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 penalties and measures established by the Board of Governors of the FIAU.

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:

23 March 2023

SUBJECT PERSON:

Rhinoceros Operations Limited

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

Offsite Compliance Review carried out in 2022

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €128,796 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 9(1) of the PMLFTR and Section 3.3.2 of the Implementing Procedures (IPs) Part II
- Regulation 7(1) of the PMLTFR and Section 3.3.2 of the IPs Part II
- Regulations 7(1) and 9(1) of the PMLFTR, Section 4.4.2 of the IPs Part I and Sections 3.2 and 3.3.2 of the IPs Part II
- Regulations 7(1) and 8(5) of the PMLFTR and Sections 3.3.2 and 3.6 of the IPs Part II
- Regulation 13 of the PMLFTR and Sections 4.9.2 and Section 9 of the IPs Part I

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Application, Timing and Extent of Customer Due Diligence (CDD) - Regulation 9(1) of the PMLFTR and Section 3.3.2 of the Implementing Procedures (IPs) Part II

While a subject person would usually be expected to apply CDD measures at the moment in time prescribed by the PMLFTR, the risk-based approach allows gaming licensees to apply customer due diligence measures when carrying out transactions that amount to or exceed two thousand euro (€2,000) or more, whether carried out within the context of a business relationship or otherwise. Monitoring for the €2,000 threshold is therefore essential.

In this respect, the Company operated 5 domains and players can have multiple accounts on different brands. However the compliance review revealed that despite the risks associated with such setup being acknowledged in the Company's AML Policies, the policies fell silent on the obligation to calculate the €2000 threshold collectively for a player who opts to register multiple accounts on different brands. Indeed, when asked if there were any systems in place to detect the opening of multiple accounts by the same user, Company officials explained that the checks conducted only produce a result if the user registers multiple accounts on the same brand. So much so that during the player profiles review, it transpired that 4 players who had multiple accounts, had the threshold date calculated per brand.

Consequently, the Committee concluded that considering the serious and systematic failures observed, the Company breached Regulation 9(1) of the PMLFTR and Section 3.3.2 of the IPs Part II.

Identification and Verification - Regulation 7(1) of the PMLTFR and Section 3.3.2 of the IPs Part II

The personal information to be collected, and the extent of verification to be carried out, is to be determined in accordance with the risk posed by the respective client. Nonetheless, during the review, it transpired that the Company failed to obtain and verify players' place of birth and/or nationality, for 8 of the 25 players that had an assigned risk rating of higher than low.

Committee Members expressed that due to insufficient information with regards to the players' personal details, the Company failed to establish systematic procedures for identifying an applicant for business. As a result, and in the absence of such detail, the Company was not able to ensure effective mitigation of risks including that of identity fraud and impersonation. This since such shortcoming could have potentially hindered the Company from determining that the customer is who he claims to be.

In view of the resulting shortcomings, the Committee considered the Company to have breached its obligations in terms of Regulation 7(1) of the PMLTFR and Section 3.3.2 of the IPs Part II.

Information on the Purpose and Intended Nature of the Business Relationship - Regulations 7(1) and 9(1) of the PMLFTR, Section 4.4.2 of the IPs Part I and Sections 3.2 and 3.3.2 of the IPs Part II

The extent of the information/ documentation to be collected, should reflect the level of ML/FT risks identified. Where the risk is not high, a declaration from the customer with details such as the nature of employment/business and usual annual salary can suffice. However, where the risk of ML/FT is higher, the information obtained would need to be supplemented by means of independent and reliable information and documentation.

In this respect, the Committee noted that prior to May 2022, the Company had no procedures in place by which to collect any Source of Wealth information from the customer, nor did it conduct any open-source checks or use statistical models to obtain same. Indeed, it was revealed that the Company failed to request any Source of Wealth information from the players in sixteen (16) files reviewed or was otherwise requested more 30 days after the €2,000 threshold was reached in an additional six (6) files.

Furthermore, in understanding the expected level of activity, the Company was using statistical data to develop behavioural models against which to eventually gauge a customer's activity. However, the Committee observed that this statistical data approach was being adopted for all players irrespective of their risk rating. Concerns in this regard were held given that 9 players reviewed had a medium-high risk rating, and the IPs are clear in stating that the use of statistical data is incompatible with high-risk situations.

The Committee discussed the serious repercussions of not having established measures to ensure that information is obtained to create a comprehensive customer business and risk profile. This shortcoming impinges on the Company's ability to effectively monitor the activity of its customers in order to detect unusual or suspicious activity and to analyse such alerts with the aim of determining whether the filing of Suspicious Transaction Reports (STRs) to the FIAU is warranted.

For these reasons, the Committee deemed the Company to have seriously and systemically failed from adhering to Regulations 7(1) and 9(1) of the PMLFTR, Section 4.4.2 of the IPs Part I and Sections 3.2 and 3.3.2 of the IPs Part II.

Inability to Complete Customer Due Diligence Procedures - Regulations 7(1) and 8(5) of the PMLFTR and Sections 3.3.2 and 3.6 of the IPs Part II

In one file, although the player reached the €2,000 threshold on the 22 December 2020, it was only on 24 August 2021 that the Company requested the provision of source of wealth information. Moreover, despite failing to provide same within a 30-day period, the account was left as active until 24 May 2022. On 24 May 2022 the player's account was blocked for withdrawals and deposits, however of concern was that although the player had not provided the requested documentation the withdrawal block was lifted on 8 June 2022.

In discussing the matter at hand, the Committee recognized that there may be various reasons why a customer may not be forthcoming in the provision of the required information or documentation. However, when such situations arise, on the lapse of the 30-day window the Company was not to allow any activity of any kind on the account held in the customer's name or provide any other service to the customer. To this end, whilst acknowledging that the Company decided to keep the account blocked, it had to ensure that the account has a NIL balance at the time it is blocked, with any funds standing to the credit of any such account being disposed of.

Thus, in view of the breaches outlined above, the Committee determined that the Company has failed to honour its obligations in terms of Regulations 7(1) and 8(5) of the PMLFTR and Sections 3.3.2 and 3.6 of the IPs Part II.

Record Keeping - Regulation 13 of the PMLFTR and Sections 4.9.2 and Section 9 of the IPs Part I

Throughout the compliance review, it was evident that the application of record-keeping by the Company was not in line with its regulatory requirements. For instance, the Company declared that PEP screening records that did not result in any potential hits were only retained as of May 2021, whilst records of potential positive hits were stored since October 2019. Matters were further exacerbated since despite adopting a new procedure in May 2021, the file review revealed that records were still not being appropriately recorded.

The Committee discussed that the Company was required to retain records of any business relationship it enters into. These records are to include any documentation and information produced or obtained in complying with their obligations under the PMLA, the PMLFTR as well as the Implementing Procedures. These records are not only intended to show that the Company complied with its obligations at law but are also indispensable for the Company to monitor the relationships against the initial searches and checks carried out.

In view of the above, the Committee determined that the Company failed in maintaining an efficient record-keeping procedure for PEP screening checks and in being able to retrieve information in a timely manner. Hence, the Committee found the Company to have breached Regulation 13 of the PMLFTR and Section 4.9.2 and Section 9 of the IPs Part I.

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

After taking into consideration the abovementioned breaches by the Company, the Committee decided to impose an administrative penalty of one hundred twenty-eight thousand seven hundred and ninety-six Euro (€128,796) with regards to the breaches identified in relation to:

- Regulation 9(1) of the PMLFTR and Section 3.3.2 of the Implementing Procedures (IPs) Part II
- Regulation 7(1) of the PMLTFR and Section 3.3.2 of the IPs Part II
- Regulation 7(1) and 9(1) of the PMLFTR, Section 4.4.2 of the IPs Part I and Sections 3.2 and 3.3.2 of the IPs Part II
- Regulations 7(1) and 8(5) of the PMLFTR and Sections 3.3.2 and 3.6 of the IPs Part II
- Regulation 13 of the PMLFTR and Section 4.9.2 and Section 9 of the IPs Part I

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. In doing so, the Committee took into consideration the importance of the obligations breached, the level of seriousness of the findings identified, and the extent of ML risk such failures could lead to. The Committee also considered the Subject Person's size and the impact that the Subject Person's failure may have had on both its operations and on the local jurisdiction. The level of cooperation portrayed by the Company and its officials throughout the supervisory process were also factored in.

Under normal circumstances, a Follow-Up Directive would be imposed for the breaches identified in terms of Regulation 21(4)(c) of the PMLFTR, however the Committee took into consideration that the Company is in the process of surrendering its licence. Had the Company not initiated the surrender of its licence, a process to follow up on the measures necessary to ensure compliance with the local AML/CFT legislative provisions, both in relation to the failures for which the Company has been found in breach (as relayed above), as well as on the remedial actions that the Company would have initiated.

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:

- The requirement to link multiple accounts to be able to monitor the activity for the determination of the €2,000 threshold. Such linking is at all more indispensable to monitor all the customer activity in general and in line with the Company's ongoing monitoring obligations particularly in identifying activity that significantly deviate from that expected or that is otherwise anomalous or suspicious.

- The provision of products on a non-face-to-face basis increases the risk of ML/FT and customer impersonation which is due to a number of factors. These include, but are not limited to, the ease of accessing services at any time and from any location, the possibility of setting up multiple accounts

and avoiding detection, the absence of physical documents that can be viewed and the speed with which transactions carried out. Subject persons should therefore remain diligent when undertaking CDD measures as well as assess whether the measures applied, provide sufficient comfort that the customer exists and that he/she is truly who he/she says he is.

- 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 source of wealth 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.

- Screening for PEP status has to be carried out regularly, but it is important that this is done within thirty days of the €2,000 threshold being met, even where licensees may have already screened customers to determine if they were PEPs earlier on in the course of the business relationship. While comprehending that if the time span between the PEP screening and the €2,000 threshold is short one would not need to carry out a fresh check immediately, if there is significant time-lapse between the check and the threshold being reached, one has to ensure that an update check is carried out

27 March 2023