relation to the obligations to identify and verify the customers were observed. Consequently, the Committee determined that the Bank had minor breaches with regards to the obligations in terms of Regulation 7(1)(a) of the PMLFTR and Section 3.1.1.2 of the IPs applicable at the time of the compliance examination[3].

Regulation 7(1)(c) of the PMLFTR and Section 3.1.4 of the IPs applicable at the time of the review – Purpose and Intended Nature of the Business Relationship

Mobile Banking customers

The Bank was not collecting adequate and comprehensive information in relation to the purpose and intended nature of the business relationship, including information relating to the customer's source of wealth (SOW) and expected source of funds (SOF). Moreover, from the compliance examination it resulted that none of the mobile banking customers had information on the anticipated level and nature of the transactions, with the Bank rebutting this finding and stating that it was collecting the customer's income bracket and occupation. However, upon reviewing the information that the Bank was collecting, the Committee confirmed that the Bank was not obtaining information on the expected value and volume of the transactions that the customers would be undertaking. Additionally, in certain instances, the Bank did not even collect the customer's occupation or their expected SOF. Likewise, in other instances, the Bank only collected basic and generic information on the customer's occupation, such as 'businessman' or 'self-employed individual'. The Committee stressed that this information is not sufficient to establish a comprehensive customer profile, even when information on the value of the income would have been obtained.

It was also observed that no SOW information was collected for 96% of mobile banking customers reviewed. Upon reviewing the Bank's submissions, the Committee noted that the Bank did not appreciate the difference between SOW and expected SOF, as the information that the Bank claimed to have obtained for the SOW related more to the expected SOF. While it cannot be discounted that one's SOW will also be one's expected SOF, this cannot be taken for granted and a subject person should as a minimum always establish the customer's SOW and then ask if the funds that are to be used throughout the relationship are to be generated by the same business/activity/employment or if the source is different. In the latter case, the subject person would then have to obtain information, and if necessary, documentation on the expected SOF. It was also noted that, if a customer had other means generating his/her wealth, such as investments or inheritance, these means would not be featured in the profile since only one entry could be chosen by the customer when compiling the onboarding form. Additionally, the information obtained was also considered as basic and generic. For example, in one instance, the information that the Bank obtained for SOW indicated that the customer worked in 'delivery'. In view of this, the Committee determined that the Bank did not collect sufficient and adequate information on the purpose and intended nature of the business relationship for mobile banking customers.

Loan customers

The compliance examination also revealed that none of the loan customer files held information relating to the purpose and intended nature of the business relationship. Neither did the customer files hold information relating to the customer's occupation, SOW and expected SOF. The Committee took into consideration that although the rationale for taking a loan is quite self-explanatory (i.e., to help cover

[3] Currently Section 4.3.1 of the IPs

immediate cash needs since these were short term loans), the Bank was still expected to understand and determine the purpose for taking out such a loan (i.e., ascertain the actual need for a loan) and whether it makes sense for the customer to take a loan. Although the Bank informed the Committee that these loans were subject to a repayment schedule, the schedule was neither found on the customer file nor submitted with the Bank's representations. Therefore, the repayment frequencies could also not be understood.

While the Committee took into consideration that the Bank has since started a remediation exercise, it could not discard the fact that the Bank was in breach of its obligation until the time of the compliance examination.

EFDIS Customers

The Committee members noted that the information collected by the Bank with regards to the customer's occupation and expected SOF was very generic, with instances noted where the form only included that the customer was a 'worker' or an 'employee'. Likewise, no information with regards to the SOW and anticipated level and nature of the business activities was found in the loan files reviewed. Here again, the Committee remarked that the Bank had failed to understand the difference between the SOW and expected SOF. Thus, it was determined that the Bank was not ensuring that it collected information on the purpose and intended nature of the business relationship, and neither did it have a comprehensive customer risk profile.

Therefore, it was concluded that the Bank lacked appreciation of the importance to obtain sufficiently detailed information (and evidence when the risks posed require it) to understand and form a comprehensive customer business and risk profile. While taking note of the good actions taken by the Bank (such as for example remediating to ensure that the loans are repaid by the person who undertook the loan, and calculating the expected deposits using the customer's age and income, amongst others, as explained in the Bank's submissions), it was also observed that the Bank does not seem to be keen on appreciating the shortcomings in relation to the necessity to obtain information (and where necessary documentation) on the SOW, as well as comprehensive understanding of the expected SOF. This, particularly noticeable from the Bank's representations, confirming a lack of appreciation for obtaining such information.

In view of the fact that the Bank failed to collect comprehensive information on the purpose and intended nature of the business relationship, the Committee determined that the Bank has systematically breached its obligations in line with Regulation 7(1)(c) of the PMLFTR and Section 3.1.4 of the IPs applicable at the time of the review[4].

Regulations 11(5) and 11(8) of the PMLFTR and Section 3.5.3.1 of the IPs applicable at the time of the review – Politically Exposed Persons

From the compliance examination it transpired that screening for PEP exposure was not being carried out in an adequate manner. While for mobile banking customers the screening was carried out in an automated manner, for loan customers and EFDIS customers, the screening was being carried out manually. However, no records of this manual monitoring were retained on file or provided to the Officials during the compliance examination.

The Committee was informed that following the compliance examination, the Bank provided a word/notepad document indicating that screening was carried out. However, the Committee members concluded that this document could not be considered as adequate, both because it was provided following the compliance examination (during the wrap up meeting) and because its format was not reliable (in view

[4] Currently Sections 4.4.1 and 4.4.2

of the fact that such word/notepad document could easily be edited and that it did not include an audit trail). Whilst the Bank stated that the information on the word/notepad document was extracted from a system, the process was not carried out during the compliance examination and neither was the system shown to the Officials during the compliance examination, therefore the Committee could not accept the Bank's submissions.

Therefore, the Committee determined that the Bank breached its obligations in terms of Regulations 11(5) and 11(8) of the PMLFTR and Section 3.5.3.1 of the IPs for the loan and EFDIS customers.

Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 3.1.5 of the IPs applicable at the time of the review – Ongoing Monitoring

Finding: Inadequate transaction monitoring rules applied by the bank

Mobile Banking customers

The transaction monitoring measures that the Bank was applying with regards to mobile banking customers were ineffective. As the threshold set in place by the Bank, which was set at Euro 5,000 was not taking into consideration the aggregate amounts of the transactions taking place, which were below such threshold. Therefore, cumulatively, the customers could carry out multiple transactions which would add up to more than the Euro 5,000 threshold set by the Bank, without the Bank's systems picking this up and reviewing these transactions. Furthermore, the monitoring was being done manually daily, and the Bank was experiencing a backlog, which further confirms the inadequacy of its monitoring processes. The Committee was also disappointed to note that prior to April 2018, the Bank held no reasons as to why alerted transactions were being released. Whilst the Bank informed the Committee that these transactions were all being received from regulated credit institutions which were subject to scrutiny, Committee members expressed that the duty to monitor these transactions rested with the Bank, irrespective of whether these transactions originated from other credit institutions. Moreover, whereas the Bank argued that this product does not allow for cash payments, the Committee took into consideration the ease with which the online transactions take place, and thus determined that the latter risk cannot be overlooked.

Apart from this threshold, the Bank also had a threshold for outgoing payments which exceed the Euro 100,000 threshold, however this threshold was considered as too high. Although the Bank in its representations indicated that it had revised this threshold to Euro 25,000 in June 2018, this could not be confirmed during the compliance examination and Bank officials had eventually confirmed that this threshold had not yet been implemented.

Moreover, the Committee could not overlook the fact that the Bank's internal audit had already identified that the transaction monitoring processes were inadequate, yet the Bank had failed to act on the findings arising from the internal audit. This discovery posed serious concerns as to the Bank's regard towards its AML/CFT obligations and its role in combating ML/FT risks (at least up until the compliance examination). Although the Bank indicated that its transaction monitoring systems were offset by technical issues, the Committee reiterated that technical issues cannot be used as an excuse for the fact that transactions were not being monitored in a diligent manner. Furthermore, the Committee expressed that the issues revealed during the compliance examination went beyond mere technical issues but were more indicative of flawed systems and procedures.

Committee members concluded that the transaction monitoring being carried out by the Bank for the mobile banking customers was neither robust nor efficient, both because of the risk that the service is susceptible to, including the lack of efficient thresholds created by the Bank, and because of the volume of customers that were making use of this service. The Committee also considered that the Bank was not managing to adequately monitor the flagged transactions in a timely manner, as was evident from the backlog.

In view of this, the Committee concluded that the Bank was in breach of its obligations at the time of the review.

Loan customers

In relation to loan customers, the Committee noted that the Bank did not have a monitoring system in place to monitor loan repayments, and thus the Bank could not detect any additional repayments and it could not confirm whether the repayments were being carried out by the customer or by third parties. Whilst the Bank informed the Committee that it has started a remediation exercise focusing on obtaining the payor information and identifying instances where loans are paid prematurely or whether no single repayment has taken place, the Committee determined that at the time of the compliance examination the Company was not privy to this information. The risks that this product carries, especially funding of terrorism risks, could not be ignored, especially when no loan repayments take place, and the customer would have used the funds either way. Committee members reiterated that prior to the remediation exercise, the Bank could have unknowingly facilitated ML/FT.

Committee members determined that the Bank has breached its obligation at the time of the compliance examination.

EFDIS customers

The Committee noted that this product was only offered to individuals residing in a particular EU jurisdiction. The funds deposited were being held in a 'Nostro account' with another local bank, however the Bank was not able to review and stop a payment or a transaction from being executed, because transactions were not passing through the Bank's own portals/system. The Committee was concerned to note that when Officials asked to review the transactions of every client file, these transactions were not available, and thus not even a-posteriori transaction monitoring was being carried out by the Bank. In addition, as part of the submissions, the Bank provided statements to demonstrate that customer transaction information could be extracted, however this neither showed nor confirmed that the Bank was carrying out any monitoring on these transactions.

Although the Bank indicated that since December 2019, the funds were no longer being held in this 'Nostro account', the Committee determined that at the time of the compliance examination the Bank could not effectively monitor these transactions.

In view of the above, the Committee determined that the Bank systematically breached its obligations at the time of the compliance examination.

Finding: The Bank's screening of payments to and from high risk and prohibited jurisdictions is ineffective

Payments to or from high-risk jurisdictions or jurisdictions prohibited by the Bank were being alerted for review, however at times these transactions were released in error. For example, in one instance, a customer received a payment of over Euro 1 million from a business based in Panama. Although the Bank's systems stopped this payment and raised an alert, the transaction was still released. Whilst the Bank admitted that this payment was released in error and that the customer was breaching the Bank's terms and conditions, the Committee could not comprehend how this error could occur, particularly since the system had in fact stopped the transaction from being executed.

Overall, in relation to the Bank's obligation to monitor transactions, the Committee concluded that the Bank had wide spread failures and found the bank in serious and systemic breach of its obligations in terms of Regulation 7(1)(d) and 7(2)(a) of the PMLFTR and Section 3.1.5 of the IPs[5].

Regulation 15(3) of the PMLFTR – Suspicious Transaction Reporting

During the compliance examination it resulted that the Bank had failed to submit several suspicious transaction reports despite clear and evident suspicious behaviour. Examples of these cases are being relayed hereunder:

Case 1: This customer was noted to have transferred a payment of Euro 15,000 to a foreign national. When the transaction was queried by the Bank officials, the customer threatened to close the account and when her account was suspended, she threatened to report this to the Maltese authorities. The customer's clarification for the payments was considered as suspicious, as it indicated that the payments were being sent to help poor children and families, help her partner who was part of the military and that if more information is divulged, she would be putting the military in danger. The Bank decided that it was not necessary to submit an STR as the value of the funds transferred was in line with the profile of the customer and that the payment pattern was not a ML/FT typology. However, Committee members did not agree with the Bank's assertions, noting possible risks of fraudulent activity taking place or the customer serving as a money mule. The Committee highlighted, that the fact that the Bank had suspended the account for some time indicated that even the Bank had concerns about the payments being executed. Despite this, it allowed the activity to resume without obtaining any reassurance of the legitimacy of the transactions taking place. Committee members thus, determined that there was sufficient ground to suspect that this payment was suspicious and anomalous, and that an STR was merited.

Case 2: The Committee noted how this customer was an EU individual who was working in a non-EU jurisdiction. As per the information held at onboarding, the customer had a salary bracket of between Euro 25,000 to Euro 50,000 annually. However, it was noted that the transactions received were amounting to between Euro 2,000 and Euro 6,000 monthly, with these incoming transactions at times being received twice in the same month (in one month in particular, the customer received two transfers of Euro 4,000 each in a span of 10 days). The customer was also receiving his wife's salary from an EU bank account, and then transferring this salary to her account, which was also held with the Bank. It was further noted that the funds were then withdrawn in cash and at times, multiple withdrawals of the same amount were taking place on the same day, withdrawn from ATMs located in the non-EU Jurisdiction. The customer was queried about the cash withdrawals by the Bank's Fraud department as it was feared that the account was subject to fraud, however the Bank confirmed that in its view, the withdrawals were not considered irregular, without any justification as to how it arrived at this conclusion. Committee members, however, were disappointed to note that the Bank suggested that these withdrawals are linked to the Bank's lower withdrawal fees rather than understanding the rationale behind the voluminous cash transactions. Although the Committee considered that the payslips submitted with the Bank's representations and the funds received in the customer's account were matching, the pattern of the transactions taking place was in fact suspicious. The Committee could not understand why an EU individual who was working in a non-EU jurisdiction required a bank account in Malta, and why his salary and that of his wife were being transferred to a Malta account for it to be then withdrawn in cash from ATMs located in the non-EU jurisdiction. Members of the Committee held that the way the transactions were structured, made it difficult to monitor the activity being carried out since the audit trail of the transactions was disrupted the minute the funds were withdrawn in cash from ATMs in the non-EU jurisdiction. The customer was creating an additional layer in the transaction cycle and eliminating any traceability with the cash withdrawals. Furthermore, this took place against a background where the customer was a law enforcement officer stationed in a non-EU jurisdiction known to have issues with organised crime and drug trafficking. The

[5] Currently Sections 4.5.1(a) and 4.5.2 of the IPs.

Committee held that there were sufficient grounds to suspect that anomalous activity was being carried out, which merited the submission of an STR.

Committee members, noted that the Bank did not have sufficient regard to such an important obligation, particularly observing that from the information available at the Bank, almost 19% of the transactions reviewed required a suspicious transaction report to the FIAU. The Committee determined that these findings were serious in nature and confirmed that the Bank had breached its obligations in terms of Regulation 15(3) of the PMLFTR at the time of the compliance examination.

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

After taking into consideration the abovementioned findings, the Committee decided to impose an administrative penalty of Euro 653,637 with regards to the breaches identified in relation to:

- Regulation 5(1) of the PMLFTR.
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 4.1 of the IPs applicable at the time of the review.
- Regulation 7(1)(a) of the PMLFTR and Section 3.1.1.2 of the IPs applicable at the time of the review.
- Regulation 7(1)(c) of the PMLFTR and Section 3.1.4 of the IPs applicable at the time of the review.
- Regulations 11(5) and 11(8) of the PMLFTR and Section 3.5.3.1 of the IPs applicable at the time of the review.
- Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 3.1.5 of the IPs applicable at the time of the review.
- Regulation 15(3) of the PMLFTR.

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 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:

- Updates to the BRA together with its methodology.
- Updates to the CRA's methodology.
- The Bank's plan to ensure that active customers and newly onboarded customers are adequately assessed.
- The Bank's plan to ensure it collects and records information relating to the purpose and intended nature of the business relationship and that it builds a comprehensive customer business and risk profile.
- Updates on the Bank's PEP screening.
- Updates on transaction monitoring systems and reports.
- Updates on the Bank's procedure for internal and external suspicious transaction reporting.

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 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.

To determine the appropriate administrative measure to impose, the Committee considered that the Bank did not have good measures in place, particularly for important obligations, such as that to monitor the business relationship and transactions taking place. Moreover, the Committee could not ignore that the Bank was not appreciating several red flags certain relationships presented and did not take the actions

necessary by informing the authority of these anomalous or suspicious behaviours or transactions. The Bank's shortcomings in understanding and assessing risks and in building comprehensive customer profiles also portray a lack of awareness about the necessity to have a solid compliance culture and AML framework to the standards expected by a local credit institution, to avoid the risks of being misused for ML/FT purposes. The importance and seriousness and at times systemic nature of the failures observed could not be discounted, especially when considering that the Bank adopts a business model based on non-face to face interaction with customers and processes transactions through remote means of communications. The Committee further considered that the Bank's lack of regard towards ML/FT risks could have led to the unintentional facilitation of ML/FT, also stemming from a number of relationships/transactions that should have been reported to the Authority. This also meant that the Bank's inadequate and at times systemic flaws in the measures adopted to combat ML/FT risks where not only of determent to its own operations but also of possible impact on the jurisdiction. The Committee however, viewed as positive the overall good level of cooperation demonstrated, and the actions taken by the Bank since the compliance review or those it planned to take to enhance compliance with its AML/CFT obligations. The size and operations of the Bank as a credit institution in carrying out relevant financial business were also taken into account. The Committee took into consideration that the breaches identified were a result of the Bank's lack of adherence to the AML/CFT obligations imposed by the PMLFTR and the FIAU's IPs. The Committee also ensured that the penalty imposed is effective, dissuasive, and proportionate to the seriousness and at times systemic nature of the failures identified.

Key take-aways

- A business risk assessment is necessary not only because it is a legal obligation, but most importantly because it is the foundation of a solid AML/CFT framework. This assessment must be comprehensive in assessing all actual or potential risk factors, as well as in assessing the effectiveness of the control measures implemented. Such assessment cannot be skewered on focusing only on limited risk factors, but it must be a holistic understanding of risks and controls.
- Customer risk assessments aid in understanding the specific risks of a business relationship, and therefore to subsequently allocate the necessary controls to manage and mitigate the identified risks. A one size fits all approach is therefore not possible, unless there is a uniform, logical grouping, and a proper assessment of all relevant risk factors, since inevitably the different specifics of the different risk elements present different risks and therefore the risk criteria considered have to cater for these specifics.
- The purpose and intended nature of the business relationship includes important information that is crucial to create a good customer business and risk profile. Details of the employment of business endeavours, the source of the customer's wealth, the expected source that would fund the operations through the relationship established, and the expected level of activity through the accounts need to be obtained. The degree of information and documentation collected will vary depending on the perceived level of risks, always ensuring that the customer's profile is well understood.
- Effective measures in place to monitor the business relationship and transactions carried out are an important tool that subject persons must have to safeguard their operations from being misused and to safeguard the jurisdiction. Having effective transaction scrutiny measures in place, especially where the business activity of the subject person involves the processing of a considerable volume of transactions, means that the subject person has implemented the necessary measures to monitor the activity. An example of such a measure could be through the introduction of scenarios that are based on the business model and transactional history experienced. This enables transactions to be captured both before the transaction is executed (particularly important for high-risk transactions) and after the transaction has taken place and to

analyse the transaction with a view to determining that there is a lawful, logical business or economic rationale for it and is supported with evidence. One must ensure that structuring is also factored into the monitoring measure implemented.

- While the fact that money may be derived from another credit institution of repute is an important safeguard, this only shows the flow of funds and not the source that generated them, and therefore subject persons should ensure that this is adequately catered for.
- If utilising thresholds, subject persons should ensure that customers are well grouped and that thresholds are in line with the grouping, so that anomalous and large transactions are captured. Setting too high value thresholds defeats the purpose of having transaction scrutiny measures in place.
- The measure implemented to scrutinise transactions has to feature in all products offered and all types of customers serviced, and jurisdictions exposed to. This has to be a holistic measure covering even low risk customers. One must ensure that the monitoring measure implemented is robust and comprehensive enough to capture those transactions that require attention.
- Independent Audits are an indispensable tool to capture any inconsistencies or shortcomings that require action. However, implementing this measure without acting on the Audit's conclusions is futile. Subject persons do not only require having their own reviews in place, but more importantly to take the necessary actions on findings identified, particularly for shortcomings that have a bearing on the ability to review a relationship and determine the need to report to the authority.
- All legal obligations mentioned above are aimed at managing and mitigating ML/FT risks. However, when risk of ML/FT is evidenced from transactional or customer behaviour, subject persons are required not only to have systems in place to monitor those transactions; but should also have procedures and processes in place for reviewing alerts generated with a view to determining whether there is the need to submit a suspicious report to the FIAU. Anomalous complex or large transactions that do not have an economic or lawful rationale should be thoroughly reviewed and escalated to the authority. An STR is also necessary where a lawful purpose and source of funding substantiated with evidence cannot be established. Important red flags include unexplained movement of funds, sudden changes in behaviour, the suspicious request to terminate the relationship following a request for information/documentation, the involvement of certain jurisdictions within the business relationship, especially the involvement of multiple jurisdictions without an economic rationale, as well as large value transactions without supporting documentation. These are all red flags that should be catered for in the determination of whether a suspicious report should be submitted to the FIAU. One must be careful in that one red flag on its own may not be sufficient for the submission of a suspicious report and therefore it is very important that determinations are made based on a comprehensive analysis of all red flags and evidence available.
- Subject persons are required to support and evidence the considerations taken to submit a suspicious report whenever determining that there is knowledge or suspicion that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to funding of terrorism or that a person may have been, is or may be connected with money laundering or the funding of terrorism.

11 August 2022

APPEAL – On the 1st September 2022, the FIAU was served with a copy of the appeal application filed by the Bank before the Court of Appeal (Inferior Jurisdiction) from the decision of the FIAU as detailed above. The grievances brought forward by the Bank include, inter alia, that the process leading to said decision breached the Bank's right to a fair hearing and thus such decision has no legal effect; that the penalty

imposed by the FIAU is arbitrary, disproportionate and excessive, and that the FIAU based its decision on considerations and conclusions which are factually and legally incorrect, without taking into account the Bank's representations.

Pending the outcome of the appeal, the decision of the FIAU is not to be considered final and the resulting administrative penalty cannot be considered as due, given that the Court may confirm, vary or reject in part, the decision of the FIAU. As a result, the FIAU may not take any action to enforce the administrative penalty pending judgement by the Court.

This publication notice shall be updated once the appeal is decided by the Court so as to reflect the outcome of the same.

1 September 2022