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:

10 November 2026

SUBJECT PERSON:

N1 Interactive Limited

RELEVANT ACTIVITY OR FINANCIAL BUSINESS CARRIED OUT:

Gaming Company

SUPERVISORY ACTION:

Compliance Examination carried out in 2022

SETTLED AMOUNT:

€139,602

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

An administrative penalty of €232,671 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 N1 Interactive 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 €232,671 was reduced by forty percent (40%), resulting in a revised administrative penalty of €139,602.

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

LEGAL PROVISIONS BREACHED:

- Regulations 5(5)(a), 7(1)(c), 7(1)(d) and 7(2)(a) of the PMLFTR, Sections 3.4, 4.4.2, 4.5.1(a) and 4.5.2 of the FIAU Implementing Procedures – Part I (the IPs – Part I), and Sections 3.2(iii) and 3.2(iv) of the FIAU Implementing Procedures – Part II for the Remote Gaming Sector (the IPs – Part II)
- Regulations 5(5)(a) and 5(5)(a)(ii) of the PMLFTR and Sections 3.4 and 3.5 of the IPs – Part I

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Customer Profiling and Transaction Monitoring – Breach of Regulations 5(5)(a), 7(1)(c), 7(1)(d) and 7(2)(a) of the PMLFTR, Sections 3.4, 4.4.2, 4.5.1(a) and 4.5.2 of the IPs – Part I, and Sections 3.2(iii) and 3.2(iv) of the IPs – Part II

The Report identified shortcomings in relation to the collection of source of wealth (SoW) information and supporting documentation for a substantial proportion of players. During the compliance examination, the Company was also found not to have collected information on the anticipated activity for any of the player profiles reviewed. In most affected cases, the relevant information and documentation had not been obtained whatsoever, while in others these were collected after the lapse of 30 days from when the €2,000 deposit threshold was reached. Furthermore, although the Company's AML Procedure made reference to the requirement surrounding the collection of SOW information and supporting documentation, limitations in the Company's infrastructure impeded their effective implementation in practice. At the time of the examination, the Company's AML procedures also lacked sufficient detail regarding the extent and type of SOW information/documentation required based on the player's assigned risk rating.

The identified shortcomings in the Company's customer profiling framework directly undermined the effectiveness of its transaction monitoring since they prevented the Company from establishing sufficiently comprehensive player profiles against which transactions could be scrutinised. In fact, despite the vast majority of players reviewed having deposited, and in many instances lost, significant amounts, the Company was found not to have obtained sufficient SoW/source of funds (SoF) information and/or supporting documentation. Several cases also involved significant transactional velocity over short periods, further underscoring the need for timely profiling and effective scrutiny of transactions.

In its representations, the Company submitted that it had introduced a SoW/SoF questionnaire that would be automatically triggered upon a player meeting the €2,000 deposit threshold, irrespective of the player's risk rating. This questionnaire, a copy of which was provided by the Company, requires information on players' anticipated levels of activity, SoW, and SoF, and captures data points such as their source of income, annual earnings, expected level of spending, employment status, and occupation. Ultimately, the questionnaire is intended to establish a player's financial circumstances and anticipated level of activity, while also providing a basis against which subsequent transactional activity can be assessed. The Company further explained that accounts are now blocked where the required information or supporting documentation remains outstanding beyond the prescribed period. As for transaction monitoring, the Company explained that it had implemented an automated, alerts-based system incorporating real-time monitoring logic to detect unusual deposit patterns, high-value and high-velocity transactional activity, withdrawals without corresponding wagering activity, and potential structuring. This system is supplemented by monthly reviews of leading depositors to assess consistency between observed activity, behavioural patterns, and SoF information. In addition, the Company will be implementing further enhancements including monitoring of the wider customer base to identify deviations between the declared

profile and the actual activity. Lastly, the Company also reported that it had since updated its AML/CFT policies and procedures to address the abovementioned shortcomings, copies of which were provided, whilst also ramping up resources across management and operational levels of its AML/CFT function to support effective implementation.

Customer Risk Assessment (CRA) - Breach of Regulations 5(5)(a) and 5(5)(a)(ii) of the PMLFTR and Sections 3.4 and 3.5 of the IPs Part I.

During the compliance examination, the Company was found to be using an automated CRA system, updated weekly to reflect changes in player activity. The Report identified shortcomings in the Company's policies and procedures relating to the CRA, which did not specify that a CRA is required to be conducted for business relationships, nor did it mandate the documentation of the rationale underlying the CRA and resulting risk assessments outcomes. In terms of the CRA methodology applied by the Company at the time of the compliance examination, it was found to lack sufficient depth and clarity on the scoring and the calculation of the overall risk rating. Furthermore, certain high-risk indicators were not adequately reflected in the CRA, such as those linked to jurisdictional exposure and transactional activity, thereby resulting in an overall risk rating that did not always reflect the level of ML/FT risk presented.

In its representations, the Company acknowledged the above-described deficiencies identified in relation to its CRA policies and procedures, further explaining that enhancements had commenced both prior to and during the compliance examination as part of its remediation plan. In addition, the Company noted that the legacy CRA had since been replaced by a revised model which assesses country, age, politically exposed person (PEP) and sanctions, lifetime value, payment, and monthly spend risks. The assessment draws on a range of data points, including player age and date of birth, duration of the relationship, country of residence, aggregate deposits and cashouts, payment method utilised, and monthly spend levels. Weighted multipliers apply to lifetime value and monthly spend, enabling high deposits to potentially trigger a high-risk classification and enhanced due diligence measures.

The Company also outlined further improvements supporting the ongoing refinement of its CRA framework. These include configurable rule weightings, risk categories and score ranges, functionality to assess the impact of proposed changes, and the ability to enable or disable rules as well as to add, remove or modify risk factors. The abovementioned remedial actions were evidenced through the updated CRA methodology submitted by the Company.

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 timing, implementation, and effectiveness of its customer profiling, transaction monitoring and CRA processes. 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 undertaken remediation to address the matters identified. In particular, the Committee took into account the Company's implementation of a SoW/SoF questionnaire that is automatically triggered upon reaching the €2,000 deposit threshold, the replacement of the previous CRA process with an automated risk-scoring framework incorporating customer and transactional risk indicators, as well as the deployment of automated, alerts-based transaction-monitoring system, which is supplemented by monthly reviews of the highest depositors. The Committee also positively considered the

Company's cooperation demonstrated throughout the examination, representations, and settlement process.

Having considered the foregoing, the Committee assessed whether it could offer 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 successful efforts undertaken by the Company to initiate the implementation of 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 €232,671. By means of the execution of the settlement agreement, this penalty was reduced by forty percent (40%):

- Admission of breaches following the receipt of the Potential Breaches Letter, up to the submission of the Representations (15%); and
- Remediation implemented before the intervention carried out by the FIAU (25%).

This resulted in a revised administrative penalty of one hundred thirty-nine thousand six hundred two euro (€139,602).

Key Takeaways

- Subject persons are to remember that the main purpose for collecting information and/or documentation on the customer's business/occupation/employment and SoW 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.

- 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.

13 November 2026