Settlement Agreement 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 Penalties and Measures established by the Board of Governors of the FIAU.

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

DATE ON WHICH SETTLEMENT WAS CONCLUDED:

17 September 2026

SUBJECT PERSON:

European Lotto and Betting Limited

RELEVANT ACTIVITY OR FINANCIAL BUSINESS CARRIED OUT:

Gaming Company

SUPERVISORY ACTION:

Compliance Examination carried out in 2022

SETTLED AMOUNT:

€61,607

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

An administrative penalty of €94,780 and a Follow-Up Directive in terms of Regulations 21 and 23(1)(c) of the Prevention of Money Laundering and Financing of Terrorism Regulations (the PMLFTR).

A settlement agreement was entered into by European Lotto and Betting Limited (the Company) and the FIAU in accordance with Regulation 22 of the PMLFTR, as further elaborated in the Settlement Agreement Policy issued by the FIAU in April 2026[1]. By means of the execution of the settlement agreement, the Company has satisfied all the conditions included in the aforementioned Settlement Agreement Policy. Accordingly, the original administrative penalty of €94,780 was reduced by thirty-five percent (35%), resulting in a revised administrative penalty of €61,607.

[1] https://fiaumalta.org/app/uploads/2026/04/Settlement-Agreement-Policy.pdf.

LEGAL PROVISIONS BREACHED:

- Regulations 5(5)(a) and 13 of the PMLFTR and Sections 3.5.2, 3.5.3 and 9.2(a)(iii) of the FIAU Implementing Procedures – Part 1 (the IPs – Part I), and Sections 2.1.2, 2.1.3, 2.2.1, 2.2.2, 3.3.1(v) and 3.3.2 of the FIAU Implementing Procedures – Part II for the Remote Gaming Sector (the IPs – Part II)
- Regulations 5(5)(a) and 7(1)(c) of the PMLFTR, Sections 4.4.2 and 4.4.3 of the IPs – Part I, and Sections 3.2(iii) and 3.3.2 of the IPs – Part II;
- Regulations 7(1)(d), 7(2)(a), and 11(9) of the PMLFTR, Sections 4.5.2, 4.5.2.2 and 4.8 of the IPs – Part I, and Section 3.2(iv) of the IPs – Part II;
- Regulation 11(5) of the PMLFTR, Section 4.9.2.2 of the IPs – Part I, and Section 3.2 of the IPs – Part II.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Customer Risk Assessment (CRA) - Breach of Regulations 5(5)(a) and 13 of the PMLFTR and Sections 3.5.2, 3.5.3 and 9.2(a)(iii) of the IPs – Part 1 and Sections 2.1.2, 2.1.3, 2.2.1, 2.2.2, 3.3.1(v) and 3.3.2 of the IPs – Part II

During the compliance examination, the Company was found to be operating two Customer Risk Assessment processes: a manual process and an automated system. Both methodologies were considered inadequate, as they did not sufficiently assess key customer, payment, and interface risk factors. The automated system also used gaming activity data with limited historical coverage and restrictive scoring, making higher-risk classifications difficult to reach. The Report also identified inconsistencies in the application of the process, including conflicting risk ratings, unsupported default low-risk classifications for a large customer segment, delays in completing assessments after applicable thresholds were met, and instances where no assessment was carried out for certain account structures (such as master accounts).

In its representations, the Company submitted that its framework drew on several interconnected control areas and ongoing monitoring measures. It further explained that it has discontinued its two CRA methodologies and replaced them with a single, documented and consistent CRA methodology, delivered through a multi-layered framework. This framework assesses customer, geographical, product, payment, transaction and interface risks, and takes into account the customer's expected level of activity, which is determined through statistical data as part of a risk-based approach. This was evidenced through the Company's latest CRA methodology, as well as through the examples of CRAs provided.

The Company also clarified that certain account structures are now subject to a risk assessment before onboarding and that the issue resulting in delays in the completion of the relevant CRAs had been remediated. In this regard, the Company's policies and procedures evidence that a CRA is conducted for each customer who reaches a cumulative deposit threshold of EUR 2,000 within a 180-day period.

Customer Profiling – Breach of Regulations 5(5)(a) and 7(1)(c) of the PMLFTR, Sections 4.4.2 and 4.4.3 of the IPs – Part I, and Sections 3.2(iii) and 3.3.2 of the IPs – Part II

The Report found that the Company had not, in a number of instances, obtained and recorded sufficient information to establish a comprehensive customer profile. The Report further noted that the Company's policies and procedures for assessing expected customer activity were not sufficiently robust, as these were not risk-based, and instead focused heavily on pre-defined thresholds and economic indicators across the entire customer base in a uniform manner.

In its representations, the Company submitted its updated customer profiling framework which ensures that customer information is collected, reviewed and updated on a continuous and risk-sensitive basis throughout the business relationship. The Company explained that customer profiles are established at onboarding and developed through ongoing monitoring, CRA triggers and EDD reviews. Information on occupation, expected activity, SOW/SOF and customer behaviour is obtained through open-source checks, transactional analysis and direct customer requests, where warranted. The Company's policies and procedures further evidence the implementation of statistical models and country-specific loss thresholds to identify activity inconsistent with the customer's profile and to support timely escalation, review and action. It also outlines circumstances which would, where applicable, warrant further SoW and/or SoF substantiation.

Transaction Monitoring - Breach of Regulations 7(1)(d), 7(2)(a), and 11(9) of the PMLFTR, Sections 4.5.2, 4.5.2.2 and 4.8 of the IPs – Part I, and Section 3.2(iv) of the IPs – Part II

The Report found that the Company's transaction monitoring framework did not adequately support the ongoing scrutiny of customer activity. Monitoring was mainly driven by pre-defined transactional thresholds, notwithstanding policy requirements to apply enhanced scrutiny to complex, unusually large, or otherwise unusual transactions. The Report further noted that several reviewed customer files exhibited indicators warranting enhanced scrutiny, including high transaction volumes, sudden deposit spikes, the use of multiple payment methods, and transactions involving third-party accounts. Despite the presence of these risk indicators, enhanced reviews and adequate source of wealth (SoW) and source of funds (SoF) assessments were not consistently performed.

Following the compliance examination, the Company updated its transaction monitoring framework which operated through several interlinked control streams, supported by automated and ancillary monitoring tools. It maintained that customer activity was subject to continuous oversight and that enhanced measures, including additional information requests, documentary substantiation, and account restrictions or closures, were applied where relevant triggers were met. Furthermore, the Company has implemented controls to identify any potential third-party payments though daily reports and real-time alerts. It further explained that it has since started assessing transactional activity against the customer's risk profile, known financial circumstances and expected level of activity. In addition to this, the Company also provided as evidence file-specific submissions and outlined that remedial action was taken in relation to files with identified shortcomings, in line with its internal procedures and regulatory obligations.

Politically Exposed Persons - Breach of Regulation 11(5) of the PMLFTR, Section 4.9.2.2 of the IPs – Part I, and Section 3.2 of the IPs – Part II

For a number of customer files reviewed, PEP screening was not always carried out within the required timeframe following the customer reaching the applicable deposit threshold of €2,000.

In its representations, the Company stated that this stemmed from an error in the configuration of the PEP screening reports at the time, which has since been rectified. Further, the Company also provided evidence that it uses an automated third-party screening solution for this purpose. Customers reaching the applicable threshold within a 180-day rolling period are automatically identified through the Company's internal reporting system, submitted for screening, and thereafter subject to regular rescreening.

THE COMMITTEE'S REASONS FOR ENTERING INTO SETTLEMENT

The Committee considered that the administrative breaches identified during the 2022 Compliance Examination stemmed from deficiencies in the Company's AML/CFT framework as implemented at the time, particularly in relation to the effectiveness and consistency of its CRA process, customer profiling, transaction monitoring and PEP screening controls. While the shortcomings affected the Company's ability to demonstrate a sufficiently comprehensive and risk-sensitive understanding of its customers during the relevant period, the Committee noted that the Company had taken active steps to address the matters identified. In particular, the Committee took into account the implementation of a single documented CRA framework, enhancements to the customer profiling and transaction monitoring processes, the remediation of reporting and screening configuration issues, the reassessment of relevant customer populations, and the introduction of more systematic ongoing monitoring and review mechanisms. The Committee also positively considered the Company's cooperation throughout the process, including the submissions and supporting evidence provided during the representations stage.

Having considered the foregoing, the Committee assessed whether it could propose a settlement agreement in accordance with Regulation 22 of the PMLFTR, as further elaborated in the FIAU's Settlement Agreement Policy. Whilst the Committee is of the view that the administrative breaches involved were serious and systematic, warranting the imposition of an administrative penalty and a Follow-Up Directive, it also took into account the Company's admission of the administrative breaches, the efforts undertaken by the Company's Board of Directors to implement remedial measures prior to the Settlement Process, and the effective investment in compliance made by the Company towards enhancing its AML/CFT compliance framework. The Committee therefore considered that the matter merited a settlement agreement proposal, while still ensuring that the administrative measure imposed remained effective, proportionate and dissuasive.

Taking into consideration all relevant elements, the Committee decided to impose an administrative penalty of €94,780. By means of the execution of the settlement agreement, this penalty was reduced by thirty-five percent (35%):

- Admission of breaches following the receipt of the Potential Breaches Letter, up to the submission of the Representations (15%); and
- Remediation implemented after compliance visit or at representation stage (20%).

This resulted in a revised administrative penalty of sixty-one thousand six hundred seven euro (€61,607).

Key Takeaways

- In accordance with Section 3.5 of the IPs – Part I, subject persons must implement a robust CRA framework that comprehensively considers the relevant risk pillars, including customer, geographical, product/services/transaction and delivery channel/interface risks. Such framework should be clearly documented, consistently applied and capable of producing risk-sensitive outcomes based on the customer's specific risk factors.

- 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.

- Subject persons are to remember that the main purpose for collecting information and/or documentation on the customer's nature of employment and source of wealth is so that they can establish a business and risk profile and eventually scrutinise transactions against such profile. The availability of the said information (and documentation, where the risk is higher) is key to detect any unusual activity in the course of the business relationship.

- Subject persons are required to maintain an effective transaction monitoring framework capable of promptly identifying transactions that are inconsistent with a customer's profile, appear unusual or suspicious, or lack an apparent business or economic rationale. Where warranted on a risk-sensitive basis, additional information and supporting documentation should be obtained to verify the legitimacy of such transactions.

- 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