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 administrative 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:

31 August 2023

SUBJECT PERSON:

CS Litto Limited

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

Compliance review carried out in 2020

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €52,889 and a Reprimand in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 5(1) of the PMLFTR and Section 3.3 of the Implementing Procedures (IPs) Part I.
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs Part I ad Section 2.2 of the IPs Part II.
- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs Part I and Section 3.2 of the IPs Part II.
- Regulation 7(1)(d) and Regulation 7(2)(a) of the PMLFTR, Section 4.5 and Section 4.8 of the IPs Part I and Section 3.2 and Section 3.3 of the IPs Part II.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment (BRA) – Regulation 5(1) and Section 3.3 of the IPs Part I

The methodology adopted by the Company and the information contained within its BRA provided at the time of the compliance examination was deemed not comprehensive for several reasons, this since it failed to:

- Consider the risks associated with interface/delivery channel. Hence, the Company's BRA failed to identify the risks it faced from onboarding players on a non-face to face basis. This, despite the nature of the Company's operations which unavoidably exposes it to interface risk deriving across all its operations, hence such risk had to equally be considered. Also, such risk understanding is a crucial consideration in line with the four (4) risk pillars of the IPs.
- Refer to quantitative data being used in determining the likelihood of risks materialising. For example:
    - The Company offered a casino-based product, however, the BRA did not consider the number of players that resorted to such a product.
    - In the case of potentially anonymous payment methods (including pre-paid cards), the Company's BRA failed to consider the number of players that resorted to such payment methods.
- Assess the effectiveness of the controls in place and how they mitigate the AML/CFT risks posed to the Company.

Notwithstanding, the Company's proactive approach to revise subsequent BRA's provided to the FIAU following the examination through the annual REQ submission was positively acknowledged.

Customer Risk Assessment (CRA) - Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs Part I and Section 2.2 of the IPs Part II.

The CRA methodology adopted by the Company as at the time of the compliance examination was found to be inadequate as, similar to the BRA, this was also not considering the risk posed by the interface/delivery channel for each of its players.

Also, for all customers sampled as part of the examination, the Company failed to provide the CRA document illustrating the assessment of risks carried out. Instead, the Company merely provided a 'timeline of events' document which only indicated the final risk rating assigned to the players, this without providing any information on the risk factors that formed the basis of such rating and therefore there was no rationale behind the determination of such risk rating.

Purpose & Intended Nature - Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs Part I and Section 3.2 of the IPs Part II

Whilst acknowledging that for the majority of the players the Company did provide screenshots of SoW/SoF questionnaires which included a question specifically on the expected level of activity of the players, the Company failed to obtain information on the expected level of activity from two of the player profiles reviewed which were rated as posing a low risk of ML/FT. Nor did the Company obtain a declaration from the customer with employment details or annual salary. Hence, this prevented the Company from building a comprehensive customer business and risk profile for these players.

While the Company stated to have obtained the required information from a statistical model, which would have been a good approach for customers not rated as high risk, the reputability of such source was deemed inadequate as the Company failed to provide evidence that it has the required access to obtain the necessary data to establish the expected level of activity for such customers.

However, positively, the Committee noted that such failures were one off instances, and the Compliance Review did not identify findings with respect the purpose and intended nature of the business relationship in the majority of the files reviewed.

Transaction Monitoring - Regulations 7(1)(d) and 7(2)(a) of the PMLFTR, Section 4.5 and Section 4.8 of the IPs Part I and Section 3.2 and Section 3.3 of the IPs Part II

For one player reviewed during the examination, it was noted that the Company failed to adequately scrutinize the transactions undertaken. This since despite the changes in gaming patterns or other irregular activities taking place on this particular player profile, the Company failed to conduct checks in a timely manner to ensure that the funds derived from legitimate sources. More details are set out hereunder:

- The player declared that he will be depositing approximately €16,000 per month. However, over a five-month period the player deposited over €90,000 and withdrew none. Monthly deposits ranged from €18,000 to €28,000.

  The Company had collected a bank statement showing a closing balance of approximately €120,000 and the player's salary amounting to approximately €2,400 being credited in the bank account. However, although the player had a high balance in his bank account, there was not enough documentation to confirm that such funds were from his own savings. This, also because the bank statement did not provide details to understand from where the closing balance was being sourced, but rather the balance the customer had in his bank account. Hence, the Company was expected to verify the source of such savings and, especially, clarify how the player managed to source over €90,000 in deposits from what appeared to be a monthly salary of €2.4k per month.

  In its representations, the Company held that it had on file another bank statement (for the same bank account which shows an even greater closing balance of approximately €164,000 and a payment of €7,700 being received in the bank account (which related to a work bonus). Despite this, the Company was still required to confirm the origin from where such wealth had derived. Also, the player's employment information (office worker) was very generic and certainly not enough for the Company to ascertain the veracity of the player's statement that his assets represented the savings deriving from his employment income. The Company should have enquired and requested for further evidence to confirm from where the customer was funding his gaming activity.

Whilst acknowledging that the Company did eventually temporarily suspend the player's account, this was done after the player had deposited over €40,000 without collecting any documentation. The Committee also noted that the Company did eventually fully suspend the account, this was done 5 months after the players registration and coincided with the time of the examination, however it could still not disregard that the Company failed to ascertain the veracity of the customers accumulated wealth and still allowed the player to deposit over €90,000 in such a short period of time.

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

When deciding on the appropriate administrative measures to impose, in addition to the specific breaches outlined above, the Committee took into consideration the importance of the obligations being breached, the level of seriousness, and at times systemic nature, of the breaches identified, as well as the extent of ML/FT risk such failures could lead to.

The Committee was particularly concerned with the Company's failure to conduct adequate transaction scrutiny in a timely manner to ensure that the funds derived from legitimate sources with respect to one of its players. Moreover, the Company's BRA revealed various shortcomings which convey that this assessment was not reflecting all the threats and vulnerabilities to which the Company's business was exposed to. Furthermore, the Committee considered that the CRA methodology adopted by the Company at the time of the compliance examination was inadequate due to lack of consideration to interface/delivery channel risk posed and absence of the rationale behind the individual ratings assigned to each player.

The Committee also considered the Company's size, that this is not a large gaming institution as well as the impact that the subject person's failures may have had on both its operations and on the local jurisdiction. The good level of cooperation portrayed by the Company throughout the supervisory process was also factored in, including the Company's statements that it had already commenced working on remediating its position following the compliance review. This was also evidenced through documentation provided as well as explained by Company representatives during their oral hearing with the Committee. However, overall the Committee couldn't but note that, at least up until the compliance review, the failures observed confirm that the Company did have failures in adhering to its AML/CFT obligations, and that its regard to such obligations had to be enhanced.

After taking into consideration the abovementioned, the Committee decided to impose an administrative penalty of €52,889 with regards to the breaches identified in relation to:

- Regulation 5(1) of the PMLFTR and Section 3.3 of the IPs Part I.
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs Part I ad Section 2.2 of the IPs Part II.
- Regulation 7(1)(d) and Regulation 7(2)(a) of the PMLFTR, Section 4.5 and Section 4.8 of the IPs Part I and Section 3.2 and Section 3.3 of the IPs Part II.

In addition to the above, the Committee also issued a Reprimand in relation to the below breach:

- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs Part I and Section 3.2 of the IPs Part II.

The nature of the breaches identified should have also resulted in the imposition of remedial actions in terms of Regulation 21(4)(c) of the PMLFTR. However, the Committee took into account that the Company has ceased to carry out relevant activity and has demonstrated that it has no intention to restart activities. Had the Company not taken this decision, a process to follow up on the measures necessary to ensure compliance with the local AML/CFT legislative provisions, both in relation to the failures for which the Company has been found in breach (as relayed above), as well as on the remedial actions that the Company would have initiated.

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:

- Section 3.3.1 of the IPs Part I lists the quantitative factors which subject persons should consider for the identification of the threats and vulnerabilities to which subject persons are exposed. These include, inter alia, the number of customers within each customer risk type, the volume of business, the number of customers from a given jurisdiction, the number of customers per each product and service. Consideration of quantitative elements is crucial to enable a true understanding of risk expose, that is focussed on the subject person's own business operations.

- Section 3.3.2 of the IPs requires all aspects of the BRA to be documented and evidenced, this including (a) the methodology adopted to conduct the assessment, (b) the reasons for considering a risk factor as presenting a low, medium or high risk and others.

- The lack of a documented methodology to determine the frequency/likelihood of its risk factors and the strength of the mitigating measures could lead to inconsistencies between the final risk ratings assigned and ultimately to an inadequate assessment of the ML/FT risks the Company may be exposed to and the mitigating measure to be applied. While being able to explain one's risk is indicative of sound knowledge of the risks the subject person is or could potentially be exposed to, documenting such understanding and having the right approach to determine the threats, vulnerability and impact is essential.

- Subject persons are to consider all the risk factors each individual customer may present. In the absence of an adequate CRA, the subject person may end up attributing risk ratings that do not truly reflect the customers' risks. One must keep in mind that it is only through the CRA that the correct level of CDD and the necessary degree of controls can be applied. Customer behaviour, income streams and circumstances do change by time and therefore the CRA can never be a one time assessment of the customer but it has to be updated from time to time. Moreover, the subject person must ensure that when updating the CRA, the new information is factored in without erasing any other details and information which were previously considered.

- The subject person is to clearly understand in a comprehensive manner the purpose and intended nature of the business relationship, and clearly document same. It is only once the Subject Person has a clear view of same that it can ensure whether the service being provided is in line with the customer profile and whether the same customer falls within its risk appetite.

- The use of statistical models for developing a customer business and risk profile, to develop behavioural models against which to eventually gauge a customer's activity is acceptable when the risk is not high. However, in selecting such approach subject persons have to ensure that they use official economic indicators or else own data collected over time. Whatever the approach it is important to keep documentary evidence of the same and ensure that in the case of official economic indicators these are obtained from reliable sources.

- Monitoring customer behaviour against the business profile established or against the available information is indispensable. If the activity does not match such information or is otherwise anomalous or out of the normal patters, subject persons have to enquire about the source that is funding such activity. Documentary evidence may be necessary depending on the circumstances of the case. The subject person has to be sure that the activity is being funded through legitimate means. If circumstances warrant, subject persons should take approaches to restrict the business operations until such time that the customer provides the required information/documentation. If this is not provided or is otherwise unsatisfactory, it is important to consider filing a report with the FIAU.

31 August 2023