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:

1 August 2025

RELEVANT ACTIVITY CARRIED OUT:

Land Based Casino

SUPERVISORY ACTION:

Compliance Review carried out in 2022

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €26,498 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulations 5(1) and 5(4) of the PMLFTR and Sections 3.3 and 8.1 of the Implementing Procedures (IPs);
- Regulation 5(5)(a)(ii) and Section 3.5 of the IPs;
- Regulation 9(1), 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.3 and 4.7 of the IPs;
- Regulation 7(1)(d), 7(2)(a), 11(1)(b), 11(1)(c) and 11(9) of the PMLFTR and Section 4.5 and 4.9 of the IPs;
- Regulations 9 and 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs;
- Regulation 5(5) of the PMLFTR and Sections 3.4 and 5.4 of the IPs;
- Regulation 13 of the PMLFTR and Section 9.2 of the IPs,
- Regulation 5(5)(e) of the PMLFTR and Sections 7.1, 7.2, 7.3 and 7.5 of the IPs.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment (BRA) - Regulations 5(1) and 5(4) of the PMLFTR and Sections 3.3 and 8.1 of the IPs

A BRA was in place at the time of the examination which did consider the majority of the threats and vulnerabilities that the Company may be exposed to and an assessment of the controls applied. Also, the Company did demonstrate knowledge and awareness of the ML/FT risks to which its business is exposed to. Notwithstanding, deficiencies were noted within the Company's BRA methodology, making it unable to fully assess the risks of ML/FT it was exposed to and to adequately apply the required mitigating measures to manage them.

For example, the Company's BRA failed to consider the potential ML/FT risk exposure through the products it provided. Particularly, the extent of unallocated slot machine sessions undertaken by its customers without inserting their membership cards was not considered. Also, while considering links to non-reputable, medium and high-risk jurisdictions, the Company did not identify the main ML/FT risks emerging from such jurisdictions and how such risks may have exposed the Company's operations.

Customer Risk Assessment (CRA) - Regulation 5(5)(a)(ii) and Section 3.5 of the IPs

The Company was assessing the potential risks of ML/FT posed by its customers based on predefined parameters defined as part of its policies and procedures. However, the methodology adopted was not comprehensive enough to enable the Company to fully understand the risks posed by its customers and to effectively apply the required controls. This since, additional ML/FT risk factors were required to be assessed, including: (i) the customer's reputation, and behaviour risk, as well as the potential ML/TF risk from where the customers derive their wealth, their employment or the source of the funds to be used during the business relationship and (ii) clear rationale as to which countries pose the attributed geographical risk.

Customer Due Diligence (CDD) - Regulation 9(1), 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.3 and 4.7 of the IPs

Application, Extent and Timing of CDD Measures

Regulation 9(1) provides that gaming licensees shall 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. Notwithstanding, the Company incorrectly calculated the €2,000 threshold since the Company was not considering the cumulative deposits made since registration for those cases where there was an element of duration[1].

[1] This is being explained within the specific context of the review and the findings on the SP. Land Based Gaming operators have to carry out CDD even when a customer seeks to establish a business relationship, independently of whether or not the €2,000 threshold was reached.

While acknowledging that the Company takes a prudent approach to identify and verify (ID&V) customer at entry point, it should ensure that its policy requires the updating of the ID&V information and/or documentation of its customers once the €2,000 threshold is reached, particularly when significant time may have lapsed between the first entry and the € 2,000 threshold being reached.

Inadequate residential address verification measures applied

For 25% of the files reviewed it was determined that the Company failed to verify its customer's residential address. While acknowledging that it is highly unlikely that any casino customer, would also be carrying documentation verifying his/her permanent residential address when first visiting the casino (in instances where the identification document does not include details on the address of the customer), in these instances the customer subsequently entered the casino multiple times after reaching the €2,000 threshold.

Transaction Monitoring & Enhanced Due Diligence (EDD) - Regulation 7(1)(d), 7(2)(a), 11(1)(b), 11(1)(c) and 11(9) of the PMLFTR and Section 4.5 and 4.9 of the IPs

A transaction monitoring tool was in place by the Company at the time of the compliance review which provided the Company with an amalgamated view of the customers activity. However, shortcomings were identified in relation to the Company's obligation to scrutinise transactions taking place.

Specifically, for 42% of the files reviewed, the Company solely relied on the information provided by the customer within a predefined generic form without corroborating the same with evidence, despite the amounts dropped as well as the higher risk ratings involved. In another 27% of the files, despite the activity undertaken which should have served as an additional trigger, the Company failed to actively obtain any information on the source funding their activity (such as their income brackets) and SoW of such players, this to ensure that the activity undertaken is in line with the customer profile or otherwise. For five of such files, the concerns were further exacerbated given the players' material connection to non-reputable jurisdictions for which the Company was required to undertake EDD measures. Some examples illustrating transaction monitoring and EDD breaches, as applicable, are presented hereunder.

- Over a six-year period, a player dropped €150,850 and although the customer visiting the casino regularly, no information was obtained in terms of the customer's annual income. Thus, the Company did not have enough information to whether the gaming activity was in line with the player's income and confirm that the amount dropped over such a period was deriving from legitimate sources. Moreover, despite the player not providing the requested SoW documentation he was still allowed entry to the casino.

- Over a two-year period, one player dropped €270,415 and when completing the EDD form the player declared an annual income ranging between €20,000 - 49,000 from his employment. Yet this was not corroborated with evidence. While noting the reference to the customer's occupation and income brackets, more documentation with respect to his earnings would have enabled a better assessment of whether the activity is in line with his declared occupation.

It is important to note that all customer files in which shortcomings pertaining to the application of EDD measures were noted also featured deficiencies in transaction monitoring. Therefore, when analysing the portion of customer files reported under the transaction monitoring obligation, the Committee took a holistic approach for files that also had EDD failings, considering breaches related to both obligations in its assessment.

Politically Exposed Persons - Regulations 9 and 11(5) of the PMLFTR and Section 4.9.2.2 of the IPs

Whilst acknowledging that the Company obtained information on the customer's PEP status during the registration process, the Company was required to ascertain whether the status of a customer changed to that of a PEP upon reaching the €2,000 threshold. However, for 30% of the files reviewed it was noted that the Company failed to assess whether the customer was a PEP once the €2,000 deposit threshold was attained, which in most cases the €2,000 deposit threshold was hit several months after initial registration. Notwithstanding, it was positively acknowledged, that since 2019, the Company also introduced a PEP screening system to ensure that customers are regularly monitored, and any hits duly alerted.

Policies & Procedures - Regulation 5(5) of the PMLFTR and Sections 3.4 and 5.4 of the IPs

During the interviews conducted with various employees, any suspicious activity was first to be escalated to the surveillance department that would review the recording and, only if deemed necessary would this be reported to the MLRO. However, the Company is to ensure that its policies and procedures are clear that potential suspicion or knowledge of ML/FT is to be immediately reported to the MLRO. While the policies and procedures did not adequately reflect this, no instance of delayed reporting to the FIAU was observed as part of the review.

Training - 5(5)(e) of the PMLFTR and Sections 7.1, 7.2, 7.3 and 7.5 of the IPs

It was positively acknowledged that the majority of the Company's employees did attend AML/CFT training. However, the training provided was deemed not comprehensive, this since it was not tailored to the Company's AML Policies and Procedures and the ML/FT risks associated with the land-based sector.

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 of twenty-six thousand four hundred and ninety-eight Euro (€26,498) with regards to the breaches identified in relation to:

- Regulations 7(1)(d), 7(2)(a), 11(1)(b), 11(1)(c) and 11(9) of the PMLFTR and Section 4.5 and 4.9 of the IPs

When deciding on the administrative measure(s) to impose, the Committee took into consideration all the information made available by the Subject Person, both during the compliance examination, as well as in the representations submitted. The Committee also considered the importance of the obligations breached, together with the overall seriousness of the findings identified and their material impact. The Committee further noted that the Company did not adequately scrutinize the activity undertaken by some of its players and failed to apply to the appropriate EDD measures when required, which failure could have led to the unintentional facilitation of ML/FT, thus exposing the Company and the jurisdiction at large to unmanaged risks.

As part of reaching its final decision, the Committee also considered the nature, the size and operations of the Company. Positively, the Committee factored in the good level of cooperation exhibited by the Company throughout the entire process and the regard to its AML/CFT obligations. The Committee has also considered the remedial action taken by the Company both before and after the compliance review. Lastly, the Committee ensured that the penalty imposed is effective, dissuasive and proportionate to the failures identified and the ML/FT risks that were perceived during the compliance examination.

In addition to the imposition of an administrative penalty, the Committee served the Company with a Remediation Directive in terms of the FIAU's powers under Regulation 21(4)(c) of the PMLFTR. The purpose of this Directive is for the FIAU to ensure that the Company enhances its AML/CFT safeguards and performs all the necessary remedial actions to attain compliance with its AML/CFT legal obligations emanating from the PMLFTR and the IPs. By virtue of this Directive, the Company is being directed to remediate the identified breaches through the following remedial actions:

- Provide an updated BRA which shall thoroughly consider the potential ML/FT risks that the Company may be exposed to;

- Implement CRA measures that cater for a comprehensive understanding of risks and that allows for the consideration of all the information necessary to risk assess customers;

- Ensuring that it has systems in place which allows for the determination of the €2,000 deposit threshold by taking into account deposits effected by the customer since registration as opposed to the deposits effected by the customer during one gaming session; This to ensure that on a risk based approach especially where significant time has passed between the first entry and the threshold being reached, updated CDD measures and PEP checks are carried out.

- Enhance the measures it has in place to monitor the customer activities to be able to determine instances where the customer gaming activity is not in line with the information available or otherwise where there are material deviations from the patterns of usual gaming activity;

- Revise the Company's measures implemented to ensure that it requests more detailed information and documentation to effectively manage the risks posed by high-risk customers.

- Provide updated Policies and Procedures which adequately cater for the shortcomings identified as part of this review.

- Expected to ensure that it has the necessary measures in place to be able to easily and effectively retrieve all the necessary data, information and documentation necessary to prove compliance with its legal AML/CFT obligations;

- Ensure to provide tailored AML/CFT training to all its employees.

The Directive served on the Subject Person shall ascertain that sufficient and tangible progress is achieved on the adoption and implementation of all the procedures and measures referred to above. In the event that the requested information and/or supporting documentation are not made available within the stipulated timeframes, or the Subject Person falls short of its obligations in terms of this Directive, the subject person's default will be communicated to the Committee for its eventual actions, including the possibility of the imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21(1) of the PMLFTR.

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:

- When assessing the ML/FT risk within the BRA, while the exposure to high-risk and non-reputable jurisdictions may be low, in instances where such exposure exists, subject persons are still to ensure to undertake an assessment of the ML/FT risk tied to the specific jurisdictions and to ensure to apply the required mitigating measures. Also, merely stating that all EU/EEA jurisdictions are of low risk without a valid assessment backing up such a generic all-encompassing statement is not acceptable. Instead, subject persons should consider the potential risks specific to each jurisdiction to which it was exposed to, including and not limited to risks of tax evasion, corruption, bribery and terrorism financing.

- Gaming licensees shall 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. Therefore, monitoring is essential and gaming licensees should ensure that they are able to determine the moment in time when CDD measures need to be undertaken that is, either when the €2,000 threshold is met or when a business relationship is established (due to the element of duration).

- While collecting information from pre-defined forms may aid in monitoring the activity undertaken by players, it is imperative for subject person to ensure that the any forms used enable the collection of sufficient details to be able to understand the customer. This would necessarily include details about the source funding their gaming activity (more often than not through details about their employment) and corroborate the statements made when required, this including where higher risk is observed and when material activity is being undertaken. understanding the source of wealth of customers may also be required where their funding streams are derived through the same.

- It is acknowledged that it is highly unlikely that any casino customer, would be carrying with them verification documents pertaining to their permanent residential address (unless their identification document includes as much). Therefore, the IPs encourage Casino Licensees to inform their customers beforehand that in the eventuality of habitual visits to the Casino, customers would be required to produce additional documentation to verify their residential address.

1 August 2025