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.

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 OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

12 December 2023

SUBJECT PERSON:

Trannel International Limited

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

Off-site compliance examination carried out in October 2020

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of €222,736, a Follow-Up Directive and a Reprimand

LEGAL PROVISIONS BREACHED:

- Regulation 5(5)(a) of the PMLFTR, Sections 3.5.1 and 3.5.2 of the IPs – Part I, and Section 2.2.2 of the IPs – Part II
- Regulation 13 of the PMLFTR and Sections 9.2 and 9.5 of the IPs – Part I
- Regulations 7(1)(c), 11(1) and 11(2) 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 7(1)(d), 7(2)(a) and 11(9) of the PMLFTR and Sections 4.5.1(a), 4.8 and 4.9.2.3 of the IPs – Part I

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

<u>Customer Risk Assessment (CRA) – Breach of Regulation 5(5)(a) of the PMLFTR, Sections 3.5.1 and 3.5.2 of the IPs – Part I, and Section 2.2.2 of the IPs – Part II</u>

Lack of Documented CRA

Although the Company did have a CRA methodology in place, several shortcomings were identified in relation to such methodology, as outlined in the following sub-section. In terms of the CRA process, it was noted that a significant portion of the customers who reached the €2,000 deposit threshold, as included in the Company's active client list, were without a risk rating. Therefore, there was a lack of evidence that the majority of the Company's customers had been duly risk assessed and assigned an appropriate risk rating during the course of the business relationship.

In its deliberations, the Committee reminded that the obligation for subject persons to carry out a CRA has been in force since the inception of the IPs in 2011, which is well before gaming licensees started being considered as subject persons in terms of Regulation 2 of the PMLFTR. Consequently, once gaming licensees became subject persons on 1 January 2018, they were required to prioritise the requirement of undertaking a risk assessment on their customers. The Company's failure to conduct a documented CRA for the majority of its customer base not only constituted a breach of its obligations, but also hampered its ability to determine the proper level of CDD to be applied, as well as the degree and extent of ongoing monitoring to be performed.

Notwithstanding the above, the Committee positively acknowledged the fact that following the compliance examination, the Company proactively remediated this deficiency by ensuring that all its customers were adequately risk assessed. Moreover, the Committee commended the fact that the Company implemented an automated risk assessment model that becomes operational upon account registration. Through this model, customers are risk assessed even before exceeding the €2,000 deposit threshold, with their risk ratings continuously updated based on gaming activity and other relevant factors. It is important to note that the Company took these remedial actions from its own initiative, before being instructed by the Committee to do so.

Inadequate CRA Methodology

During the compliance examination, the CRA methodology employed by the Company was found to be ineffective and inadequate, as explained below:

- At the time of the compliance examination, the Company did not have a system in place to link multiple accounts held by the same customer, thereby impeding a holistic assessment of the customer's activity across all accounts. Moreover, each individual customer account underwent a risk assessment in isolation, independently from any other accounts associated with the same customer. To substantiate this sub-finding, the compliance examination report referred to a number of player profiles that formed part of the examination sample where the customer was active in more than one account, yet the Company failed to identify and incorporate the connections between accounts within the risk assessment. Despite the concerns noted, the Committee recognised the fact that following the compliance examination, the Company introduced a new system which allows for the linkage of different accounts belonging to the same customer. Furthermore, alerts are now generated at the customer level rather than at the individual account level.

- The risk assessment algorithm was significantly focused on the transaction risk pillar, assigning a disproportionately lower weighting to the two other risk pillars that the Company took into

consideration as part of its CRA process, namely the customer and geographical risk pillars. Compounding matters further, the individual risk items considered in relation to customer and geographical risk were limited, merely consisting of the customer's age and country of registration respectively. This is clearly not sufficient, and for both risk pillars, the CRA methodology should have taken into account a wider range of factors and consideration. Furthermore, while cognisant of the fact that the Company's business is carried out exclusively on a non-face-to-face basis, and that as a result, all customers are onboarded in this manner, the Company was still expected to incorporate the interface/delivery channels risk pillar in its CRA. Doing so would have ensured that the potentially heightened risks associated with non-face-to-face interactions with customers and the presence of any third party deposits are duly accounted for.

- For 40% of the player profiles reviewed, the risk ratings assigned following a manual review conducted by the Company's AML team were deemed inappropriate in light of certain risk factors identified, such as significant deposit amounts, velocity of transactions and the use of higher risk payment methods. Additionally, in the case of certain player profiles, there was a discrepancy between the indicated risk ratings and other player specific information uncovered during the compliance examination. Notably, this included customers awarded a 'higher' risk rating[1], who should have received a different risk categorisation to better capture the risks inherent in the business relationship.

While not diminishing the significance of the shortcomings observed in the Company's CRA methodology, the Committee recognised the fact that at the time when the Company's representations were submitted in 2022, the Company was in the process of developing a new CRA framework with the objective of introducing an enhanced risk system that allocates the appropriate weighting to individual risk items and mitigating actions. The Company also indicated that efforts were underway to refine the CRA methodology, with the ultimate aim of assigning all customers a risk rating reflective of their perceived ML/FT risks.

Record Keeping Procedures – Breach of Regulation 13 of the PMLFTR and Sections 9.2 and 9.5 of the IPs – Part I

The Committee was informed of various instances where the Company fell short of fully complying with its record keeping obligations. Specifically, for 70% of the player profiles reviewed, the Company failed to retain a copy of the open source intelligence obtained from the internet, opting only to include the webpage links and a brief note describing the contents of the same. This practice increases the risk of losing valuable information should the webpage links change, or should the information be altered or removed in the future. In relation to one of the player profiles reviewed, the Company also neglected to maintain all the necessary transactional information, including the account identifying number(s) used to affect bank deposits. Lastly, it was observed that the Company was unable to extract and provide the essential data related to the players' risk ratings in a timely and efficient manner.

In spite of the above, the Committee positively noted at the time of its representations, the Company was storing all relevant KYC documentation, including SOW/SOF documents, in the JIRA system, thereby ascertaining that soft copies of documents are retained and linked to the relevant account/customer. There are also restrictions in place so that access to sensitive information pertaining to a player's income is limited

[1] A higher risk rating is assigned to those customers identified by the Company's system as requiring manual review by the Company's AML team. Subsequently, based on this review, the customer would be classified as low, medium or high risk accordingly.

to authorised personnel only. Moreover, in addressing the issue concerning the absence of copies of the open source intelligence gathered, the Company outlined that it was actively exploring solutions to save webpage links and other relevant documents in its internal system, and as an interim measure, a copy of the webpage links in PDF format was being retained.

Purpose and Intended Nature of the Business Relationship, Enhanced Due Diligence (EDD) and Ongoing Monitoring: Scrutiny of Transactions – Breach of Regulations 7(1)(c), 7(1)(d), 7(2)(a), 11(1), 11(2) and 11(9) of the PMLFTR, Sections 4.4.2, 4.5.1(a), 4.8 and 4.9.2.3 of the IPs – Part I, and Sections 3.2(iii) and 3.3.2 of the IPs – Part II

The compliance examination report also raised concerns regarding the Company's non-compliance with its obligations related to: (a.) the collection of information pertaining to the purpose and intended nature of the business relationship, particularly regarding the player's income, SOW and SOF; (b.) the application of EDD measures; and (c.) ongoing monitoring, specifically the scrutiny of transactions. The findings identified in relation to each of the aforementioned three distinct obligations are summarised below:

- Purpose and intended nature of the business relationship – Failure to obtain sufficient information related to the player's SOW and SOF for 50% of the player profiles reviewed.
- EDD – Failure to apply EDD measures for 30% of the player profiles reviewed and failure to implement adequate EDD measures for another 30% of the player profiles reviewed.
- Transaction monitoring – Failure to appropriately scrutinise transactions for 80% of the player profiles reviewed.

Some examples illustrating the deficiencies relayed above on a player profile-by-player profile basis are presented hereunder:

- Player profile 1 (high risk) – Over a period of less than three months, this player made deposits of approximately €300,000 and incurred losses amounting to over €200,000. Although a review was carried out on the player by the AML team, this was only after deposits had already surpassed €70,000. As part of the review process, open source intelligence checks were conducted, revealing that the player had a number of companies registered in his name, one of which had been through a bankruptcy procedure. However, there was a lack of details regarding the extent to which the player benefitted from such ownership, including potential sources of funding for his gaming activity such as salary earnings, dividend distributions and other similar disbursements. A spike in deposit activity was also noted, with the player depositing €8,000 in the first month of activity, followed by a significant increase in deposits to €120,000 in the second month. The combination of the substantial deposit amounts, short timeframe for the voluminous activity, and large deposit spike collectively represented high risk indicators that should have prompted the collection of SOW/SOF information and/or supporting documentation, the application of EDD measures, and the scrutiny of the transactions involved. The fact that one of the companies owned by the player underwent a bankruptcy procedure should have raised a further red flag.

- Player profile 2 (high risk) – In under one and half years, this player made deposits of €3.5 million and reached a net deposit figure of more than €750,000, utilising at least 12 different payment methods. Additionally, it was observed the player's deposits and withdrawals primarily followed a non-closed loop pattern, lacking a clear link between the payment methods used for deposits and withdrawals respectively. In a SOW questionnaire completed one month after registration, the player declared that he is a merchant for goods/services and has a salary of circa €20,000

per month. While a third party due diligence report regarding the player indicated that he owned three companies, the Company failed to gather information/documentation concerning the financial performance of these businesses. Adding to this, even though the player provided a tax return indicating that his total income and assets exceeded €3 million, most of the listed assets were relatively non-liquid, predominately comprising of securities. In the case of this player profile, despite there being evidence that the player had a certain level of accumulated wealth, the reality was that the player's activity was still inconsistent with the income available at his disposal. Thus, in view of the high risk factors detailed above, which include the high value and volume of deposits, relatively short timeframe for the activity, utilisation of multiple deposit methods, and non-closed loop transactions, the Company was expected to apply adequate EDD measures and scrutinise the player's transactions.

- Player profile 3 (higher risk) – Over a period spanning less than three months, this player made deposits of over €350,000 and incurred losses equal to approximately €150,000. Residing in Vietnam, the player claimed that he works as a manager, earning around $20,000 per month. However, the Company did not obtain any additional information/documentation to substantiate the player's source of income and ensure it was sufficient to sustain the player's gameplay. This oversight is especially critical when taking into account the low average salary in the player's country of residence, which contrasts with his declared monthly salary. Exacerbating matters further, there were instances where the player received funds from potential third party e-wallets, significantly elevating the risk associated with the business relationship. Hence, given the large deposits made, rapid velocity of transactions, and presence of third party deposits, the Company should have collected information and/or supporting documentation related to the player's SOW/SOF, applied EDD measures, and scrutinised the player's transactions.

The Committee acknowledged the fact that following the completion of the compliance examination, the Company started to proactively remediate some of the shortcomings detailed above. Particularly commendable was the comprehensive overhaul of the Company's AML/CFT Procedures Manual, with substantial revisions aimed at introducing more detailed requirements for key obligations such as the CRA and EDD. Moreover, the Committee noted at the time when the Company's representations were submitted, the Company was in the process of implementing a set of financial triggers designed to ensure that players exhibiting high levels of activity shortly after registration are flagged, leading to the collection of additional information and/or documentation, if necessary.

In relation to the specific player profiles for which breaches were identified in relation to these three obligations, the Committee observed that in most instances, the Company took remedial action by retrospectively re-assessing the players' profiles and closing the implicated accounts. For certain player profiles where unusual or suspicious transactions/activities were detected, the Company sometimes went a step further by filing an STR with the FIAU.

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

After taking into consideration the above-mentioned findings, the Committee decided to impose an administrative penalty of €222,736 for the breaches identified in relation to:

- Regulation 5(5)(a) of the PMLFTR, Sections 3.5.1 and 3.5.2 of the IPs – Part I, and Section 2.2.2 of the IPs – Part II
- Regulation 13 of the PMLFTR and Sections 9.2 and 9.5 of the IPs – Part I

- Regulations 7(1)(c), 11(1) and 11(2) 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 7(1)(d), 7(2)(a) and 11(9) of the PMLFTR and Sections 4.5.1(a), 4.8 and 4.9.2.3 of the IPs – Part I

It is essential to highlight that the breaches related to the purpose and intended nature of the business and EDD represent a failure to implement appropriate measures for player profiles displaying high risk elements and characteristics. For this reason, the Committee determined that a combined administrative penalty covering both these breaches should be imposed. However, a separate administrative penalty was deemed necessary for the specific breach concerning transaction monitoring. This is because when considering the player profiles in question, the Company was required to scrutinise the transactions involved given their high value and rapid velocity.

In arriving at the final amount of the administrative penalty to impose, the Committee took into consideration the importance of the AML/CFT obligations that the Company has breached, together with the seriousness of the findings identified and their material impact, as extensively explained above. The Committee also considered the fact that the Company was providing services to customers without adequate safeguards in place, which could have led to the unintentional facilitation of ML/FT. Moreover, the Committee took into account the nature, size and operations of the Company, including the voluminous gaming activity it was facilitating, as well as the risks associated with its exposure to third party payments. Furthermore, the Committee contemplated how the services provided by the Company and the AML/CFT controls it had in place or lacked may have impacted the local jurisdiction as a whole. The level of cooperation exhibited by the Company throughout the entire process, along with the overall regard that the Company has towards its obligations, were other factors taken into consideration by the Committee. Additionally, the Committee took note of the Company's commitment towards updating and enhancing its AML/CFT processes, as well as the remedial actions that the Company stated to have initiated or implemented. Further recognition was given to the proactive approach taken by the Company to initiate remediation on its own accord, displaying an appreciation of the risks it faced in the absence of sufficient AML/CFT controls. Lastly, the Committee ensured that the administrative penalty imposed is effective, dissuasive and proportionate to the failures identified and the ML/FT risks that were perceived during the compliance examination.

In addition to the imposition of an administrative penalty, the Committee issued a Reprimand to the Company for the breaches identified vis-à-vis Regulation 13 of the PMLFTR and Sections 9.2 and 9.5 of the IPs – Part I, as well as served the Company with a Follow-Up Directive in terms of its powers under Regulation 21(4)(c) of the PMLFTR. The purpose of this Directive is for the FIAU to ensure that the Company enhances its AML/CFT safeguards and performs all the necessary remedial actions to attain compliance with its AML/CFT obligations emanating from the PMLFTR and the IPs issued thereunder. In virtue of this Directive, the Company is expected to make available an Action Plan containing an overall status play of the current remediation measures being implemented by the Company, which shall include:

- The latest CRA methodology and any other related documents to ensure that the shortcomings identified in relation to such methodology have been duly rectified.
- Evidence that all existing customers who reached the €2,000 deposit threshold underwent a thorough risk assessment and were assigned an appropriate risk rating.
- Updates on any remedial actions already undertaken or planned by the Company to ensure that its record keeping procedures are not only well-documented, but also consistently followed in practice.

- Updates or further enhancements made to the procedures associated with the collection of information and supporting documentation related to the purpose and intended nature of the business relationship, primarily focusing on the customer's income, SOW and SOF.
- Updates or further enhancements made to the procedures associated with the application of EDD measures in high risk scenarios.
- Updates or further enhancements made to the procedures associated with ongoing monitoring, particularly in terms of the scrutiny of transactions.

As part of the Follow-Up Directive, the FIAU shall ascertain that tangible progress is achieved in the implementation of measures aimed at effectively addressing the failures identified. This shall not only include a review of policies and procedures, but also meetings and interviews with key officials actively involved in the remediation efforts. Moreover, the follow-up action may encompass system walkthroughs and a review of a sample of customer files. In the event that the requested information and/or supporting documentation is not made available within the stipulated timeframes, the Company's default will be communicated to the Committee for its eventual actions, including the possibility of the imposition of an administrative penalty in terms of the FIAU's powers under Regulation 21(1) of the PMLFTR.

The administrative penalty hereby imposed is not yet final and may be appealed before the Court of Appeal (Inferior Jurisdiction) within the period 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

- In the context of the remote gaming sector, the transaction risk pillar plays a crucial role in determining the overall ML/FT risk posed by each individual customer; however, relying solely on this risk pillar does not allow subject persons to establish a complete customer profile. Indeed, a holistic assessment of the other risk pillars ensures a more accurate customer risk rating, resulting in a lower risk rating if risks are mitigated or a higher risk rating if risks are aggravated. This will render subject persons better or worse off in terms of the level of CDD and ongoing monitoring measures to be applied.

- The prevalence of third party deposits poses a significant ML/FT risk because it involves the use of funds potentially derived from illicit sources that are disguised as gaming transactions. In such cases, subject persons often face challenges in corroborating the actual source that funded the customer's activity. Moreover, these deposits increase the risk of fraud as the individual making the deposit may not have legal authority to utilise the funds.

- In line with Section 9.1 of the IPs – Part I, subject persons are required to retain records of any business relationship they enter into and of any transaction they carry out, including all transaction that take place within the context of a business relationship. In addition to various other aspects, it is crucial for subject persons to maintain records on: (a.) information pertaining to the CRAs carried out; (b.) information obtained on the purpose and intended nature of the business relationship; (c.) information collected to establish the customer's business and risk profile; and (d.) any supporting evidence and records necessary to reconstruct all transactions carried out or facilitated by the subject person.

- Maintaining efficient record keeping procedures enables subject persons to retrieve and/or grant access to information in a timely manner when so requested by the authorities in accordance with the applicable laws. Of particular importance, subject persons need to ascertain that all relevant data

pertaining to their customers is adequately maintained and is easily accessible, including the risk ratings assigned, facilitating the swift extraction of customer lists on demand.

- In the context of the remote gaming industry, from an AML/CFT perspective, to comply with the requirement to obtain information, and if necessary, supporting documentation, on the anticipated level and nature that is to be undertaken throughout the business relationship, it is sufficient for subject persons to collect information regarding the player's expected income over a specified period of time (typically monthly or annually). This is because based on such information, subject persons will then be able to infer the player's anticipated level of activity and confirm that such activity does not go beyond what was known and evidenced about the player's income or wealth. The established expected level of activity would then be monitored in comparison with the player's gaming activity, ascertaining that any discrepancies are captured.

- Gathering information regarding the activities from which the customer derives his/her wealth and the expected source and origin of the funds to be used throughout the business relationship is indispensable for formulating a comprehensive business and risk profile that is reflective of the ML/FT risks posed by the customer in question. On a risk sensitive basis, it may be necessary for subject persons to verify the information obtained with supporting documentation. While information derived from open source intelligence checks may prove useful in establishing the customer's profile, it is imperative that subject persons ascertain the veracity and reliability of this information. In some cases, open source intelligence may need to be substantiated through the collection of additional information and/or documentation from the customers, especially if there is a lack of details regarding the sources funding the customer's activity.

- Situations that, by their nature, represent a higher risk of ML/FT, and consequently, when assessed individually or collectively, may warrant the application of EDD measures, include substantial gaming activity and deposits amounts, rapid velocity of transactions, the use of multiple and higher risk deposit methods, any third party deposits, and the presence of PEPs.

- As part of their ongoing monitoring obligations, subject persons are obligated to scrutinise the transactions executed by their customers. Particular emphasis should be placed on cases involving large values and/or volumes of transactions within a relatively short period of time, transactions deemed unusual or suspicious, as well as transactions deviating from the known and expected behaviour of the customer. When scrutinising transactions, is it critical for subject persons to ensure that documentation provided by the customer offers clarity about the funding used to affect transactions. In particular, subject persons must exercise caution when a customer indicates that his/her SOW/SOF is partly or even fully composed of non-liquid assets, unless there is evidence that these have been disposed of. Third party deposits also represent a significant risk that needs to be effectively managed. Since gaming activity is not typically funded by third parties, subject persons need to investigate the links and rationale behind such instances. Furthermore, it is paramount that subject persons remain vigilant and ascertain that this does not become the norm, suggesting that a player may, in reality, be a front for others.

12 December 2023