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:

11 July 2023

SUBJECT PERSON:

MT SecureTrade 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 €53,179 in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR).

LEGAL PROVISIONS BREACHED:

- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the Implementing Procedures (IPs) Part I and Section 3.2(iii) of the IPs Part II.
- Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5.1(a) of the IPs Part I.
- Regulation 5(5) of the PMLFTR and Section 3.5.1 of the IPs Part I and Sections 2.1.2, 2.2.1 and 3.3.2 of the IPs Part II.
- Regulation 11(1), 11(2), 11(9) of the PMLFTR and Section 4.9.2.3 of the IPs Part I and Section 3.3.2 of the IPs Part II.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Purpose and Intended Nature of the Business Relationship – Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the Implementing Procedures (IPs) Part I and Section 3.2(iii) of the IPs Part II

It was noted that the Company failed to obtain information in relation to the players' occupation, employment, or the activities from which the customer was deriving his wealth, as well as the anticipated

level of activity for 30% of the files reviewed. The Committee observed that the Company failed to provide any evidence that it had indeed obtained information on the purpose and intended nature of the business relationship for these three files. It also noted that although the Company seemed to have a mitigation measure in place as per the Company's representations and policies and procedures, wherein a player was not allowed to withdraw until the source of wealth questionnaire is submitted, this same measure is not always effective as it should be in practice. This since some players were still allowed to withdraw pending the submission of the questionnaire. As to the anticipated level of activity, whilst understanding and acknowledging the fact that it is harder to obtain the expected level of activity in a precise manner due to the possibility of recycled winnings, the Committee commented that the Company is still obliged to at least have some sort of indication or idea of the amount of money the respective players will be using to fund their gameplay.

Ongoing Monitoring – Scrutiny of Transactions – Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5.1(a) of the IPs Part I

Insufficient transaction monitoring was noted for 70% of the files reviewed and this despite changes in gaming patterns or other irregular activities. Examples highlighting the same are being relayed hereunder:

- This particular player was allocated a low-risk rating. He registered several accounts with different brands in the span of four years. His fifth account was flagged on the same day of its registration and this due to high deposits noted. The Company carried out an investigation and open source checks due to this, however, it still failed to collect information relating to the player's source of wealth and this despite the large deposits. The Company subsequently collected the source of wealth questionnaire, however it still failed to obtain any source of wealth and source of funds documentation. The player proceeded to deposit large sums of money. The Company eventually did ask the player to submit source of wealth documentation, however the payslip provided was deemed to be insufficient by the Company itself. The Committee considered the Company's representations wherein the Company held that it had also obtained the player's employment contract which confirmed that the salary was paid once every two weeks rather than monthly. However, the employment contract was not made available to the Committee. Thus, the Committee could not come to the decisive conclusion that the transactions carried out were actually in line with the player's income. It further held that although source of wealth documentation was indeed requested, this was requested seven and a half months late, with no indication as to the employment of the player. The Committee acknowledged that the Company carried out open-source checks, and whilst it did agree that such checks help subject persons understand and build up the player's profile, it also pointed out that these open-source checks alone are not and should not be deemed to be sufficient. More evidence is needed in order to ensure that the transactions being undertaken by the player are actually in line with his profile and income.

- Another player had multiple accounts with different brands. He registered his first account on 17 July 2014 and was allocated a high-risk rating. Upon registering his third account on 10 January 2019, the player deposited and lost EUR12,000 in the span of seven days. A deposit block was subsequently imposed on this account on 16 January 2019, and this until the player completed the source of wealth questionnaire. In the meantime, the player registered another account through which he deposited and lost EUR41,400 within approximately two weeks (between 28 February and 15 March 2019). This

account was subsequently blocked on 17 March 2019, however the player registered yet another account on 9 December 2019, through which he deposited and lost EUR8,000 in five hours. This last account was then put on hold the following day. The Company eventually obtained source of wealth and source of funds documentation a month later, on 16 January 2020. The Committee took note of the Company's representations which held that the majority of the player's deposits took place before 2018 and thus before the Company was even considered as a subject person. The Committee pointed out that this fact was indeed considered and that indeed, the transactions which were considered and reported were the ones which took place in 2019. Moreover, the Committee noted that the documentation obtained in 2020 related to activity carried out in 2019, thus meaning that same should and could have been obtained earlier. The Committee further observed that it is concerning that the Company was only blocking singular accounts rather than the player, as this lead to players continuously and repeatedly registering multiple accounts and depositing drastic amounts. This pattern should have raised concerns and the Company should have in turn either blocked the master account, so that the player would not be able to open any additional accounts, or else blocked the player from registering any other account with a different brand.

Customer Risk Assessment (CRA) – Regulation 5(5) of the PMLFTR and Section 3.5.1 of the IPs Part I and Sections 2.1.2, 2.2.1 and 3.3.2 of the IPs Part II

Late CRAs were noted for 70% of the files reviewed due to the adoption of a manual risk rating procedure. These CRAs were not carried out when the respective players reached the EUR2,000 deposit threshold within a 180-day rolling period. Whilst considering the Company's representations wherein the Company stated that prior to the implementation of the system it currently uses, it used to carry out its risk assessments manually, the Committee stressed that the CRA in itself is an assessment of the particular risks which it will be exposed to in providing its services to a specific customer. Hence, it is crucial for the CRA to be performed at the time of onboarding and the fact that the Company was carrying out its CRAs manually should not justify the Company's failure to perform CRA at onboarding.

Moreover, inadequate risk ratings were attributed to 40% of the files reviewed when taking into consideration the specific risk factors posed by the same. Furthermore, there was at least one of the 33 red flags indicators set out in the Company's own AML/CFT Manual present for each of these four players. In view of this, the players' risk ratings should have been amended to reflect same. An example of this is being relayed hereunder:

- This player was assigned a low-risk rating on the same day of registration. This risk rating was not revised even though the player had deposited EUR2,100 through a prepaid card within one month and even though he had deposited EUR28,742 and lost EUR11,242 in approximately two months and two weeks, an amount which was not in line with the player's income (i.e. that of EUR3,456 monthly). The Committee stressed on the risks which arise when using prepaid cards. It further held that the use of these cards as well as the discrepancy in the income of the player and the amount deposited merited a higher risk score, this especially since both these points were listed as red flags in the Company's own AML/CFT Policy.

Enhanced Due Diligence (EDD) – Regulation 11(1), 11(2), 11(9) of the PMLFTR and Section 4.9.2.3 of the IPs Part I and Section 3.3.2 of the IPs Part II

The Company failed to carry out EDD measures on 10% of the player files reviewed who had presented more than one high ML/FT risk element. Details are being relayed hereunder:

- This player deposited a total of EUR42,089 through prepaid cards in approximately eight months. In the same period of time, the player withdrew EUR12,250 to one of his prepaid cards and bank account. Moreover, the player lost EUR29,839. Despite this information, the Company failed to apply any EDD measures. The Committee commented on the use of several payment methods and the risks attributed to the same. Prepaid cards increase the element of risk since they can be bought using cash and since no checks are carried out on the party purchasing said cards. Moreover, the person purchasing the card and the person utilising it might not be the same. The payment methods used by this player confuse the financial trail and allow the player to operate with a certain level of anonymity. In view of this, the Committee therefore concluded that this should have increase the level of risk attributed to the player and adequate enhanced due diligence measures should have been applied.

Furthermore, insufficient EDD documentation was obtained in relation to 10% of the files reviewed. Details are being relayed hereunder:

- Large transactions were deposited by this player in the span of approximately 3 months and 3 weeks (between 23 August and 16 November 2019 and between 1 and 11 June 2020). In fact, a total of EUR100,800 were deposited in this time period, EUR42,773 of which were new money. Although the Company did eventually collect documentation relating to the player's source of wealth, this was not enough to justify the gaming activity. The Committee pointed out that since the payslip provided indicated that the player had a net salary of EUR2,739 per month, this should have only led the Company to raise more questions with the player and to obtain additional evidence to substantiate the origin of all the funds being deposited.

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 fifty three thousand one hundred seventy nine euro **(€53,179)** with regards to the breaches identified in relation to:

- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs Part I and Section 3.2(iii) of the IPs Part II for the failure to collect information on the nature of employment and anticipated level of activity.
- Regulations 7(1)(d) and 7(2)(a) of the PMLFTR and Section 4.5.1(a) of the IPs Part I for the failure to scrutinise transactions.
- Regulation 5(5) of the PMLFTR and Section 3.5.1 of the IPs Part I and Sections 2.1.2, 2.2.1 and 3.3.2 of the IPs Part II for the serious and systematic failure to carry out timely and adequate customer risk assessments.
- Regulations 11(1), 11(2) and 11(9) of the PMLFTR and Section 4.9.2.3 of the IPs Part I and Section 3.3.2 of the IPs Part II for the failure to apply EDD measures and to obtain sufficient documentation.

The Committee commented that had the Company remained in operation, apart from the administrative penalty indicated above, the Committee would have also served a Directive on the Company, directing it to carry out remedial actions in order to rectify the failures observed.

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 of the findings identified, and whether these are systematic or otherwise, as well as the extent of ML risk such failures could lead to. The Committee also considered the Subject Person's size and the impact that the Subject Person's failure 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.

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 subject person is to clearly understand in a comprehensive manner the purpose and intended nature of the business relationship of its customers, and clearly document same. It is only once the subject person establishes a comprehensive profile that it can ensure whether the activity undertaken by the customer is in line with the said profile. Understanding the customer's occupation as well as the source of wealth and source of funds to be utilised, is crucial to be able to assess the customer's expected level of activity and to subsequently monitor expected activity against actual activity.

- Subject persons are to carry out CRAs when a business relationship is to be entered into or an occasional transaction is to be performed so as to not to expose their business to an increased risk of ML/FT.

- The risk-based approach mainly depends on a thorough understanding of the ML/FT risks that one faces. The risk ratings allocated to the players are a result of the risks arising from the risk factors considered. If certain risk factors are omitted, the risk rating attributed will inevitably be flawed and will not reflect a true picture of the ML/FT risks which arise with the respective business relationship.

- Where the customer presents higher risk elements (Including large value and volume of gameplay especially when taking into consideration the age and profile of the customer, and the payment methods being used by the customer), subject persons are expected to perform EDD measures. This may be done by enquiring further and gathering additional information and documentation on the transactions effected by the player and the customer's source of funds and source of wealth.

11 July 2023