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:

25 June 2024

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

Off-site Thematic Review carried out in 2020

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €49,802 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulations 5(5)(a)(ii) and 13 of the PMLFTR, Sections 3.5.2, 3.5.3 and 9.2 of the Implementing Procedures (IPs) Part I, and Sections 2.1.2, 2.1.3, 2.2.1, 2.2.2 and 3.3.2(ii) of the IPs Part II;
- Regulations 5(5)(a) and 7(1)(c) of the PMLFTR, Section 4.4.2 of the IPs Part I, and Sections 3.2(iii) and 3.3.2 of the IPs Part II; and
- Regulations 5(5)(a), 7(1)(d), 7(2)(a), and 11(9) of the PMLFTR, Section 4.5.2 of the IPs Part I, and Section 3.2(iv) of the IPs Part II.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

The Customer Risk Assessment (CRA) – Regulations 5(5)(a)(ii) and 13 of the PMLFTR, Sections 3.5.2, 3.5.3 and 9.2 of the IPs Part I, and Sections 2.1.2, 2.1.3, 2.2.1, 2.2.2 and 3.3.2(ii) of the IPs Part II.

Inadequate CRA Methodology:

It was noted that although a CRA methodology was in place and was documented, the same was not rigorous and comprehensive enough to enable the Company to understand the risks posed by customers and to effectively apply the risk-based approach. The measures applied did not include the identification and the assessment of all risks in relation to every business relationship that the Company entered into. Hence, although the Company had a risk assessment procedure in place, the risk rating process implemented was not widely effective to depict a correct risk image of the customer and to thus ensure the necessary controls are taken, this since:

- The ML/FT exposure emanating from interface risk was not recorded as part of the Company's CRA. While it is true that the same channel of delivery is used, the consideration of the risks posed by such delivery method is still to be considered this to ensure that any control measures necessary are indeed identified and implemented;

- The CRA did not cater for the risks potentially arising from the jurisdiction(s) in which the funds processed through the business relationship are actually generated. Therefore, the Company's approach to assessing the ML/FT exposure from geographical risk did not sufficiently account for the range of potential factors by which a given business relationship may link the Company to jurisdictions unrelated to a customer's residence.

- The Company limitedly considered the type and frequency of transactions, and type of payment method, thus meaning that insufficient considerations were made in relation to the product/service and transaction risk. Regard should be given to whether the product or service allows high-value transactions to take place. In relation to transaction risk, the risks associated with a player depositing €5,000 during the course of the business relationship would invariably differ than those posed by a player depositing €100,000.

- In terms of customer risk, the CRA only considered PEP and sanctions screening results. Risk factors, such as the customer's economic activity, reputation, and behaviour were not taken into account.

Moreover, it was observed that apart from the risk rating assigned, none of the files reviewed contained a documented CRA outlining the rational leading to the assigned risk score. Indeed, the Company's AML/CFT policies and procedures on the CRA process were silent on the obligation for the CRA rationale to be properly documented.

Failure to revise the CRA in a timely manner:

In addition to the deficiencies noted in relation to the CRA methodology, the Company was found to have failed to revise the customer's risk assessment in a timely manner to adequately reflect the ML/TF risk borne by the customers. Examples of which are being illustrated hereunder:

- In one file reviewed it was noted that in approximately three months, the customer deposited €161,483 and withdrew €9,610, which resulted in a net loss of €151,873. During those three months, the customer's CRA remained unchanged and marked as low. It was only during the Examination when the Company updated the customer's risk rating into high to reflect the high volume of depositing activity.

- In another file, the customer was noticeably active in two months, during which he deposited approximately €50,123 through multiple payment methods without carrying out any withdrawals, resulting in losses of the same amount. Thus, when considering the large amounts deposited and lost in such a short period of time, the use of multiple payment methods, as well as the fact that the Company did not have any SoW/SoF information about this customer (this including information on the employment) to justify high volume depositing activity, a low-risk rating was deemed to be inadequate.

Establishing the Customer's Business and Risk Profile - Regulations 5(5)(a) and 7(1)(c) of the PMLFTR, Section 4.4.2 of the IPs Part I, and Sections 3.2(iii) and 3.3.2 of the IPs Part II

The Company's policies and procedures were silent on the requirement to collect SoW information for customers who have been risk rated as medium risk. Moreover, and on this note, despite the policies and procedures requiring SoW information and/or documentation for players rated as high risk, the same was not obtained, for instance, in one file the customer was classified as high-risk, however the Company did not request any information or documentation on the customer's occupation or SoW.

Also, the Company's policies and procedures were found to be silent on the requirement to collect information on the anticipated level of activity within 30 days from reaching the €2,000 deposit threshold. This was corroborated both during the kick-off meeting, as well as from the customer files reviewed as the Company did not collate or collect any information on the anticipated level of activity for any of the customer profiles reviewed. While information pertaining to the customer's income and employment should be considered distinct from expected activity, if the subject person had collected such information on income and employment (including from statistical models when the customer is not high risk), this information would have been considered as a sufficient proxy of the level of expected activity of their customers. However, this was also not collected.

Ongoing Monitoring - Scrutiny of Transactions - Regulations 5(5)(a), 7(1)(d), 7(2)(a), and 11(9) of the PMLFTR, Section 4.5.2 of the IPs Part I, and Section 3.2(iv) of the IPs Part II

The first shortcoming observed in this regard pertained to the inadequacies to the Company's documented policies and procedures. Such document failed to outline the procedures and measures to be applied when carrying out scrutiny of transactions based on the level of customer risk. Also, no detail was provided on detecting unusual transactions, nor actions to be taken in cases where an unusual transaction was detected.

The Company also failed to conduct effective and adequate scrutiny of transactions for 10 customers reviewed. A few examples are being illustrated hereunder:

- In 20 months, one customer deposited €448,583 through multiple payment methods and withdrew €275,690, resulting in a net loss of €172,892. During the first 10 months, the accumulated losses amounted to €3,121, however, from then onwards, the customer started placing significant amounts of deposits and incurring large losses. Some of the noticeable spikes were of €23,955, €24,950, €83,180, €57,000, €78,230 and €82,000 respectively. However, the Company failed to detect and enquire about the significant departure in the customer's transaction profile in a timely manner.

- In three months, the customer deposited €161,483 and withdrew €9,610, which resulted in a net loss of €151,873. Moreover, during such period, a number of spikes in daily deposits were observed, for which no SoF was requested. These daily spikes included daily deposits of €8,999, €9,998, €9,000, €7,000 or €14,000 respectively. However, the Company failed to detect and enquire about the significant departure in the customer's transaction profile in a timely manner.

- Account opened in June 2019 and during the business relationship which lasted 7 months, the customer deposited €124,723 and effected no withdrawals which meant a Net Loss of the same amount. However, the Company failed to detect and enquire about the significant departure in the customer's transaction profile in a timely manner.

Whilst noting that the Company did not obtain sufficient level and detail of information on its customers' profile, even on the basis of the limited information obtained, the Company should have been able to identify the instances where Company should have reached out to the customers to obtain the necessary information and/or documentation and in absence of same, where necessary, to apply restrictive measures on the account of the customer.

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 forty-nine thousand, eight hundred and two Euro (€49,802) with regards to the breaches identified in relation to:

- Regulations 5(5)(a)(ii) and 13 of the PMLFTR, Sections 3.5.2, 3.5.3 and 9.2 of the Implementing Procedures (IPs) Part I, and Sections 2.1.2, 2.1.3, 2.2.1, 2.2.2 and 3.3.2(ii) of the IPs Part II;
- Regulations 5(5)(a) and 7(1)(c) of the PMLFTR, Section 4.4.2 of the IPs Part I, and Sections 3.2(iii) and 3.3.2 of the IPs Part II;
- Regulations 5(5)(a), 7(1)(d), 7(2)(a), and 11(9) of the PMLFTR, Section 4.5.2 of the IPs Part I, and Section 3.2(iv) of the IPs Part II; and

When deciding on the administrative measures to impose and on the amount of any administrative penalty, the Committee must ascertain that these are effective, dissuasive, and proportionate to the seriousness of the failures identified. In doing so, the Committee took into consideration the importance of the obligations breached, the level of seriousness of the findings identified, and the extent of ML risk such failures could lead to.

The Committee also considered the Subject Person's size and the impact such failures may have had on both its operations and on the local jurisdiction. The level of cooperation portrayed by the Company and its officials throughout the supervisory process were also factored in.

Under normal circumstances, a Follow-Up Directive would be imposed for the breaches identified in terms of Regulation 21(4)(c) of the PMLFTR, however the Committee took into consideration that the Company has since the compliance examination surrendered its licence. Had the Company not surrendered its licence, 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 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 Take aways:

- The CRA is one of the pillars of a sound AML/CFT compliance program where all the risk criteria are exhaustively considered, and an understanding of risk is obtained. The rationale which led the customer to be rated in a particular manner is to be reflected in the CRA and in turn it is to be ensured that appropriate mitigating measures/controls are applied to minimize the specific increased ML/FT risk identified. Documenting this process is important to confirm the considerations taken to arrive at the final risk score.

- Given that risk is dynamic, it is important that the CRA be reviewed from time to time, depending on the risk presented by the particular business relationship, and especially where there is an event marking a material departure from the business and risk profile of the customer.

- The collection of expected activity is mainly driven by the need to have a benchmark by which to compare transactional activity. This is particularly useful given that in the gaming sector there are instances where source of wealth information is not necessarily a requirement (when the customer is low risk).

  Expected activity (frequency and value of transactions) tends to be collected directly from the customer. While information pertaining to the customer's income and employment should be considered distinct from expected activity, if the subject person had collected such information on income and employment (including from statistical models when the customer is not high risk), this information is being considered as a sufficient proxy of the level of expected activity of their customers.

- The fact that a customer is assigned a low-risk rating does not exonerate the subject person from conducting ongoing monitoring. Changing patterns throughout the lifetime of the relationship may lead to the need to obtain more information on the customer's employment as well as the SoW and SoF. Such changes may also trigger a potential requirement to revise the customers' risk rating.

- Transaction monitoring is essential to ascertain that the player's activity is in line with the available information on the player, otherwise additional checks are required to ensure that the funds originate from a legitimate source.

25 June 2024