Administrative Measure Publication Notice

This Notice is being published by the Financial Intelligence Analysis Unit (FIAU) in terms of Article 13C of the Prevention of Money Laundering Act (PMLA) and in accordance with the policies and procedures on the publication of AML/CFT measures established by the Board of Governors of the FIAU.

This Notice provides extracts from the FIAU's decision imposing the respective administrative measures and is not a reproduction of the actual decision.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:
06 January 2023

SUBJECT PERSON:
BNF Bank plc

RELEVANT FINANCIAL ACTIVITY CARRIED OUT:
Credit Institution

SUPERVISORY ACTION:
Offsite compliance review carried out in 2020

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:
Administrative Penalty of €189,274, a reprimand, and a remediation directive.

LEGAL PROVISION BREACHED:

- Regulation 5(1) of the PMLFTR and Sections 3.3 and 3.3.1 of the Implementing Procedures (IPs) Part I.
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1, 3.5.2 and 3.5.3 of the IPs.
- Regulation 11(1)(b) of the PMLFTR and Section 4.9 of the IPs.
- Regulation 13(1) and 13(2) of the PMLFTR and Section 9.5.2 of the IPs.
- Regulation 7(2)(a) and 7(2)(b) of the PMLFTR and Sections 4.5.1(a), 4.5.1(b), 4.5.2 and 4.5.3.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURES:

Business Risk Assessment (BRA) - Regulation 5(1) of the PMLFTR and Sections 3.3 and 3.3.1 of the IPs

The Committee noted that the Bank had drafted its BRA in May 2019, over a year after the requirement to carry out a BRA first came into place. In its representations, the Bank confirmed the mentioned delay in conducting its BRA, nonetheless, it asserted that prior to the implementation of the BRA it used to carry out annual risk assessments of its money laundering (ML) risks as part of operational risks. However, while acknowledging that these documents show that the Bank did have a general understanding of its ML/FT risks and were also documenting it, the Committee noted that this only provided a basic and high-level risk assessment and did not meet the requirements of an adequate BRA as imposed by Legal Notice 430 of 2018.

In view of the above, the Bank was found in breach of Regulation 5(1) of the PMLFTR and Sections 3.3 and

3.3.1 of the IPs.

Customer Risk Assessment (CRA) - Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1, 3.5.2 and 3.5.3 of the IPs

Finding 1 – Deficiencies in the risk assessment methodology utilised by the Bank until 31 December 2019

The Committee noted that, the CRA methodology implemented by the Bank until 31 December 2019 gave no consideration as to what components could potentially classify a business relationship as low or medium risk. The Bank did not have in place a comprehensive methodology to be able to categorise the various risk factors it may face when entering a new business relationship/occasional transaction and to provide a conclusive and consistent risk rating amongst its customers.

The compliance examination revealed that the risk ratings assigned to customers onboarded by the Bank as at 2019 were based only on few considerations: whether the customer onboarded has any PEP connections, connections to high-risk/prohibited or non-reputable jurisdictions, any adverse media and dealings in a business segment/activity that is considered high-risk or prohibited by the Bank. In its representations, the Bank acknowledged that until 2019, its focus was on the identification of high-risk customers. The Committee however acknowledged that following 2019 the Bank took action on its own motion to enhance the CRA and to start carrying out the necessary updates on all customers. After due consideration, the Committee determined that the methodology used by the Bank as at December 2019 was inadequate since it did not address the specificities of medium and low-risk customers.

Finding 2 – No evidence of CRA at onboarding

The Committee noted that the CRA document that should have been conducted at customer onboarding was not provided by the Bank for any of the customer files reviewed. The Committee deemed it appropriate to consider both the present finding and the previous finding together. Reason for this being that both findings are linked together and result in the fact that the CRA methodology as documented in the Bank's policies and procedures was not adequate, as it only focused on high-risk customers and on assessing customer risk. Moreover, in practice it resulted that the Bank was not even adhering to its own policies and procedures since no CRA was being documented at onboarding stage. This goes against the spirit of the risk-based approach, since if it is not carried out at the onset of the business relationship or the occasional transaction, it becomes increasingly difficult to identify the risks actual and potential risks of customers, formulate a risk profile and allocate the necessary resources through the appropriate level of CDD on the same.

In view of the above reasons, the Committee determined that the Bank was in systemic breach of its obligations under Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1, 3.5.2 and 3.5.3 of the IPs.

Adverse Media Screening - Section 3.5.1(a) of the IPs

The compliance examination revealed that in respect of two of the customer files reviewed, the Bank had failed to carry out adverse media screening on the corporate customers at onboarding stage.

In view of the above, the Committee determined that the Bank was in breach of its screening obligations under Section 3.5.1(a) of the IPs. The Committee held that this breach will be taken into consideration together with the Bank's CRA related breaches for the purposes of the administrative measure to be imposed.

Enhanced Due Diligence- Regulation 11(1)(b) of the PMLFTR and Section 4.9 of the IPs

The Committee noted that following adverse media and alerts placed by the Bank's Compliance Unit six business relationships were risk rated as 'High'. Nonetheless, the Bank failed to perform enhanced additional measures in respect of the customer files concerned, that is, the information and documentation collected on source of funds and source of wealth (SoF/SoW) of the customers/BOs involved was not enough. In addition, the large withdrawals which were frequently affected by these customers were not thoroughly questioned by the Bank. For instance, five of the abovementioned business relationships were a group of customers and although the Bank provided some documentary evidence such as, invoices, copies of cheques and declaration forms, the business operations taking place between the parties were to be substantiated with contractual agreements. This would have enabled the Bank to comprehensively understand the expected activity to be carried out, to be able to corroborate invoices and to be able to carry out more effective scrutiny. The Committee referred to Section 4.9 of the IPs which states that subject persons are expected to gather additional information and/or documentation (as appropriate) which is more thorough and detailed, on transactions that pose a higher risk of ML/FT.

In view of the above, the Committee determined that the Bank has breached Regulation 11(1)(b) of the PMLFTR and Section 4.9 of the IPs in respect of five customer files. The Committee further determined that this particular breach shall be taken into consideration together with the Bank's breaches in relation to its transaction monitoring obligations when it comes to determining the administrative measure to impose on the Bank.

Record Keeping - Regulation 13(1) and 13(2) of the PMLFTR and Section 9.5.2 of the IPs

During the compliance examination, the Bank provided a list comprising of all active and inactive customers of the Bank. During the file review, the MFSA Officials observed that the customer list was inconclusive and therefore requested clarifications from the Bank. The Bank, subsequently, explained that this was due to a fault in the extraction process from the Core Banking System which caused the omission of a number of customer names from the customer list. The Committee, after taking into consideration, both the finding as reported in the Findings Report and the Bank's representations in this regard held that while it understands that human errors can occur and that the situation, as explained by the Bank, is indeed a genuine mistake, the fact remains that a number of customer names had not been extracted. This effected the Bank's efficiency and reliability in complying with the authorities' request, to provide its active and inactive customer lists. The Committee highlighted that it is important for the Bank to understand the importance of such request and to ensure that it has efficient record keeping measures that allow the effective retrieval of all customer information.

Thus, in view of the above considerations, the Committee determined that the Bank was in breach of Regulation 13(1) and 13(2) of the PMLFTR and Section 9.5.2 of the IPs.

Ongoing Monitoring – Regulation 7(2)(a) and 7(2)(b) of the PMLFTR and Section 4.5.1(b) and 4.5.3 of the IPs

Periodic reviews not conducted in line with internal policies

The compliance examination identified that in three customer files there was some minor lack of adherence by the Bank in performing ongoing reviews in accordance with its policies and procedures.

Although, according to the Bank's internal policies, file review for these customers should have be carried out every 12 months, the Bank delayed the review beyond this period.

In view of the above, the Committee determined that the Bank is in breach of Regulation 7(2)(a) and 7(2)(b) of the PMLFTR and Section 4.5.1(b) and 4.5.3 of the IPs

Transaction Monitoring - Regulation 7(2)(a) and 7(2)(b) of the PMLFTR and Section 4.5.1(a) and 4.5.2 of the IPs

Insufficient supporting documentation surrounding the network of companies held by the same BO

As explained hereunder, during the compliance examination a number of customer relationships carried numerous transactions for which the information held on file was insufficient:

Case 1: The corporate customer conducted a number of withdrawals. For instance, it was observed that during 2014, a total aggregate amount of around €4M was withdrawn by the same customer and the Bank did not obtain sufficient reassurance of the purpose as stated by the customer. Therefore, the Bank was expected to ascertain the veracity and legitimacy of the reasons for withdrawal, such as, by requesting from the customer an agreement between the parties delineating the payment terms, frequency and means of payment.

Case 2: A known counterparty to the company dealing in commodities issued a cheque deposit of €700,000 in 2014 to the corporate customer. The Bank provided a copy of the cheque relating to the mentioned transaction and also provided the relative special clearing form. In this regard the Committee held that the copy of the relative cheque merely indicates the means how money was transacted but does not indicate the reason why such transaction was required. Furthermore, other shortcomings were identified in relation to 19 other transactions carried out by the Bank and ranging between approximately €50,000 to almost €1,000,000. For 15 out of these 19 transactions, the Bank asserted that these were inter-company transfers between companies within the same group of companies. The Bank added that inter-company transfers are not normally flagged since they frequently relate to liquidity management purposes. Nonetheless, the Committee held that additional information in relation to the transactions carried out within the same group of companies was still expected to be obtained by the Bank, to ensure there was a legitimate purpose for the transactions taking place. Clearing off transactions as internal transfers between companies forming part of the same group is not sufficient since one had to understand the purpose behind the transfer. Furthermore, for four out of the abovementioned 19 transactions the Bank provided just 'Inward/Outward Payments' extracts explaining the transaction data. This yet again is insufficient since it explains the flow of funds but not the source and rationale for the same.

Insufficient resources/tools to conduct transaction monitoring

When it comes to the identification of any anomalies and/or suspicious transactions, the Bank relied on the manual scrutiny of Bank employees for deposits effected with the branch cashiers, and post-transaction through weekly generated reports for all transactions. It was noted that the Bank had a very limited number of internal STRs raised by the Bank employees responsible to scrutinise the weekly reports. Indeed, this amounted to only 16 during 2019. Considering the size of the Bank and the amount of transactions processed daily, this limited number of internal STRs raised in a year, poses serious concerns and does raise doubt on how truly effective the scrutiny of the weekly reports was being carried out.

In its representations, the Bank held that since 2020 it had embarked on an extensive transaction

monitoring program which would lead to the implementation of a fully-fledged automated transaction monitoring system. Besides updating the Bank's transaction monitoring framework, the CRA tool was updated to focus on reviews and transaction monitoring. Furthermore, the Bank held that it had provided specialised training to staff carrying out transaction monitoring, focusing specifically on identifiable patterns, advanced screening, monitoring of red flags and suspicious activity reporting. The topic is also discussed frequently during the various compliance outreach programmes which the MLRO undertakes with both front-office and back-office functions. In addition, the Bank held that during 2020, it also engaged a specialist data analyst which is assisting in the creation and handling of automated reporting and data extraction. The Committee also was provided with the necessary reassurance of the actions taken/planned to be taken by the Bank and it commended the Bank for such pro-active approach.

The Committee held that whilst it acknowledges the Bank's remedial actions towards enhancing its transaction monitoring system, the fact remains that as at the time of the compliance examination this Bank used to rely solely and completely on the manual scrutiny of Bank employees at the time of deposits effected with the branch cashiers and post-transaction through the weekly generated reports. The latter of which is far from achieving the effective results that one would expect. The Committee further added that transactions that cumulatively exceed the bank's reportable thresholds or any ambiguous transactional patterns cannot be successfully identified through such reports. Such a deficiency adversely influences the Bank's potential to effectively detect and flag suspicious transactions, and consequently to effectively assist authorities in defending the Maltese financial system. However, the Committee also considered that the transactions happened in or around 2015.

In view of the above, the Committee held that the Bank is in breach of Regulation 7(2)(a) and 7(2)(b) of the PMLFTR and Section 4.5.1(a) and 4.5.2.

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

After taking into consideration the abovementioned breaches by the subject person, the Committee decided to impose an administrative penalty of one hundred and eighty-nine thousand and two hundred and seventy-four euro (€189,274) in view of the Bank's failure to abide with its obligations in terms of:

- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1, 3.5.2 and 3.5.3 of the IPs.
- Section 3.5.1(a) of the IPs.
- Regulation 11(1)(b) of the PMLFTR and Section 4.9 of the IPs.
- Regulation 7(2)(a) and 7(2)(b) of the PMLFTR and Section 4.5.1(a) and 4.5.2 of the IPs.

Furthermore, the Committee decided to reprimand the Bank for its failure to conduct the BRA once the legislative requirement was introduced in January 2018 in breach of Regulation 5(1) of the PMLFTR and Sections 3.3 and 3.3.1 of the IPs as well as for its record keeping shortcomings in breach of Regulation 13(1) and 13(2) of the PMLFTR and Section 9.5.2 of the IPs.

In addition to the above, the Committee also served the subject person with a Remediation Directive in relation to:

- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5.1, 3.5.1(a), 3.5.2 and 3.5.3 of the IPs.
- Regulation 7(2)(a) and 7(2)(b) of the PMLFTR and Sections 4.5.1 (a), (b), 4.5.2 and 4.5.3 of the IPs.

The aim of this Remediation Directive is to direct the subject person to take the necessary remedial actions

to ensure that it understands the risks surrounding its operations and that it has implemented sufficient controls to mitigate the identified risks. Furthermore, it aims to ensure that the subject person is effectively addressing the breaches set out above. In virtue of this Directive:

- The Bank shall provide an updated and documented CRA measure that is to be based on the four risk pillars: customer risk, product/service risk, delivery/interface risk and geographical risks. The Bank's updated CRA measure shall be in accordance with Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1 and 3.5.3 of the IPs. The Bank shall also provide documented CRA procedures which shall include an explanation of the updated CRA methodology, that is, how each risk factor is assessed and scored, and also an explanation of how the final CRA rating is obtained. The Bank shall ensure that in the updated CRA, the rationale behind the ratings assigned to the different components of the risk factors is properly documented. All customer files have to be adequately assessed in line with the revised CRA.
- The Bank shall also provide a detailed timeline explaining the different phases of the Bank's plan to update the expired customer file reviews; an explanation and any documentation relevant to the implementation of measures it has in place to ensure that it avoids situation of overdue in the review of customer files; a timeframe for the centralisation of all customer information to enable the effective monitoring of customer files; and the records which it keeps as proof that such reviews have been carried out.
- The Bank shall also provide a documented explanation of its updated transaction monitoring system which shall highlight any scenarios, thresholds and considerations taken to monitor customer relationships and to identify behaviour or transactions that diverge from what one would expect from the customer, or that are otherwise large, complex and/or anomalous.

Through the remediation process, the Bank shall be required to provide any documentation, customer files, system walk throughs as necessary to ensure the implementation of the actions required.

When determining the appropriate administrative measures to impose, in addition to the specific considerations outlined above, the Committee took into consideration the importance of the obligations breached, the seriousness of the findings identified, and the risk of possible ML/FT caused by the breach identified. The Committee also considered the impact that the subject person's failure may have had on both its operations and on the local jurisdiction, the size of the subject person, as well as the fact that the subject person's officials were cooperative during the compliance examination. The Company's immediate actions to remediate the failures observed, and the actions initiated on its own motion prior to the imposition of the Remediation Directive were also positively considered. Furthermore, the Committee ensured that the penalty being imposed is effective, dissuasive, and proportionate to the failures identified and to the period in time within which certain breaches were committed.

In its deliberations, the Committee was very positive of the Bank's pro-active approach in both identifying shortcomings from its own motion before the review was initiated as well as taking immediate action following the compliance review on the Bank, and this without awaiting for the directive to be issued by the FIAU. The Committee also commended the Bank in its approach to notify the FIAU of the actions it took both before and following the review as well as for providing substantial details of its ongoing planned actions. The Committee was also positive as to the commitment shown by the Bank and its top management to combat ML/FT and to ensure the Bank has the highest standards to safeguard the jurisdiction from crime.

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 Takeaways

- The carrying out of a comprehensive and approved BRA is essential for subject persons to combat ML/FT risks sufficiently.

- Subject persons need to assess the risks that they are exposed to because of the business relationships they engage in. This is to be done by assessing the inherent risk which depends on the identification of the existent threats and vulnerabilities by considering risk factors including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels, as well as a consideration of reliable adverse information on the customer or its beneficial owner. In Section 3.2, the IPs provide specific definitions and explanations of what each risk factor constitutes and what elements need to be considered to assess the same; these shall be taken into consideration by subject persons when creating their CRA methodology.

- Subject persons should keep in mind that the CRA is one of the pillars of a sound AML/CFT compliance program. This measure is necessary both for determining the level of due diligence required to build comprehensive customer profiles, as well as for ascertaining the degree of on-going monitoring necessary. Therefore, not conducting an adequate CRA has serious and widespread repercussions. Furthermore, given that risk is dynamic, it is important that the CRA is reviewed from time to time depending on the risk presented. The level of detail of a CRA is to reflect the complexity of the business relationship being engaged in. The more complex the customer and the relationship, the more thorough the details required to assess it need to be, in order to ensure a comprehensive risk understanding. This will ultimately allow the effective implementation of the risk-based approach and the efficient utilisation of resources.

- Building a comprehensive customer business and risk profile is crucial to enable both an understanding of the customer, as well as the ability to monitor actual against expected activity. Obtaining information/documentation on the business operations, the source of wealth/the source of funds, the expected level of activity and the purpose of the relationship are crucial to enable the effective management of the risks presented.

- Certain higher risk situations will require more detailed information and documentation both to ensure that the risks are comprehensively understood as well as to effectively manage such higher risk situations. The carrying out of enhanced measures whenever such risks are identified, both if these occur as part of the onboarding process or throughout the business relationship either in view of changes in the customer profile or due to specific transactions, are thus necessary.

- Transaction monitoring is particularly important for subject persons to identify behaviour or transactions that diverge from the usual pattern of transactions carried out by a particular customer or that do not fit within the customer's profile. Transaction monitoring is also essential to determine whether the initial risk assessment requires updating, and whether, in view of the updated risk assessment or other considerations, the business relationship remains within the subject person's risk appetite. Effective transaction monitoring enables anomalous or large transactions to be flagged/noted, assessed, and analysed to ensure a legitimate purpose is identified and evidenced. Moreover, effective transaction monitoring measures should enable subject persons to capture high value and high-risk transactions before they are allowed to pass through the system. Higher risk transactions should not be allowed to pass through without the

prior scrutiny taking place. Effective transaction scrutiny should ultimately enable the identification of suspicious activity in relation to which a suspicious transaction report needs to be filed with the FIAU.

12 January 2023