Administrative Penalty 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 established by the Board of Governors of the FIAU.

This Notice provides selected 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:

5 April 2021

SUBJECT PERSON:

Meridian Gaming Limited

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

On-site Compliance Review carried out in 2018

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €88,937 and Remediation Directive in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR)

LEGAL PROVISIONS BREACHED:

- Regulations 5(1) of the PMLFTR and Sections 2.2.1 of the Implementing Procedures Part II Remote Gaming Sector[1]
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 2.2.1 of the Implementing Procedures Part II Remote Gaming Sector
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 4.1.1.1 of the Implementing Procedures Part I[2]
- Regulation 9(1) of the PMLFTR, Section 3.1.1.2 of the Implementing Procedures Part I, and Sections 3.2 and 3.3.2 of the Implementing Procedures Part II Remote Gaming Sector
- Section 3.2(iii) of the Implementing Procedures Part II Remote Gaming Sector
- Regulation 11(1)(b) of the PMLFTR.

[1] Any reference to the Implementing Procedures Part II Remote Gaming Sector within this publication shall be construed to refer to the Implementing Procedures Part II Remote Gaming Sector, amended 19 July 2018.
[2] Any reference to the Implementing Procedures Part I within this publication shall be construed to refer to the Implementing Procedures Part I, issued 27 January 2017.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Regulations 5(1) of the PMLFTR and Sections 2.2.1 of the Implementing Procedures Part II Remote Gaming Sector

The compliance examination revealed that the Company's Business Risk Assessment (BRA) at the time of the onsite examination did not provide a comprehensive assessment of the money laundering/financing of terrorism (ML/FT) risks that the Company was exposed to through its operations. More specifically, the Company's BRA did not elaborate on the anti-money laundering/combating the financing of terrorism (AML/CFT) risk pillars, that is, customer, product/service/transaction, interface and geographical risks in accordance with the standards set by the risk-based approach. In fact, the BRA focused on the strategic, operational, financial, legal aspects, IT and security risks.

The BRA's inadequacies were highlighted by the fact that while the Company offered a wide range of payment methods to its clients, such as bank cards, prepaid cards, and e-wallets, none of such methods was assessed for ML/FT purposes. In fact, since the Company did not evaluate the risks related with these payment methods, it could not determine the measures and controls to mitigate the same.

The Committee noted that the Company claimed that these failures were a direct result of the timing of the compliance examination which occurred in September 2018, only two months after the Implementing Procedures for the Remote Gaming Sector were issued. Whilst the Committee was aware that at the time of the onsite examination, no specific guidelines had been issued to gaming entities in relation to the obligation to perform a BRA, it reiterated that Regulation 5(1) of the PMLFTR had been in force since January 2018. Moreover, on 2 February 2018 the FIAU had issued the "Supervisory Guidance Paper on ML and TF Institutional/Business Risk Assessment" to guide subject persons on drawing up a BRA in line with the new regulatory standards. Therefore, the Committee expected the Company to, at the very least, have tried to incorporate ML/FT risks in the BRA and controls which could manage such risks in a more efficient manner.

As a result, the Committee determined that the Company was in breach of its obligations in terms of Regulation 5(1) of the PMLFTR and Sections 2.2.1 of the Implementing Procedures Part II Remote Sector in view of its failure to carry out a BRA.

Regulation 5(5)(a)(ii) of the PMLFTR and Section 2.2.1 of the Implementing Procedures Part II Remote Gaming Sector

The Company's policies and procedures indicated that it had a Customer Risk Assessment procedure in place to evaluate the ML/FT risks posed by its customers. However, the policies only referred briefly to the four risk pillars without evaluating the degree of exposure each risk factor provided. Nor did they address the way the risks are integrated into the overall customer risk rating.

It was also noted that even though the Company's Customer Acceptance Policy (CAP), illustrated a number of ML/FT red flags, it contained no reference as to how the risks are determined, evaluated, calculated and combined to conclude the comprehensive risk assessment of each customer.

In addition to this, the compliance examination revealed that the Company had not adopted any CRA and risk rating procedures. More specifically, none of the player profiles exceeding the 2,000EUR threshold included any documented CRAs. At the time of the onsite examination, the MLRO simply attempted to assign risk ratings verbally, without providing any evidence that any form of assessment

had been carried out or that these players were at least risk rated. It was also noted that the Company did not have a software tool in place to risk assess its clients, despite its statements to the contrary.

In its representations, the Company clarified that only 4,000 players out of 35,000 needed to be assessed for the purposes of conducting a CRA; an action which the Company claimed to have carried out, however it failed to provide any evidence of the same. The Committee also pointed out that the obligation to perform a CRA is independent of the percentage of the population to be assessed.

Due to the Company's failure to have in place adequate CRA measures and to ensure implementation of the same, the Committee concluded that the Company was in breach of Regulation 5(5)(a)(ii) of the PMLFTR and Section 2.2.1 of the Implementing Procedures Part II Remote Gaming Sector.

Regulation 5(5)(a)(ii) of the PMLFTR and Section 4.1.1.1[3] of the Implementing Procedures Part I

The Company provided a documented CAP which set out the criteria to determine when a business relationship may be established with a customer and when such a relationship should be refused. Furthermore, the Company made available a list of prohibited countries to the FIAU officials.

However, the compliance examination revealed that the Company had onboarded clients from countries that were on its prohibited jurisdiction list. In its representations, the Company explained that these clients were onboarded prior to the introduction of these countries on the prohibited jurisdiction list. Furthermore, the Company clarified that some of these jurisdictions were included in the prohibited jurisdictions list for reasons not related to ML/FT risks and threats.

The abovementioned facts demonstrated that the Company did not comprehensively understand the significance of the ML/FT risks connected with certain jurisdictions and markets, which may expose it to higher risks and threats. In particular, the CAP failed to distinguish between the jurisdictions that were prohibited because of specific ML/FT risks and those which were not allowed due to the business policies of the Company. The Committee also noted that upon introducing the internal restricted country list or when adding additional jurisdictions to the list, the Company should have reviewed its relationships with all of its customers. This would have enabled the Company to determine whether it should terminate any relationships in the case where the customer would be linked to a restricted jurisdiction. If not terminated, the Company should have justified the retention of the relationship and applied the necessary measures in view of the higher risks.

Based on the above, the Committee decided that the Company breached Regulation 5(5)(a)(ii) of the PMLFTR and Section 4.1.1.1 of the Implementing Procedures Part I, as the CAP of the Company was not effectively implemented.

Regulation 9(1) of the PMLFTR, Section 3.1.1.2 of the Implementing Procedures Part I, and Sections 3.2 and 3.3.2 of the Implementing Procedures Part II Remote Gaming Sector

The Committee noted that the Company did not have in place the appropriate customer due diligence (CDD) policies and procedures as will be explained in more detail.

The Company's AML/CFT policies and procedures specified that the request for proof of address of clients is a part of the Enhanced Due Diligence (EDD) process and therefore will be performed only for high-risk clients. The Committee noted that the verification of address cannot be considered as an EDD measure as it is not a mitigating risk factor in high-risk scenarios, as for example with PEP customers or issues with source of funds of clients. However, it was noted that in reality, the Company

[3] Currently section 3.4.1 of the Implementing Procedures Part I, amended on 25 September 2020.

was indeed obtaining verification of address of players as part of its CDD procedures (albeit not always as referred to further below). Therefore, it was concluded that this shortcoming was more of an inconsistency relating to the Company's procedures.

During the onsite examination, it was noted that the Company had not obtained any document verifying the player's residential address for 6 out of 20 files exceeding the EUR 2,000 threshold. On one occasion, the Company had acquired expired documentation as proof of address; whilst in another instance it had accepted a health insurance card as a valid proof of address. The report also pointed out that on two occasions, the Company's employees had accepted documents that were in languages they were not familiar with (Chinese and Danish) as verification of address and had used an online public source to translate the same. The Committee concluded that the Company had failed to follow an adequate procedure to validate the contents of the documents, especially since one of the documents was in a language which does not have a Latin alphabet, has a unique alphabet and structure, and therefore a professional translation was necessary.

Therefore, the Committee decided that the Company was in breach of Regulation 9(1) of the PMLFTR, Section 3.2 and 3.3.2 of the Implementing Procedures Part II Remote Gaming Sector and Section 3.1.1.2 of the Implementing Procedures Part I.

Section 3.2(iii) of the Implementing Procedures Part II Remote Gaming Sector

The Company's AML/CFT policies and procedures did not have any provisions regarding the Company's obligation to obtain information on the purpose and intended nature of the business relationship as part of its CDD procedures. In addition to this, 16 out of 21 player profiles did not have any Source of Wealth or expected Source of Funds (SoW/SoF). The Company clarified that it requested this type of information as part of its EDD procedures. Consequently, the Company had failed to understand that the information regarding the players' purpose and intended nature of the business relationship is a CDD requirement applicable to all customers exceeding the EUR 2,000 threshold and not only applicable to high-risk clients.

As a result, the Committee decided that the Company was in violation of Section 3.2(iii) of the Implementing Procedures Part II Remote Gaming Sector, due to its failure to have in place and implement the necessary policies to be able to establish a comprehensive customer business and risk profile.

Regulation 11(1)(b) of the PMLFTR

The Committee noted how the Company's policies and procedures had failed to grasp the difference between CDD and EDD measures. In effect, the Company was classifying all those customers who had exceeded the EUR2,000 threshold as high-risk customers and requested them to fill in a KYC Form for the purposes of collecting information about the customers' identities, specifications as to whether they are PEPs and details about their SoW/SoF. The Committee noted that this type of information that the Company requesting is a CDD and not an EDD measure because such details are basic information to establish a client's profile.

The examination review also revealed shortcomings in the way the Company implemented the abovementioned procedures. In effect, it noted that the Company was not able to provide evidence that it was collecting detailed information on the players' SoW/SoF or that a Form to declare this was being completed.

Furthermore, the Committee examined the information and the analysis of the clients' profiles. It was observed that on four occasions the Company should have implemented EDD measures to mitigate

the risks arising from these clients' profiles. The jurisdictions that these players were connected to, the high amounts they deposited, the type of payment methods which they utilised, and the lack of additional information in their profiles, evidenced that the Company had failed to understand the ML/FT high risks that it was exposed to through these specific cases. Similarly, the Company failed to apply any EDD measures to confirm that the SoW/SoF of these customers was originating from legitimate sources.

As a result, the Committee decided that the Company was in breach of its EDD obligations as prescribed in Regulation 11(1)(b) of the PMLFTR.

ADMINISTRATIVE 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 eighty-eight thousand, nine hundred and thirty seven Euro (€88,937) with regard to the breaches identified in relation to:

- Regulations 5(1) of the PMLFTR and Sections 2.2.1 of the Implementing Procedures Part II Remote Gaming Sector
- Regulation 5(5)(a)(ii) of the PMLFTR, Section 4.1.1.1 of the Implementing Procedures, Part I and Section 2.2.1 of the Implementing Procedures Part II Remote Gaming Sector[4]
- Section 3.2(iii) of the Implementing Procedures Part II Remote Gaming Sector
- Regulation 11(1)(b) of the PMLFTR

Furthermore, the Committee served the Company with a reprimand for failures to comply with Regulation 9(1) of the PMLFTR, Section 3.1.1.2 of the Implementing Procedures Part I, and Sections 3.2 and 3.3.2 of the Implementing Procedures Part II Remote Gaming Sector.

In terms of its powers under Regulation 21(4)(c) of the PMLFTR, the FIAU also served the Company with a Remediation Directive to ensure that the Company remediates the listed breaches. The Committee directed the Company to make available its policies and procedures as being relayed below and within specific timeframes:

i) A revised BRA which identifies the risks which the Company is exposed to and ensures that that the appropriate measures, policies, controls, and procedures are being adopted to prevent and mitigate such risks.

ii) An updated CRA that is based on the four risk pillars with a methodology explaining the way the CRA works, how each risk factor is scored and how the final risk rating is attained.

iii) A CAP, in line with the standards set by Implementing Procedures.

iv) Updated Due Diligence procedures which specify the information and the documentation required for the verification of a client's address in line with the Maltese regulatory framework. Furthermore, the updated policies should also provide guidance for the proper translation of any documentation that is in a foreign language. Finally, the Company shall ensure that all active client files, as well as prospective customers include the proper CDD documentation.

v) The adoption of policies, procedures, and processes which will enable the Company to establish the customer's business and risk profiles in a comprehensive manner. The information that the Company acquires should be sufficient to establish the customer's risk profiles and therefore needs to include data about the customer's business, employment and occupation.

[4] For the breaches relating to Customer Acceptance Policy and Customer Risk Assessment

vi) Updated EDD policies and procedures which shall ensure that the Company is able to identify higher risk customers and scenarios and the EDD measures that will apply.

In determining the appropriate administrative measures to impose the Committee took into consideration the representations submitted by the Company, the nature and size of the Company's operations, the origin of the Company's clients, the overall impact, actual and potential, of the AML/CFT shortcomings identified vis-à-vis the Subject Person's own operations and the local jurisdiction. The seriousness of the breaches identified together with their occurrence were also taken into consideration by the Committee in determining the administrative measures imposed.

In the eventuality that the requested documentation is not made available within the stipulated timeframes, the Committee shall be informed of this default, to assess the possibility of further eventual action, including the potential imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21 of the PMLFTR.

13 April 2021