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:

Casumo Services 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 €66,476, a Reprimand and a Follow-up Directive in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 5(1) and 5(6) of the PMLFTR, Section 3.2.2, 3.3.1, 3.3.2 and 8.1 of the Implementing Procedures (IPs) Part I and Section 2.2.1 of the IPs Part II.
- Regulation 5(5), Section 3.5 of the IPs Part I and Sections 2.1 and 3.3.2 of the IPs Part II.
- Regulation 5(5) of the PMLFTR, Section 3.4 of the IPs Part I and Section 3.2 of the IPs Part II.
- Regulation 7(1)(a) of the PMLFTR, Section 4.3.1 of the IPs Part I and Section 3.2 of the IPs Part II.
- Regulations 7(1) and 9 of the PMLFTR and Section 4.4.2 of the IPs Part I and Sections 3.2 and 3.3.2 of the IPs Part II.
- Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5.1 of the IPs Part I and Section 3.2 of the IPs Part II.
- Regulation 11 of the PMLFTR and Section 4.9 of the IPs Part I and Sections 3.2 and 3.3.2 of the IPs Part II.
- Regulations 5(5)(a) and 11 of the PMLFTR and Section 3.4 of the IPs Part II.
- Sections 7.5, 9.2 and 9.3 of the IPs Part I.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment (BRA) – Regulation 5(1) and 5(6) of the PMLFTR, Section 3.2.2, 3.3.1, 3.3.2 and 8.1 of the Implementing Procedures (IPs) Part I and Section 2.2.1 of the IPs Part II.

The examination identified some systemic shortcomings pertaining to the BRA methodology adopted by the Company at the time of the compliance examination, since it failed to:

- Adequately include quantitative elements in the assessment of the Company's threats and vulnerabilities. The Company was determining the frequency scoring on the number/volume of transactions processed within a particular risk category. While such consideration is indeed good, this, on its own, is not sufficient. In this regard, reference is to be made to Section 3.3.1 of the IPs Part I which list 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.

- Provide documented explanations into what considerations were taken to arrive at the assigned ratings, and only asserted that this was based on discussions between key employees. In this regard, reference is to be made to 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.

- Detail the ML/FT risks associated with the various jurisdictions with which the Company conducts business with or is willing to do so given that the Company merely provided a list of jurisdictions indicating solely those which were considered as high-risk jurisdictions. No reference to the sources used to assess the jurisdictions was incorporated within such list, not even with respect to those indicated as posing a high risk. Important factors to be considered include the reputability of the country as well as other factors such as countries that are known to suffer from a significant level of corruption, countries with high risks of drug trafficking or other prevalent crime risks, countries with political instability, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organisations operating within are to be considered as high risk.

- Provide the overall resulting inherent and residual risk ratings. Hence, the outcome of the BRA was unclear.

Finally, the Committee positively acknowledged the Company's commitment to revise its BRA in line with the FIAU's recommendations made at the time of the examination. Indeed, the Committee acknowledged the Company's proactive approach to revise its subsequent BRAs which were provided to the FIAU following the examination through the annual REQ submission.

Customer Risk Assessment (CRA) - Regulation 5(5), Section 3.5 of the IPs Part I and Sections 2.1 and 3.3.2 of the IPs Part II.

While acknowledging that the CRA tool adopted by the Company is comprehensive and does consider all four risk pillars in line with section 3.5 of the IPs, through the compliance examination, the Committee identified the need for additional enhancements. This since while slot games and the use of credit cards/bank accounts belonging to a player himself pose a low risk, such considerations should still feature as part of the Company's CRA methodology.

Another shortcoming noted was that over 35% of the player accounts reviewed were rated as posing a low-risk rating at registration however such rating was not re-assessed upon hitting the €2,000 deposit threshold. Further concerning is that some of these customers portrayed higher elements of ML/FT upon hitting such threshold, however a revision of the CRA was not undertaken. Yet, it was positive to note that the majority of these customers hit the €2,000 deposit threshold within a relatively short period of time following their registration with the Company.

Policies & Procedures - Regulation 5(5) of the PMLFTR, Section 3.4 of the IPs Part I and Section 3.2 of the IPs Part II

The Company's policies and procedures as at the time of the compliance examination has specific elements which were deemed to be missing, incomplete or inaccurate, this since:

- Said policies and procedures did not include the requirement to obtain the players' birth of place, nationality and identity reference number (where applicable) as information that needs to be gathered as part of the standard identification and verification process. In this regard, not only was the documented procedure inadequate but the Company was also found in practise to having failed to collect such information from some of its players.

- The Company's record keeping policy merely stated that the players' information should be kept for a minimum period as set in each jurisdiction but failed to clearly outline all of the documentation/records that must be kept. However, in this regard, no shortcomings in relation to the Company's record keeping obligations were identified in practice, hence the severity of the breach was considered as minimal.

Identification & Verification - Regulation of the 7(1)(a) of the PMLFTR and Section 4.3.1 of the IPs Part I and Section 3.2 of the IPs Part II

The Company acknowledged that it had failed to obtain information on the nationality and place of birth with respect to three high risk players and one medium risk player. However, the FIAU acknowledged that the number of instances where the Company had failed to adhere to its identification and verification obligations is low and surely not indicative of a systemic issue. Therefore, from the examination, the Committee could conclude that the Company does have good measures in pace for identifying and verifying customers.

Timing of Due Diligence Procedures - Regulations 7(1) and 9 of the PMLFTR and Section 4.4.2 of the IPs Part I and Section 3.2 and Section 3.3.2 of the IPs Part II

With respect to two medium-risk rated players, the Company did not obtain information on the purpose and intended nature of the business relationship within 30 days of reaching the €2,000 deposit threshold. In addition, no proof was provided that the Company had carried out any open-source checks or made use of statistical data in this regard. In its representations, the Company asserted that such failure was due to an oversight, however, this could not be accepted as a sufficient justification.

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

It was positively acknowledged that the Company had obtained SoW information or employment information from 57% of the player profiles reviewed, this information was considered as sufficient to also account for the players' expected level of activity.

However, with respect to the remaining players (over 40%), the Company failed to obtain information of the players expected level nor on the players SoW or employment information. Further concerning was the fact that, although the majority of the players in question were low risk, one of these players had a medium-risk rating and another player had a high-risk rating. Whilst the IPs Part II delineate that with respect to players not rated as high risk, subject persons can use statistical models instead of obtaining the player's SoW or employment information, no documented evidence was provided by the Company that it was indeed using such statistical models.

Hence, this prevented the Company from building a comprehensive customer business and risk profile for a substantial amount of its players.

Transaction Monitoring - Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5.1 of the IPs Part I and Section 3.2 of the IPs Part II

During the examination, it was noted that the Company was not conducting sufficient transaction monitoring for AML/CFT Purposes. This since despite the changes in gaming patterns or other irregular activities taking place on 30% of the player profiles reviewed, the Company failed to conduct additional transaction scrutiny and/or carry out checks in a timely manner to ensure that the funds derived from legitimate sources. Examples of which are being illustrated hereunder:

- Within the first month of activity the player deposited over €7,000 all of which via prepaid cards and withdrew none. Following of which, the player was asked to provide SoW information and the player declared an income in the range of €1,000 and €1,500 working as "Other Office and Administrative Support Workers". Instead of questioning further how the player managed to deposit €7,000 while earning €1,500, the Company allowed the player, over a span of around five months, to deposit a total of €25,000 (and withdrew none) without taking any further action. After 5 months of activity (which also coincided with the time of the examination) in which the player deposited over €25,000, SoW documentation was requested, on the same day of the request the Company also suspended the player from further depositing. However, the Company should have acted and ascertained that the players SoW originated from legitimate sources sooner.

- Throughout the first month of registration, one player only deposited €800 and withdrew none. Subsequently, this player deposited over €9,000 and withdrew none. Following this, the player deposited an additional €22,000 over two days and withdrew none. This means that this player had deposited over €30.000 in four months.

  The Company only took action by requesting for SoW documentation following the second spike in deposits. Hence, the Company should have been proactive in its approach by requesting for SoW documentation upon the first spike of deposits in order to understand the legitimacy of the player's funds prior to letting the player making further deposits. Aggravating matters further was the fact that the Company did not even have on file employment information on this particular player.

- In 2019, another player had deposited over €15,000 in a month and withdrew none. The Company had only requested this player's SoW/SoF information/documentation during the compliance examination with the player's deposits being suspended on the same day as well. This however one year from the date the significant activity was carried out by the player. Aggravating matters further is the fact that the mentioned request was only made during the compliance examination suggesting that the request was triggered by the said examination. Moreover, the Company did not even have on file employment information on this particular player.

In deciding on the administrative measure to impose, the Committee considered that in a good number of instances, the Company did consider that there was a discrepancy between the known information and the players activity, and did indeed ask for SoW information. Yet, when this was not provided or inadequately substantiated, the Company did not take all the necessary actions to ensure such information is obtained or otherwise act upon the customer's relationship with the Company in a timely manner.

Enhanced Due Diligence (EDD) - Regulation 11 of the PMLFTR and Section 4.9 of the IPs Part I and Sections 3.2 and 3.3.2 of the IPs Part II

The compliance examination revealed that one player was assigned a low-risk rating, nonetheless, within four months, the player deposited over €90,000 out of which more than €20,000 were deposited via prepaid cards and more than €2,000 via an online wallet. The player declared a monthly salary ranging between €500 and €1,000 working as a software developer. Hence, the fact that the customer deposited a significant amount of money (€90k, of which €20k from prepaid cards) through different payment methods in just 4 months when his SoW declaration declared a monthly salary ranging between €500 and €1,000 working as a software developer should have triggered the Company to consider the high-risk elements present and carried out EDD on this player.

PEP Screening - Regulations 5(5)(a) and 11 of the PMLFTR and Section 3.4 of the IPs Part II

With respect to three players, the Company had failed to carry out screening, to determine whether these were PEPs, within 30 days of reaching the €2,000 deposit threshold. In fact, these players had their first PEP checks carried out months after the said threshold was reached. Moreover, in the case of four players, although the Company had conducted PEP screening prior to the player reaching the €2,000 deposit threshold, the Company failed to carry out another PEP check within 30 days of reaching the said threshold. In the latter circumstance it was however noted that there was a short period of time between the registration date and when the customer reached the €2,000 threshold. It was also positive to note that overall, the Company had good measures in place to check the PEP status of its players.

Vetting of Employees - Section 7.5, 9.2 and 9.3 of the IPs Part I

During the compliance examination, none of the employee files provided by the Company for review contained a copy of the police conduct certificate or equivalent documentation. The Company explained that despite not maintaining a copy, a police conduct was indeed collected, vetted and then handed back to each employee. Despite the shortcoming identified, it was positively acknowledged that since the examination the Company has remediated its position in this regard by updating its documented employee screening procedure to ensure that the required checks on its employees are undertaken and adequately retained.

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 findings identified, as well as the extent of ML/FT risk such failures could lead to. The Committee was particularly concerned with the Company's BRA 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 Company failed, for a significant number of player profiles, to obtain information on the employment information of customers which would enable it to infer what could be expected from the customer in terms of its level of activity and was found to have conducted inadequate scrutiny on a number of transactions despite the changes in gaming patterns or other irregular activities taking place.

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 commitment to remediate its failures, and its statements that it had already commenced working on some action points. 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 has not given due regard towards its AML/CFT obligations.

After taking into consideration the abovementioned, the Committee decided to impose an administrative penalty of €66,476 with regards to the breaches identified in relation to:

- Regulation 5(1) and 5(6) of the PMLFTR and Section 3.2.2, 3.3.1, 3.3.2 and 8.1 of the IPs Part I and Section 2.2.1 of the IPs Part II.
- Regulation 7(1) 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), Regulation 7(2)(a) of the PMLFTR and Section 4.5.1 of the IPs Part I and Section 3.2 of the IPs Part II
- Regulation 11 of the PMLFTR and Section 4.9 of the IPs Part I and Sections 3.2 and 3.32 of the IPs Part II

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

- Regulation of the 7(1)(a) of the PMLFTR and Section 4.3.1 of the IPs Part I and Section 3.2 of the IPs Part II.
- Regulations 7(1) and 9 of the PMLFTR and Section 4.4.2 of the IPs Part I and Section 3.2 and Section 3.3.2 of the IPs Part II.
- Regulations 5(5)(a) and 11 of the PMLFTR and Section 3.4 of the IPs Part II.

In terms of Regulation 21(4)(c) of the PMLFTR, the FIAU also served the subject person with a Follow-up Directive, to be able to assess the remedial actions being implemented by the subject person in view of the breaches identified. The aim of the Follow-up Directive is for the FIAU to ensure that the Company enhances its AML/CFT safeguards and that it becomes fully compliant with the obligations imposed in terms of the PMLFTR and the FIAU's IPs, as well as perform any required follow-up measures in relation to the Company's adherence to its AML/CFT legal obligations. This also in line with the Company's commitment to enhance its AML/CFT measures. In virtue of this Directive, the Company is expected to make available an Action Plan indicating the remedial actions that it has carried out and implemented since the compliance examination, together with remedial actions which are expected to be carried out to ensure compliance following the identified breaches, this including but not limited to:

- Updated CRA measures including methodologies that cater for a comprehensive understanding of risks and that allows for the assessment to incorporate all the information considered to risk assess customers.

- Updated Record Keeping Policies and Procedures which clearly outlines the documents and records to be kept by the Company.

- The procedure relating to the collection of information and/or documentation on the purpose and intended nature of the business relationship and the measures that the Company plans to implement in order to ensure that all necessary information is obtained. Particularly, the Company shall ensure that it has measures in place to effectively understand the player's level of activity.

- The procedure and measures adopted or planned to be adopted in relation to the scrutiny of transactions.

The Directive served on the Company shall ascertain that sufficient and tangible progress is achieved on the adoption and implementation of all the procedures and measures referred to above, that customer profiles are updated and kept up to date, that customer activity is adequately understood and that the Company enhances its AML/CFT safeguards.

Finally, the Company has also been duly informed that if it fails to provide the above-mentioned action plan and supporting documentation within the specified deadline, 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 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 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:

- 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.

- Section 8.1.2 of the IPs Part I provides insight into the considerations that have to be taken by subject persons to truly understanding the risks posed by exposure to certain jurisdictions. It is to be pointed out that the higher the exposure, the more detailed the said risk assessment is to be so as to allow a comprehensive understanding of the factors contributing to the overall risk thereof. 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.

- All aspects of the BRA should be covered, including the outcome of the BRA. Therefore, it is of utmost importance that every determination and assessment taken in identifying, assessing, managing and mitigating risks, as well as the monitoring of such processes and the overall resulting inherent and residual risk rating is duly recorded in writing.

- 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. 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 discovered previously.

- As per Section 4.3.1 of the IPs Part I and Section 3.2 of the IPs Part II, standard identification procedure consists in the gathering of the following personal details: (a) name and surname; (b) permanent residential address; (c) date of birth; (d) place of birth; (e) nationality; and (f) identity reference number where applicable.

- Within the context of the remote gaming sector, the key element as to why SoW is obtained is to have sufficient information available to allow the detection of unusual activity in the course of a business relationship. To this end, licensees have to collect sufficient information and, where it is necessary, documentation to establish a customer's source of wealth as well as the expected level of activity. As to the extent of the information that licensees are to collect, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment. Where the risk is not high, a declaration from the customer with some details (e.g. nature of employment/business, usual annual salary etc.) can suffice. Social media can also be used as a source of information. However, where the risk of ML/FT is higher or licensees have doubts as to the veracity of the information collected, the information obtained would need to be supplemented by means of independent and reliable information and documentation. In developing a customer business and risk profile, licensees may also consider using statistical data to develop behavioural models against which to eventually gauge a customer's activity rather than collect source of wealth information. Where a licensee opts to adopt this approach, it is crucial to point out that this must be well evidenced and the data utilised deriving from reputable sources. Further information can be found under Section 3.2(iii) of the IPs part II.

- Transaction monitoring is essential to ascertain that the player's activity is in line with the available information on the player or otherwise that information and documentation is obtained to verify the source of such activity. In such instances, the subject person may be required to understand further and evidence the players' source of wealth and source of funds. This would be substantiated through for example obtaining financial statements of companies they own evidencing any earnings they receive, payslips, employment contracts, and other reliable and independent documentation. The value of the gaming activity taking place, the type of games played, the payment method utilised and the geographical connections all play a crucial role in understanding any high risk exposure necessitating EDD measures to be carried out.

- Section 3.4 of the IPs Part II states that screening for PEP status has to be carried out regularly, but it is important that this is done within 30 days of the €2,000 threshold being met, even where licensees may have already screened customers to determine if they were PEPs earlier on in the course of the business relationship.

31 August 2023