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.

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

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

03 October 2022

SUBJECT PERSON:

Finance Incorporated Limited

RELEVANT ACTIVITY CARRIED OUT:

Financial Institution

SUPERVISORY ACTION:

Targeted compliance review carried out in 2019

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €83,051 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 5(1) of the PMLFTR and Section 3.3 of the Implementing Procedures IPs.
- Regulation 5(5) of the PMLFTR and Section 3.4 of the IPs.
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5.1 of the IPs.
- Regulations 7(1)(a) and 7(1)(b) of the PMLFTR and Section 4.3 of the (IPs).
- Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs.
- Regulation 7(1)(d) and 7(2) of the PMLFTR and Section 4.5.1 and 4.5.2.3 of the IPs.
- Regulation 11(1)(b) of the PMLFTR and Section 4.9.1 of the IPs.
- Section 8.1 of the IPs.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment

It became evident that, at the time of the compliance review, while the Subject Person had a Business Risk Assessment (BRA) in place and a good understanding of risks, this was last revised in 2018. It was also noted

that there was no explicit factoring of the jurisdiction risk element in understanding its business wide risks (as a result a number of customer files failed to account for such jurisdiction risk exposure). Moreover, whilst the BRA did consider the risks posed by the products and services provided by the Subject Person and the measures which it was implementing to mitigate such risks, the BRA fell short in assessing the effectiveness of the controls which were in place. The Committee, thus, determined, that the Subject Person was not in a position to adequately assess whether the Money Laundering and Funding of Terrorism (ML/FT) risks, being posed on it as a result of its business relationships, were being effectively mitigated.

In view of the above reasons, the Committee determined that the Subject Person was in breach of Regulation 5(1) of the PMLFTR and Section 3.3 of the IPs for its delay in carrying out a review of the BRA and for the failure to assess, in the BRA, the effectiveness of the controls which it had in place.

Customer Risk Assessment

The Committee determined that although the Subject Person had a customer risk assessment (CRA) methodology in place, this was not rigorous and comprehensive enough to enable it to sufficiently understand the risks posed by the clients and to effectively apply the risk-based approach. This observation was made following a review of a number of customer files wherein it was revealed that the CRA was not taking into consideration all the risk factors. By way of example, in a number of customer relationships, the Company failed to assess risks deriving from onboarding customers on a non- face to face basis as well as not assessing the geographical risks present Moreover, the Subject Person itself acknowledged, in its representations, that it had shortcomings that needed to be remedied with respect to the manner in which the CRA risk weighting was being assessed and calculated.

In view of the above, the Committee decided that the Subject Person was in breach of Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5.1 and Section 8.1 of the IPs.

Policies and Procedures

Following a review of the Subject Person's anti-money laundering (AML) policies and procedures which were in place as at the time of the compliance examination, it resulted that the mentioned policies and procedures contained generic information. These did not address different levels of due diligence to be applied when onboarding customers, screening, transaction monitoring or suspicious activity reporting. Furthermore, there was no screening policy in place highlighting the main requirements to be followed by the employees conducting client screening, how to discount the false positives and the systems to be used.

Whilst not contesting the above-mentioned shortcomings, it was positive to note that the Subject Person, with its representations, provided an updated version of its AML policies and procedures. Following a review of the same, the Committee observed that these sufficiently address and explain the Subject Person's approach with respect to due diligence to be applied when onboarding customers, screening, transaction monitoring, reporting and enhanced due diligence (EDD). Nonetheless, whilst the Committee positively acknowledged the remedial actions taken by the Subject Person in this regard, it cannot ignore the fact that as at the time of the compliance review the Subject Person's documented AML policies and procedures had various shortcomings.

Consequently, in view of the above, the Committee proceeded to find the Subject Person in breach of Regulation 5(5) of the PMLFTR and Section 3.4 of the IPs.

Customer Due Diligence (Identification & Verification)

The compliance examination revealed that, in respect of circa 2% of the customer files reviewed, no identification documentation was obtained. The Committee further noted that the Subject Person did not contest this finding and did not provide any proof evidencing that it had obtained the mentioned documentation and held it on file.

As a result, the Committee held that the Subject Person was in breach of Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.3 of the IPs in respect of circa 2% of the customer files reviewed.

Enhanced Due Diligence

In addition to the Subject Person's failure that, as at the time of the compliance examination, it had no EDD procedures in place, no EDD measures were being applied on a number of high-risk files. In its representations the Subject Person held that all clients were managed under EDD in view of them exceeding pre-set thresholds. In most instances, additional onboarding documentation was being collected to verify the client relationship; three distinct searches were being conducted to monitor the client relationship during onboarding and review and ultimate beneficial ownership was being verified up to 10% ownership on all corporate entities. However, the Committee held that these measures only address risks surrounding the customer's identity, ownership and screening. Therefore, do not constitute sufficient EDD measures for risks surrounding the customer's profile. Therefore, such measures do not adequately mitigate the ML/FT risks posed on the Subject Person by a high-risk business relationship. Moreover, the Committee remarked that the Subject Person had failed to grasp the significance of the distinction between CDD measures and EDD measures and the purpose that these measures serve respectively. This was further highlighted through the fact that this distinction was not even made in the Subject constitute sufficient Person's AML policies and procedures which were in place as at the time of the compliance examination.

The Committee proceeded to review and analyse the documentation submitted by the Subject Person for the purposes of the compliance review and concluded that circa 33% of the customer files reviewed had sufficient high-risk elements as to be considered high-risk customers. This determination was done in view of the services they were rendering, the exposure to non-EU and high-risk jurisdictions and the expected volume of activity. Therefore, the application of EDD measures was required in order to gather a more thorough understanding of the business profile of these customers. The Committee noted that the mentioned customer files encompassed a number of high-risk factors concerning the product the customers were using, the value of the expected account turnover, the employment/business operations of the customer and the geographical connections of the customer. The Subject Person was expected to take these high-risk factors into consideration and apply more rigorous measures including gathering additional documentary evidence of the business operations, the customer's source of wealth (SoW) and its source of funds (SoF). Furthermore, the Subject Person should have determined the degree of enhanced scrutiny necessary on the business operations carried out through the business relationship with these high-risk customers.

On the basis of the above considerations, the Committee determined that the Subject Person is in breach of Regulation 11(1)(b) of the PMLFTR and Section 4.9.1 of the IPs in respect of circa 33% of the customer files reviewed.

Information on the Purpose and Intended Nature of the Business Relationship

Following a review of all customer files which were subject to the compliance examination, it transpired that 60% of the customer files reviewed had shortcomings concerning the Subject Person's obligation to obtain information on the purpose and intended nature of the business relationship.

In the case of 56% of the customer files reviewed, no comprehensive information in relation to the customers' expected SoF and SoW was held on file. In these files, the Subject Person merely documented a generic description such as "Salary" or "Employment" without any further information or details.

In its representations, the Subject Person acknowledged that out of the abovementioned 56% of the customer files reviewed there were files which had no information in relation to the customers' SoF held on file. With respect to some other customer files, the Subject Person held that no SoF was collected since no transactions were conducted on the client account. In the case of one customer file, it held that whilst the SoF was well known to the Subject Person, this was not documented. In the case of the remaining customers, the Subject Person held that all customers had taken an initial loan from a bank account in their own name and that, thus, the SoF of these customers originated from another bank account within the EU. However, the Committee declared that there is a requirement to obtain information (and documentation as may be necessary) in relation to the expected SoF independently of whether transactions are allowed to pass through. The reason is that this is the information collected at onboarding and it relates to expected and not actual SoF. The fact that the customers utilised Banks in EU jurisdictions is a good risk assessment factor but that cannot be said to be the expected SoF since one is required to understand the source and not the flow of funds. In relation to information not being documented, the Committee remarked on the importance of documenting everything in writing to confirm such understanding and the timings of when this was obtained. Therefore, the explanations provided by the Subject Person were not relevant justifications as to exonerate it from complying with the obligation to document and hold on file the expected SoF in respect of these customers. Furthermore, the Subject Person, in its representations, acknowledged its failure to have SoW information/documentation held on file in respect of all the above-mentioned customer files.

Additionally, in respect of 60% of the customer files reviewed the Subject Person was holding on file insufficient details regarding the anticipated level and nature of activity of the business relationship. In these files there was no explanation as to what is expected throughout the business relationship. Also, no information was held on file to support the rationale for the customer seeking a business relationship. Moreover, the Subject Person, in its representations, held that these were individual customers and acknowledged that the onboarding process warranted an improvement.

The Committee determined that the Company's shortcomings were factual and that these conveyed that, at least up until the compliance examination, the Subject Person had disregard towards its obligations to evaluate and understand the risk profiles of its customers. Moreover, it became apparent that the Subject Person had a lax approach when it comes to ensuring that the customer information is adequately and comprehensibly collected and considered.

As a result, the Committee declared that the Subject Person was found in breach of Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs in respect of 60% of the customer files reviewed.

Ongoing Monitoring: Transaction Monitoring and Document Monitoring

As at the time of the compliance examination, the Subject Person's transaction monitoring was automatic for: 5,000 Euro/+ transactions in the case of individual accounts; 10,000 Euro/+ transactions in the case of corporate accounts; and in the case of smaller transactions made in the same day by the same sender that in total make up one of the mentioned thresholds. Transactions that fall outside these three rules were being monitored manually.

The Committee noted that the transaction monitoring system which was being implemented by the Subject Person failed to cater for the large volume of transactions processed by the Subject Person and it failed to comprise all possible ML/FT risks which may be posed by each business relationship. Thus, allowing for the implementation of the risk-based approach and more effective utilisation of resources. Consequently, the Committee held that this transaction monitoring system has to be updated and refined in order to comprise rules which are more risk-based according to the business activity of each customer. The updated transaction monitoring system must be compatible with the products/services offered by the Subject Person, and it shall be adjustable to match different customer profiles. Moreover, the Committee added that to determine whether there is a reasonable explanation for an unusual transaction, the Subject Person shall require the collection of information and/or documentation which clearly indicate that there is a legitimate reason for that transaction or for any divergence from the customer's usual transaction activity. For this purpose, the Subject Person may request information and/or documentation following: the source of funds of that transaction; any new operational activities; any significant relevant changes relating to the customer and; any other information that the Subject Person deems reasonably necessary to be satisfied that the funds are derived from legitimate sources. Encompassing a one size fits all approach threshold-based monitoring is not effective nor efficient and increases risks of having transactions slipping through the net in view of the large volumes of alerts that may be generated. The level of data to be obtained should allow the Subject Person to come to a reasonable conclusion on the legitimacy of the transaction, but should not be excessive, disproportionate or irrelevant; the requests should be within the context of the transaction and the customer's profile.

Positively, in its representations, the Subject Person, held that it has progressed towards the building of an in-house dynamic transaction monitoring system which is based on the individual customer profile. The Committee acknowledged the Subject Person's self-imposed plan of action and also took into consideration the fact that no breaches, on the part of the Subject Person, were found in respect of specific transactions carried out by its customers. However, the Committee held that it cannot ignore the fact that as at the time of the compliance examination, the Subject Person's transaction monitoring system had the above-mentioned shortcomings, and the risks that the same presented.

Furthermore, 14 client files were found to have never undergone a review since being onboarded. In its representations, the Subject Person asserted that high risk customers are reviewed annually; medium risk customers are reviewed every 2 years and; low risk customers are reviewed every 3 years. Notwithstanding this, the Committee noted that the Company was not adhering to its own imposed measure, this without entering into the merits of carrying out reviews on trigger events, which reviews are indispensable.

After taking all of the above considerations into account, the Committee held that the Subject Person is in breach Regulation 7(1)(d) 7(2) and Section 4.5.1 & 4.5.2.3 of the IPs.

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

After taking into consideration the abovementioned breaches by the Subject Person, the Committee decided to impose an administrative penalty eighty-three thousand and fifty-one euro (€83,051) with regards to the breaches identified in relation to:

- The Subject Person's failure to carry out EDD in terms of Regulation 11(1)(b) of the PMLFTR and Section 4.9.1 of the IPs in respect of 20% of the customer files reviewed and its failure to have the necessary policies and procedures relating to EDD in place in accordance with Regulation 5(5) of the PMLFTR and Section 3.4 of the IPs; and
- The Subject Person's failure to obtain information on the purpose and intended nature of the business relationship in terms of Regulation 7(1)(c) of the PMLFTR and Section 4.4 of the IPs in respect of 60% of the customer files reviewed and its failure to have the necessary policies and procedures in place detailing the information to be obtained in this regard in accordance with Regulation 5(5) of the PMLFTR and Section 3.4 of the IPs.

Furthermore, the Committee decided to reprimand the Company for failing to adhere to the customer due diligence requirements established by Regulation 7(1)(a) and 7(1)(b) of the PMLFTR and Section 4.3 of the IPs in respect of circa 2% of the customer files reviewed.

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

- Regulation 5(1) of the PMLFTR and Section 3.3 of the IPs for the Subject Person's shortcomings in relation to its BRA;
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5.1 of the IPs for the Subject Person's shortcomings in relation to its CRA methodology;
- Section 8.1 of the IPs for the Subject Person's failure to carry out a jurisdiction risk assessment on non-EU jurisdictions with which 56% of the customer files reviewed had connections; and
- Regulation 7(1)(d) and 7(2) of the PMLFTR and Section 4.5.1 & 4.5.2.3 of the IPs for the Subject Person's failures in relation to its ongoing monitoring obligations.

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 Subject Person was requested to:

- Provide revised version of the BRA in accordance with Regulation 5(1) of the PMLFTR, Section 3.3 of the IPs. This BRA shall incorporate a revision of the Subject Person's ML/FT risks and of the mitigating measures in place as well as a section specifically dedicated to the assessment of the effectiveness of the controls which the Subject Person has in place. The Subject Person is likewise expected to evaluate the reputability as well as the risks prevailing under the jurisdictions that it is operating in and the jurisdictions that its customers are connected to;
- Make available an updated and documented CRA measure, in accordance with Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.5.1 and 3.5.3 of the IPs, based on the four risk pillars: customer risk,

product/service risk, delivery/interface risk and geographical risk. The Subject Person 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 risk rating is obtained. The Subject Person shall ensure that in the updated CRA, the rationale behind the ratings assigned to the different components of the risk factors is properly documented. Particularly, the geographical risk consideration shall also factor in the considerations taken in the BRA, but at a customer level. Moreover, the Subject Person is expected to carry out a review of all its active clients in order to make sure that the risk assessments maintained by the Subject Person are accurate, adequate and in accordance with the updated CRA methodology of the Subject Person;

- Carry out a review of its active customer files and update the same in accordance with the information and documentation necessary to form a comprehensive customer profile and to ensure that the information on the purpose and intended nature of the business relationship of all its customers; and
- 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 customer behaviour/transactions that diverge from what would be expected from a particular customer. Moreover, the Subject Person is requested to provide the documented procedure which it follows to carry out the review of its client files and to also provide the records which it keeps as proof that such reviews have been carried out.

The Subject Person was informed that 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 its consideration and possible eventual action.

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 obligation, 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 overall 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 has also been positively considered. Furthermore, the Committee ensured that the penalty being imposed is effective, dissuasive and proportionate to the failures identified.

Key Takeaways

- When performing the BRA, and following the determination of the inherent risk, subject persons shall also consider the AML/CFT measures, policies, controls and procedures it already has in place or which need to be adopted. Moreover, the effectiveness of these measures, policies, controls and procedures are to be assessed and established. Following this, subject persons shall determine whether the remaining residual risk falls within their risk appetite. Importantly, any material divergence in business, such as the introduction of new products, the divergence of the customer segment serviced or the increase in transactional value and volume, amongst others should trigger the updating of the BRA.

- Subject persons are expected to evaluate the reputability as well as the risks prevailing under the jurisdictions that it is operating in and the jurisdictions that its customers are connected to. Such jurisdictional risk assessment shall take into consideration indices which assess the risks of ML/FT and prevalent crimes in the country, such as the Basel AML Index, the Corruption Perception Index and so

forth. The Company is also expected to consider FATF public statements and other similar statements issued by other bodies including the EU Commission. A subject person's BRA should reflect the requirements imposed by Section 8 of the IPs as imposed by the IPs. Following the identification of the jurisdictions to which subject persons is exposed to, the BRA should also include the assessment of certain risk factors associated with that particular jurisdiction. Following the evaluation of risks, subject persons are expected to arrive at a final scoring, document it and be able to explain the rationale behind the assigned rating. In any jurisdiction risk assessment carried out it is always indispensable to consider both the reputability as well as the risks prevalent in a jurisdiction. Whilst ML/FT risks should be considered, other risks linked to political instability, prevalent crimes, rule of law etc., should also be taken into account.

- Subject persons shall assess the risks that they are exposed to as a result of the business relationships they engage in. This shall be done by assessing the inherent risk which depends on the identification of the existent threats and vulnerabilities which as specified by Regulation 5(1) of the PMLFTR can be done by considering "risk factors including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels". The IPs in Section 3.2 provide specific definitions and explanations of what each risk factor constitutes and what elements shall 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, which 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 be 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 entered into, in that the more complex the customer and the relationship entered into the more thorough the details to assess to enable a comprehensive risk understanding.

- The subject persons' AML/CFT policies and procedures must be adequately reviewed and approved by senior management and should be aligned with what the subject person practices.

- The carrying out of EDD measures are indispensable where the risk presented cannot be mitigated and managed through the implementation of normal CDD measures. Therefore, subject persons shall ensure that there is a significant consideration of which risks can be mitigated and managed through the carrying out of normal CDD and which risks require the implementation of EDD.

- In terms of Regulation 7(1)(c) of the PMLFTR, subject persons are required to assess and, where appropriate, obtain information and/or documentation on the purpose and intended nature of the business relationship. Such information is crucial to determine the customer's business and risk profile and to enable the effective management of risks presented.

- It is pertinent that subject persons comprehend the importance of the distinction between expected and actual SoF. At onboarding, subject persons are required to obtain sufficient information to be confident that they sufficiently understand from where the business activity to be carried is expected to be funded. Subsequently, throughout the business relationship and if circumstances so warrant, certain transactions may require clarification which would necessitate the obtaining of documentary evidence to understand the source that funded such transactions. This could be either because the

transaction diverges from that expected, or such transaction is of higher risk or of a substantial value, therefore necessitating more reassurance as to its veracity and source of funding.

- 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 and scrutiny should also enable the Company to identify suspicious activity in relation to which a suspicious transaction report shall be filed with the FIAU. Customer profiles need to be reviewed and updated in line with the risks they present, but also in view of trigger events that would signal a possible divergence form the normal business.

- The transaction monitoring system to be applied by the subject persons shall be compatible with the products/services offered by them and it shall be adjustable to match different customer profiles. It is inefficient and ineffective to create one size fits all threshold-based monitoring. Rather the scenarios and thresholds included should enable the effective application of the risk-based approach in order to ensure the best risk-based coverage of transactions (both before and after they occur).

07 October 2022