Administrative Measure Publication Notice

This Notice is being published by the Financial Intelligence Analysis Unit (the FIAU) in terms of Article 13C of the Prevention of Money Laundering Act (the 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.

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

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

14 July 2026

SUBJECT PERSON:

Goldwin Ltd

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

Compliance examination carried out in 2022

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

An administrative penalty of €80,907 in terms of Regulation 21 of the Prevention of Money Laundering and Financing of Terrorism Regulations (the PMLFTR)

LEGAL PROVISIONS BREACHED:

- Regulation 5(5)(a)(ii) of the PMLFTR, Section 3.5 of the FIAU Implementing Procedures – Part I (the IPs – Part I) and Sections 2.2.1 and 2.2.2 of the FIAU Implementing Procedures – Part II for the Remote Gaming Sector (the IPs – Part II)
- Regulation 11(5) of the PMLFTR, Section 4.9.2.2 of the IPs – Part I, and Section 3.4 of IPs – Part II

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Customer Risk Assessment (CRA) – Breach of Regulation 5(5)(a)(ii) of the PMLFTR, Section 3.5 of the IPs – Part I, and Sections 2.2.1 and 2.2.2 of the IPs – Part II

The compliance examination report revealed that the Company had not established or implemented a CRA methodology in line with regulatory requirements. Moreover, it transpired that CRAs made available to the Supervisory Officials in respect of the sampled player profiles had been prepared solely for the purposes of the compliance examination. With respect to the remainder of its customer base, the Company assigned players a first and latest risk categorisation at different stages of the business relationship, based on a very limited set of data points, including the player's country of registration, registration or affiliate source, email domain, and the status of Customer Due Diligence (CDD) process.

According to the Committee, such risk categorisations did not amount to fully-fledged CRAs, particularly since they failed to encompass all four risk pillars and included insufficient detail as to the manner in which the resulting risk ratings were derived. In this regard, the Committee noted that the customer risk and product/service/transaction risk pillars were entirely omitted, with the remaining two pillars, i.e., geographical risk and delivery channels/interface risk, being addressed only to a limited extent. More specifically, geographical risk was partially considered through the customer's country of registration, whilst delivery channels/interface risk was partially considered through the registration or affiliate source. Taking into account the above-mentioned points, the Committee could not accept the system-generated risk ratings, in isolation, as being tantamount to a CRA. The Committee also noted with concern that, within its representations, the Company did not provide any evidence whatsoever to demonstrate that its customer base had subsequently been risk assessed afresh, so as to ensure that a proper CRA was in place for all players.

The Company's lack of compliance with its CRA obligations resulted in a failure to understand the money laundering and funding of terrorism (ML/FT) risks presented by its customers, and how such risks were identified, assessed, weighted, and ultimately translated into a single reasoned customer risk rating. This shortcoming, in turn, significantly impaired the ability of the Company to implement effective and proportionate CDD and ongoing monitoring measures. The seriousness of the matter is further compounded when considering the substantial value and volume of transactions processed by the Company during a period in which no meaningful CRA controls were in place.

In its deliberations, the Committee emphasised that, having regard to the dates on which the Company obtained its licence from the Malta Gaming Authority (the MGA) and subsequently became operational, it had, by the time of the compliance examination, systematically failed to carry out a proper CRA in respect of virtually its entire customer base for a period spanning over two years. The Committee also noted that not only had the CRA obligation been in place since the inception of the IPs – Part I in May 2011, but that, by the time the Company started servicing customers, the FIAU's expectations in relation to risk understanding and assessment, including within the context of the remote gaming sector, were clearly established and widely known. Further to this,

ample information and guidance concerning the requirements relating to the CRA had been made available to subject persons for several years by that point.

Even though the Committee was aware of the fact that, post-compliance examination, the Company implemented various updates to its internal policies and procedures and initiated an internal audit exercise to identify areas necessitating remediation and improvement, such actions do not negate the material shortcomings observed in the Company's CRA framework. Of particular concern was the absence of a documented CRA methodology at the time of the compliance examination, coupled with the Company's failure to conduct CRAs for its customers, instead relying solely on the allocation of initial and latest risk categorisations which could not be accepted as constituting a proper CRA that is grounded in the four risk pillars and meets the requirements of the PMLFTR and the IPs.

Politically Exposed Persons (PEPs) – Breach of Regulation 11(5) of the PMLFTR, Sections 4.9.2.2 of the IPs – Part I, and Section 3.4 of the FIAU Implementing Procedures – Part II

During the compliance examination, it transpired that PEP screening had not been carried out within thirty (30) days of the €2,000 deposit threshold being reached for all player profiles reviewed. Notably, the earliest PEP checks evidenced were dated only a few days or weeks prior to the commencement of the compliance examination, or were performed during the course of the examination itself.

Although the Committee acknowledged that this deficiency was remediated following the compliance examination, the fact still remains that, for a prolonged period of time, the Company had operated without checking whether its customers qualified as PEPs, thereby potentially exposing the Company to a heightened level of risk without the required mitigating measures and controls in place. Indeed, had any customers actually been PEPs, this would have merited the application of Enhanced Due Diligence (EDD) measures, as required by law.

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

After taking into consideration the above-mentioned findings, the Committee decided to impose a combined administrative penalty of €80,907 for the breaches identified in relation to:

- Regulation 5(5)(a)(ii) of the PMLFTR, Section 3.5 of the IPs – Part I, and Sections 2.2.1 and 2.2.2 of the IPs – Part II
- Regulation 11(5) of the PMLFTR, Section 4.9.2.2 of the IPs – Part I, and Section 3.4 of IPs – Part II

In arriving at the final amount of the administrative penalty to impose, the Committee took into consideration a range of factors. The Committee could not but stress the importance of the AML/CFT obligations breached, together with the overall seriousness of the findings identified and their material impact. However, the Committee is cognisant of the fact that the Company's licence was cancelled by the MGA in 2025 and that it no longer carries out relevant activity, which alleviates concerns regarding future risk exposures. During its deliberations, the Committee also considered the nature, size, and operations of the Company, and how the services it rendered may have impacted the local jurisdiction as a whole. Adding to this, the Committee factored in the level of cooperation exhibited by the Company throughout the entire supervisory process, the overall regard towards its AML/CFT

obligations, and the fact that some degree of remediation was at least attempted on the part of the Company. Lastly, the Committee ensured that the administrative penalty imposed was effective, dissuasive and proportionate to both the failures identified and the ML/FT risks perceived during the compliance examination.

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 takeaways

- In accordance with Section 3.5 of the IPs – Part I, it is essential for subject persons to ensure the implementation of a robust CRA framework that comprehensively covers each of the four risk pillars, namely, customer risk, geographical risk, product/services/transaction risk, and delivery channels/interface risk, taking into account the relevant risk factor specificities outlined in Section 3.5.1(a) of the IPs – Part I and Section 2.2.2 of the IPs – Part II. In terms of timing, the CRA is to be carried out upon the establishment of the business relationship and, within the context of the remote gaming sector, no later than thirty (30) days from the point at which the €2,000 deposit threshold is reached.

- Once completed, the CRA is not intended to remain static and should, as per Section 3.5.1 of the IPs – Part I, be reviewed and updated on an ongoing basis, commensurate with the level of risk associated with the particular business relationship, and especially where an event arises marking a material departure from the customer's established risk profile, as may be identified through the ongoing monitoring of transactions.

- The CRA should also be capable of producing consistent and risk-sensitive outcomes, without undue reliance on subjective judgements that could result in variations across assessments. Moreover, the CRA process needs to be clearly documented, outlining the underlying methodology applied, the relevant risk factors considered, and the manner in which such factors are weighted and assessed, this to support the assignment of a risk rating that accurately reflects the ML/FT risks associated with the customer concerned.

- As delineated in Section 4.9.2.2 of the IPs – Part I, subject persons must have appropriate procedures in place that enable them to determine whether a customer or a beneficial owner (current or prospective) is a PEP, and to subsequently apply EDD measures when establishing or continuing business relationships with such a person. Furthermore, for remote gaming operators, Section 3.4 of IPs – Part II requires that PEP checks be performed within thirty (30) days of the €2,000 deposit threshold being met.

16 July 2026