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.

It is pertinent to note that this notice provides select information from the FIAU's decision imposing the respective administrative measures and is not a reproduction of the actual decision.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

26 December 2022

SUBJECT PERSON:

Nesh Limited

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

On-site compliance review carried out in 2020

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of €198,126

LEGAL PROVISION BREACHED:

- Regulation 5(1), (3) and (4) of the PMLFTR and Section 3.3 of the FIAU's Implementing Procedures, Part I
- Regulation 5(5)(a)(i) of the PMLFTR and 3.5 and 3.5.2 of the IP Part I, Section 2.2.1, of the FIAU's Implementing Procedures Part II
- Regulations 7(1)(a), Section 4.3.1 of the IPs Part I and Sections 3.2(i) of the FIAU's Implementing Procedures Part II
- Regulation 7(1)(c) of the PMLFTR and Section 3.2(iii) and (iv) of the IPs Part I and Section 3.3.2 of the FIAU's Implementing Procedures Part II
- Regulation 7(2)(a) of the PMLFTR, Section 4.5.2 of the IPs Part I and Section 3.2 (iv) of the IPs Part II

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURES:

Business Risk Assessment – Regulation 5 (1) (3) and (4) of the PMLFTR and Section 3.3 of the FIAU's Implementing Procedures, Part I

The Company's Business Risk Assessment (BRA) was not comprehensive due to two main reasons: the methodology and the final residual risk.

First, the methodology of the BRA was not comprehensive and did not provide the criteria used to identify specific scenarios. The Company also did not provide a transparent, complete and satisfactory view of the methodology it adopts to compute the various components of the BRA.

Additionally, the Company did not clarify the way that the BRA was implemented and how each risk factor and risk criteria within each factor was considered. The Company provided no explanation as to how the risk classification was achieved, and only listed a number of considerations within each risk factor, and a risk classification assigned to it.

The Committee therefore concluded that considering the failures observed in the BRA the Company was found in breach of Regulations 5(1), (3) and (4) of the PMLFTR and Section 3.3 of the Implementing Procedures, Part I.

Customer Risk Assessment (CRA) - Regulation 5(5)(a)(i) of the PMLFTR and 3.5 and 3.5.2 of the IP Part I, Section 2.2.1, of the FIAU's Implementing Procedures Part II

During the compliance examination it was noted that the Company had not provided any policies or procedures which expressly explain the methodology and risk factors that should be taken into consideration when carrying out the CRA, how the final risk score of the customer is to be determined, what weight each parameter is allocated and how it contributes to its final risk score.

The Committee noted that the Company implemented a Customer Acceptance Policy (CAP). It also observed that the CAP referred to customer classifications as Low, Medium and High. While this could be of assistance in determining the customer risk element in the CRA, much more detail was necessary to assess the individual customer risks in an effective manner. Therefore, this could not be considered equivalent in any manner to the obligation to have CRA policies and procedures in place.

Moreover, the Committee noted that there was no evidence of CRAs carried out. Indeed, from all the profiles reviewed in relation to CRA, only two files had a risk classification rating but there was no explanation of how the rating was reached.

Thereby, the Committee concluded that the Company is in breach of Regulation 5(5)(a)(i) of the PMLFTR and 3.5, specifically 3.5.2 of the IPs Part I, and Section 2.2.1 of the IPs Part II.

Customer Due Diligence - Regulations 7(1)(a), Section 4.3.1 of the IPs Part I and Sections 3.2(i) of the FIAU's Implementing Procedures Part II

The compliance review identified several instances where the obligation of Customer Due Diligence was not adhered to. For instance:

- In one file, the Company did not obtain and provide any documentation which could verify the identity and residential address of the player.
- In another file, the document obtained by the Company to verify the permanent residential address of the player did not bear an issue date and the document was not as a minimum a utility bill.
- Additionally, another file was also in breach because the document obtained by the company was

unclear and illegible.

In view of this, it was determined that the Company was not in compliance with its customer due diligence obligations, and thus was found in breach of the regulations.

Purpose and Intended Nature of the Business Relationship - Regulation 7(1)(c) of the PMLFTR and Section 3.2(iii) and (iv) of the IPs Part I and Section 3.3.2 of the IPs Part II

The compliance examination identified that the Company relied on basic and generic information to build the risk profile of the customer, hence shortcomings in the Company's ability to obtain sufficient information/documentation to at least understand the nature of the customer's employment or business activities and the expected level of activity were identified.

In view of these facts, the Committee concluded that at the time of the examination the Company had substantially inadequate policies and procedures in relation to purpose and intended nature of the business relationship.

Therefore, the Committee determined that this finding constitutes a breach of Regulation 7(1)(c) of the PMLFTR and Section 3.2(iii) and (iv) of the IPs Part I and Section 3.3.2 of the IPs Part II.

Ongoing Monitoring – Scrutiny of Transactions – Regulation 7(2)(a) of the PMLFTR, Section 4.5.2 of the IPs Part I and Section 3.2 (iv) of the IPs Part II

The Company did not obtain information on the purpose and intended nature of the business relationship; therefore, it was not possible to determine whether all the player profiles reviewed were in line with their expected transactional activity and whether additional action was necessary.

The Company did not provide evidence to demonstrate that spot checks, dip sampling or any form of oversight of players' activity were conducted as part of its ongoing monitoring obligations. However, apart from the Company's inability to monitor actual against expected activity even in the absence of a profile, the transactions could still have been monitored and captured by the Company.

Indeed, three (3) player profiles carried out transactions which diverged from either their previous activity or were not synonymous with what one would have expected in the first place. The transactional activity of these three (3) player profiles had increased drastically compared to that seen previously. By way of example, one (1) player profile was a twenty-two (22) year-old who deposited over eight-thousand-euro (€8,000) in cash in approximately ten (10) days. No information other than his age had been requested from the player by the subject person. Considering his age, the Company should have queried the deposits that were carried out in such a relatively short period of time.

Hence, the Committee determined that in these three (3) files the Company had breached its legal obligations in terms of Regulation 7(2)(a) of the PMLFTR, Section 4.5.2 of the IPs Part I and Section 3.2 (iv) of the IPs Part II.

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

After taking into consideration the abovementioned findings together with (i) the nature of the services and products offered by the Company including the size of the Company; (ii) the fact that no representations were submitted by the Company; (iii) the Company was overall cooperative during the compliance examination (iv) the seriousness and at times systemic nature of the obligations breached; iv) the impact that such breaches could potentially have on both the Company and the local gaming industry, (vi) the fact that when the compliance examination took place, the Company had an overall low level of adherence to its AML/CFT legal obligations, as well as a failure to have adequate regard to

ensuring the effective implementation of such obligations (vii) the fact that the Company surrendered their MGA license on 12 August 2021, the Committee decided to impose an administrative penalty of one-hundred and ninety-eight thousand, one hundred and twenty-six euro (€198,126) with regards to the breaches identified in relation to:

- Regulations 5(1), (3) and (4) of the PMLFTR and Section 3.3 of the Implementing Procedures, Part I
- Regulation 5(5)(a)(i) of the PMLFTR and 3.5 and 3.5.2 of the IP Part I, Section 2.2.1, of the IPs Part II
- Regulations 7(1) (a), Section 4.3.1 of the IPs Part I and Sections 3.2(i) of the IPs Part II
- Regulation 7(1)(c) of the PMLFTR and Section 3.2(iii) and (iv) of the IPs Part I and Section 3.3.2 of the IPs Part II
- Regulation 7(2)(a) of the PMLFTR, Section 4.5.2 of the IPs Part I and Section 3.2 (iv) of the IPs Part II

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

By way of clarification the Committee could not proceed to impose a Directive to rake remedial action on the Company, because it had filed for the surrender of its license as explained above.

The administrative penalty hereby imposed is not yet final and may be appealed before the Court of Appeal (Inferior Jurisdiction) within the period as prescribed by the applicable law. It shall become final upon the lapse of the appeal period or upon final determination by the Court.

Key Take aways:

- Subject persons need to assess the risks that they are exposed to because of their operations and the business relationships they engage in. This needs to be done by assessing the inherent risk which depends on the identification of the existent threats and vulnerabilities that arise from risk factors including those relating to customers, countries or geographical areas, products, services, transactions and delivery channels. This level of understanding must exist both at the business level and at an individual customer level (in line with the parameters prescribed in the Implementing Procedures Part II applicable to the remote gaming sector).

- Understanding the purpose and intended nature of the business relationship is crucial. While the purpose of entering a business relationship with a gaming company is self-explanatory, information regarding the nature of employment/business, as well as the usual annual salary is indispensable. On a risk sensitive basis, gaming operations could also have availed of statistical data to develop behavioural models such as through official economic indicators or else data collected over a period by the operator itself and which allows for the creation of a profile of an average player.

- Monitoring customer activity against that expected and the available information on the customer is important. This allows for effective monitoring to be attained. However, where no or limited information is available one should still be able to monitor the activity over time and understand whether there is activity that is either not within the normal activity or is not in line with that of similar players or is exceptionally large or anomalous.

29 December 2022