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:

26 June 2023

SUBJECT PERSON:

Glitnor Services Limited

RELEVANT ACTIVITY CARRIED OUT:

Remote Gaming Operator

SUPERVISORY ACTION:

Compliance review carried out in 2019

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €236,789, 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, 3.2.4, 3.3.1, 3.3.2 and 8.1 of the Implementing Procedures (IPs) Part I and Section 2.2.2 of the IPs Part II.
- Regulation 5(5) and Regulation 5(5)(a)(ii) of the PMLFTR, Sections 2.1.2, 2.2.2 and 3.3.2 of the IPs Part II and Section 3.4.1 of the IPs Part I.
- Regulation 5(5)(a) of the PMLFTR and Section 3.4 of the IPs Part I.
- Regulation 9 PMLFTR and Sections 3.3.2 of the IPs Part II.
- Regulation 7(1) PMLFTR, Section 4.4.2 IPs Part I and Section 3.2(iii) IPs Part II.
- Regulation 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5 and 4.5.2.2 of the IPs Part I.
- Regulation 11(1) and 11(9) PMLFTR, Section 4.5.1(a) IPs Part I and Section 3.2 and 3.3.2 IPs Part II.
- Regulation 11(5) PMLFTR, Section 4.9.2.2 IPs Part I and Section 3.4 IPs Part II.
- Regulation 15(1)(a) PMLFTR and Sections 5.1.2(b) ad 5.1.3 of the IPs Part I.
- Regulation 5(5)(e) PMLFTR and Sections 7.3 and 7.4 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, 3.2.4, 3.3.1, 3.3.2 and 8.1 of the IPs Part I and Section 2.2.2 of the IPs Part II.

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 all the risks that the Company is exposed to in a comprehensive manner, including:
    - Conducting a thorough consideration of the risks emanating from the products offered rather than solely relying on generic risks emanating from 'Casino Games' and 'sports betting'.
    - Factoring the risks faced through placing reliance on other parties to obtain certain CDD obligations.
    - Incomplete assessment of the Company's jurisdictional risks given that only the 'reputability' of a particular jurisdiction was considered and this without referencing the source/s used to rate such jurisdictions. Hence, the Company should have considered 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.
- Include quantitative data in determining the likelihood of the risks materialising, such as the number of customers and the jurisdictions that the Company had dealings with.
- Provide an evaluation of the strength and effectiveness of the mitigating measures adopted with respect to each risk scenario identified.
- Provide the overall resulting inherent and residual risk ratings. Hence, the outcome of the BRA was therefore completely 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 and also in line with the requirements applicable at law.

Customer Risk Assessment (CRA) & Customer Acceptance Policy (CAP) - Regulation 5(5) and Regulation 5(5)(a)(ii) of the PMLFTR, Sections 2.1.2, 2.2.2 and 3.3.2 of the IPs Part II and Section 3.4.1 of the IPs Part I

The Company's CRA policy and procedures provided during the examination did not adequately consider the 4 risk pillars in line with the IPs, this since:

- In terms of interface/delivery risk, the Company's CRA procedures merely stated that it ensures that third party Customer Due Diligence (CDD) and verification procedures are equivalent to that expected by the MGA.
- Also, in terms of the geographical ML/FT risks, the Company was not considering the customer's residence and geographical elements in connection to the customer's source of wealth/funds.
- When assessing the ML/FT risks of the customer, no consideration was made to the risk posed by the customer's Source of Wealth (SoW) or economic profile, including elements such as whether the customer has a single source of regular income or multiple sources of income.
- When it comes to product and transaction risk, the Company's CRA procedures only referred to a limited number of risk factors in connection with payment methods and total deposits. Hence it failed to consider the risks in connection to the gaming product/service being provided to that specific customer.

The Committee positively acknowledged that since the compliance examination, the Company has adopted a new CRA scoring methodology which considered all the four risk pillars in line with the IPs, however it could still not disregard that at the time of the examination its procedures were significantly lacking.

Further concerning is that for all the files reviewed as part of the examination, officials were not provided with a CRA, this even though such players had all exceeded the €2,000 threshold. In its representations, the Company held that a CRA had been conducted however a risk-rating was not formally assigned and no additional action was taken as none of these players were identified as posing a high risk. The Company stated that such rationale shall be adequately documented going forward. Whilst acknowledging the Company's plan to remediate its shortcomings, the Committee could not ignore the fact that no evidence was provided by the Company to prove that a CRA was carried out in respect of all of the customers reviewed for the purposes of the compliance examination.

Finally, the Committee noted that the Company's CAP does not cover all the requirements set out in Section 3.4.1 of the IPs Part I, in that the Company's CAP does not:

- Provide any examples of customers that pose a higher risk than average to ML/FT.
- Provide risk indicators that can lead to a relationship being considered as low, medium or high.
- Indicate the level of CDD including ongoing monitoring which will be applied depending on the risk rating.

The above failures further corroborate issues identified above with respect to the Company's obligations to have CRA measures in place. In its representations, the Company held that a new CAP was adopted after the examination, however, following a review of the mentioned new CAP, the Committee concluded that the shortcomings outlined in the previous version of the CAP still subsist in the new version.

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

The Company's policies and procedures as at the time of the compliance examination were missing, incomplete or inaccurate, this since:

- Said policies and procedures did not mention and explain the requirement to develop a customer business and risk profile.
- Some sections of the procedures are inapplicable to the Company. E.g., one section of the Company's policies states that due diligence and probity checks need to be carried out on corporate customers, this despite that the Company does not offer its services to corporate customers and does not subcontract to any third parties.

Identification & Verification - Regulation 9 PMLFTR and Sections 3.3.2 of the IPs Part II

For three of the player files reviewed, the Company admitted that it had failed to obtain proof of identity and residential address documents within the 30-day legal timeframe. It added that this shortcoming shall not happen again since going forward an automatic alert shall trigger once the customer reaches total deposit or withdrawals of €2,000.

Although the number of cases where the Company's processes were not followed is low and surely not indicative of a systemic issue, the Committee could not ignore the fact that as at the time of the compliance examination the Company has failed to obtain proof of identity and residential address documents within the legal timeframes.

Purpose & Intended Nature - Regulation 7(1) PMLFTR, Section 4.4.2 IPs Part I and Section 3.2(iii) IPs Part II

During the examination, the Company's policies and procedures dealing with the requirements to collect information on the purpose and intended nature of the business relationship were deemed as not being in line with the obligations at law. This because the said policies and procedures did not require the Company to request SoW and Source of Funds (SoF) information and/or documentation and to create a business and risk profile upon a customer reaching the €2,000 deposit threshold.

In addition, the Committee noted that in its representations, the Company provided risk ratings of all the customers reviewed, this however without explaining how it arrived at such ratings. The Committee took these risk ratings into account only to account whether the company implemented the customer profiling measures depending on the risk ratings it provided. It stressed that its approach with regards to this is not to be viewed as an acceptance on the Committee's part that the Company had adequate CRA measures or that it even was in agreement with the said risk ratings, but as a means to understand whether the Company understood the level of CDD necessary in comparison to the identified level of risk.

To this effect, the Committee noted that notwithstanding, the Company itself had assigned a medium risk rating to eight (8) players. For such players, the Company neither obtained SoW/SoF information directly from them nor any statistical data as explained in the IPs Part II. This despite that as stated in the IPs Part II, although SoW information need not be obtained by subject persons with respect to low risk customers, it has to be obtained for medium and high-risk customers.

Also, during the examination it was identified that no information regarding the anticipated level of activity was obtained from the Company for any of the player files reviewed. Apart from this, the Committee noted that no sufficient information on the players' employment was obtained which information would have at least served as an indication of the players' expected level of gaming activity. The Company in its representations stated that information is sought on every player and a clear understanding is obtained of the expected level of play of each customer that is based on a combination of both statistical modelling and player information. The Committee positively acknowledged the Company's comments, noting this could be the right approach, however these were not supported with any evidence. Thus, the Committee could only but conclude that the finding found at the time of the examination subsists.

Transaction Monitoring - Regulation 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5 and 4.5.2.2 of the IPs Part I

During the examination, it was noted that the Company had in place a set of 'Alerts' to monitor transactions undertaken by its players, however, these were not deemed comprehensive enough to combat ML/FT. This particularly since, the alerts failed to cover divergences from the customer's usual depositing amounts/gaming patterns and risk profile. The Committee positively acknowledged that following the examination, the Company has implemented additional transaction monitoring thresholds to ensure the level of spending is in line with the risk profile of the customer.

However, the Committee cannot disregard the fact that during the examination the Company failed to conduct additional transaction scrutiny and checks to ensure that the funds derived from legitimate sources, this following changes in gaming patterns or other irregular activities noted for 7 players. Examples of which are being illustrated hereunder:

- After a month and a half from registering as a customer of the Company, one player deposited over €3,000 across 38 transactions ranging between €25 and €100 in 9 days. The highest deposits were made on 2 subsequent days with the player depositing €800 on each day. These 2 days should have served as a trigger for the Company to question such spike, especially when considering that the player was a relatively new customer and no information on his income was known to the Company. Despite this, the player's activity went unnoticed for another 6 months, until then the player had already deposited a total of €35,000 and withdrew a total of €25,000, thus losing approximately €10,000 in less than 8 months. Up until the day of the examination, no evidence was found indicating that ongoing monitoring checks were carried out on this player. Moreover, the Company was still short of, at least, understanding the income streams of this customer.

- During the first 2 months of registration the player deposited €1,972 and withdrew €1,420, the month after €3,837 were deposited and €3,395 withdrawn. The next 2 months, the player deposited €11,030 and withdrew €9,701 and the subsequent month, the player deposited a total amount of €7,362 and withdrew €5,249. Throughout the 13-month relationship, the player deposited a total of €61,942 and lost €12,040. The Committee noted that despite the number of frequent deposits and accumulated amount deposited, the Company failed to conduct any checks or enquiries about the player's SoW/SoF.

Enhanced Due Diligence (EDD) - Regulation 11(1) and 11(9) PMLFTR, Section 4.5.1(a) IPs Part I and Section 3.2 and 3.3.2 IPs Part II

The Company's AML/CFT Manual provided during the examination stated that the application of EDD is required in 'high risk cases', however, it did not explain which kind of situations or customers would qualify as 'high risk cases'.

While cognisant of the Company's failures in its CRA obligations, the activities undertaken by 10 players led the Committee to find the Company in having failed to carry out EDD measures in order to confirm that the players' funds derived from legitimate sources. This since, such players held elements of high-risk of ML/FT (including significant deposits/ losses and use of high-risk payment methods), for which the Company should have immediately applied enhanced due diligence. Examples of which are being illustrated hereunder:

- In less than 3 months, a 30-year-old player from a non-EU jurisdiction deposited a total of around €12,100 all via pre-paid cards and never withdrew any winnings. Notwithstanding the high volume of deposits made within a short time span and the use of high-risk payment methods, no EDD measures were conducted and no SoW/SoF information or documentation nor employment details were requested by the Company.

- Another player registered in July 2019 and deposited €8,450 in 2 days with the Company failing to carry out EDD to determine the legitimacy of such large transactions.

- In less than 2 months, a 43-year-old non-EU resident player, deposited a total of €18,867 via Prepaid cards and an e-wallet. The player throughout these 2 months withdrew a total of €8,944 which left him at a loss of €9,923. Notwithstanding that the player originated from a non-European country, was using a high-risk payment method and made such deposits and losses in a period of two months, no EDD measures were conducted and no SoW/SoF information or documentation nor employment details was requested by the Company.

- Across circa 3 months, another player deposited a total of €15,200 and only withdrew around €711. No EDD measures were conducted and no SoW/SoF information/documentation nor employment details was requested by the Company, despite the fact that the player originates from a non-European country and deposited and lost around €14,500 all made via high-risk payment methods including two distinct e-wallets.

PEP Screening - Regulation 11(5) PMLFTR, Section 4.9.2.2 IPs Part I and Section 3.4 IPs Part II

At the time of commencement of the compliance examination the Company had failed to conduct PEP screening on over 80% of its customers, all of which reached the €2,000 deposit threshold. Aggravating matters further is the fact that, although the Company stated that it had conducted the said PEP screening during the compliance examination (still failed to adhere to the 30-day timeframe stipulated by the IPs Part II), it eventually resulted that it still failed to perform PEP screening on 5 of such players. Finally, the Committee positively acknowledged the Company's statement that the remediation process undertaken shall ensure that all customers are screened upon reaching the applicable threshold. This shall be closely monitored by the Committee since understanding the extent of PEP exposure is also crucial to satisfy the EDD requirements when dealing with PEPs.

Internal Reporting - Regulation 15(1)(a) PMLFTR and Sections 5.1.2(b) ad 5.1.3 of the IPs Part I

During the examination, one player was noted to have lost €5,462 in less than five months and earns €300 monthly according to the payslip provided. Such player was found to having ignored 3 requests made by the Company and provided inadequate documentation for another 2 while finally replied with a document from another gaming provider suggesting that the player exceeded USD 500,000 worth of "Eligible transactions" within one year.

Despite providing additional explanations as part of the Company's representations, the Committee highlighted that the Company still held sufficient information to cast doubt on the veracity of the customer. This since, the customer provided insufficient information and, in some instances, ignored the Company's requests altogether. The customer had a VIP status with another gaming website and had more than €500,000 of eligible transactions as well as having significant balances on both his bank statements yet having a € 300 monthly salary as source of wealth. Although faced with these discrepancies between the player's incoming salary and the transactions being carried out by him, the Company failed to, for instance, to request for further information as to whether the player in question is a professional one which would have aided the Company to further understand from where the player was generating his funds.

In view of the above, it was determined that the Company should have flagged an internal report to the MLRO to understand whether there was any suspicion that the player's funds were being generated illicitly. However, in the taking of the administrative measure to impose the Committee considered that the Company did have some information/ documentation to confirm the VIP status of the customer with another company.

Training - Regulation 5(5)(e) PMLFTR and Sections 7.3 and 7.4 of the IPs Part I

At the time of the compliance examination, two main shortcomings were noted in relation to the Company's adherence to its training obligations:

- The Company's training material was too generic and not tailored specifically to the Maltese AML/CFT Regulations and the Company's Policies and Procedures. This since it was found that the training provided by the Company to its employees did not provide enough information by when an internal report should be escalated and the information to be included. Also, no reference to was made to its CAP or the CRA and did not refer to the risks that arise after compiling the BRA.

- Deficiencies when it comes to proper record keeping of the AML/CFT training being delivered to employees and a list of employees who would have undergone such training.

Finally, the Committee positively acknowledged the Company's statement that a refresher training course has been undertaken by all staff following the examination and that all new employees are now subjected to the induction AML Training.

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 issues when it comes to ascertaining that the gaming activity entertained by it was in line with the customers' funding abilities. Furthermore, the Company's inability, at times, to at least cross-check the players' gaming activity against basic information on the employment and the inability to manage heightened risks of certain customers serviced by it was also a cause of concern for the Committee. 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. 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 €236,789 with regards to the breaches identified in relation to:

- Regulation 5(1) and 5(6) of the PMLFTR, Section 3.2.2, 3.2.4, 3.3.1, 3.3.2 and 8.1 of the IPs Part I and Section 2.2.2 of the IPs Part II.
- Regulation 5(5) and Regulation 5(5)(a)(ii) of the PMLFTR, Sections 2.1.2, 2.2.2 and 3.3.2 of the IPs Part II and Section 3.4.1 of the IPs Part I
- Regulation 9 PMLFTR and Sections 3.3.2 of the IPs Part II
- Regulation 7(1) PMLFTR, Section 4.4.2 IPs Part I and Section 3.2(iii) IPs Part II
- Regulation 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5 and 4.5.2.2 of the IPs Part I
- Regulation 11(1) and 11(9) PMLFTR, Section 4.5.1(a) IPs Part I and Section 3.2 and 3.3.2 IPs Part II
- Regulation 11(5) PMLFTR, Section 4.9.2.2 IPs Part I and Section 3.4 IPs Part II

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

- Regulation 9 PMLFTR and Sections 3.3.2 of the IPs Part II
- Regulation 15(1)(a) PMLFTR and Sections 5.1.2(b) ad 5.1.3 of the IPs Part I

In terms of its powers under 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. 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 CAP and Policies and Procedures which reflect the procedures that are adopted in practice.

- 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 collected. The Company shall also ensure that it has measures in place to effectively understand the player's level of activity. The Company is also required to provide a plan for the updating of all its active customer relationships this to ensure that it has a comprehensive customer risk profile as well as to assess such risks.

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

- The procedure and measures relating to the carrying out of enhanced due diligence measures for higher risk situations.

- Updates on the training provided to all employees, irrespective of the level of seniority. The Company is to make available a training log highlighting the training attended and the respective employees' roles within the Company.

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 lase of the appeal period or upon final determination by the Court.

Key Takeaways:

- Risk understanding is the pillar for the comprehensive implementation of an effective AML/CFT regime. This is both at the business and customer level. Through an understanding of the business risks one would be able to identify the areas within its operations that are of highest risks and which necessitate the greater resources for the effective management of such risks. The customers serviced have to be well and completely understood, enabling an understanding of the risks each customer will present to the Company and the measures that are necessary to manage such risks. Ultimately, the customers being serviced expose the subject person to risks deriving from the product/service provided by it, the source that is funding the customer's activity and the jurisdictional exposure. Moreover, it is to be pointed out that the risks posed by the customers' jurisdiction exposure could have a bearing onto the extent of the risks posed by the customer, its activities and its source of funding. It cannot be stressed enough that the carrying out of a CRA is crucial since on the basis of the CRA, the proper level of CDD can then be applied which should be commensurate to the identified risks.

- 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. Although detailed SoW information need not be obtained by subject persons with respect to low risk customers, it has to be obtained for medium and as well as evidenced for high-risk customers (or any other ranges in between). When it comes to medium risk customers, this obligation to obtain SoW information can be exonerated if the subject person opts to consider using statistical data to develop behavioural models against which to eventually gauge a customer's activity. It is however 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.

- 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.

- One has to consider that even if at times the value of the deposits made is within the annual income (or the statistical representation of the same), there still has to be an assessment as to the degree and extent to which one is expected to deposit such considerable amounts. Thus, where the amounts deposited by a customer are of a relatively high value, even if these amounts may be in line with the customer's profile, the licensee is still obliged to carry out the necessary level of monitoring depending on the risks such customer presents. Ultimately, if players gamble all or the majority of their annual income, one has to factor in how they are also coping with daily expenses. This may therefore be, a good indicator that there are other sources funding such activity. It is therefore of heightened importance to obtain independent and reliable information and documentation on the source of wealth and source of funds used by the customer to fund the deposits.

26 June 2023