Administrative Measure Publication Notice

This Notice is being published by the Financial Intelligence Analysis Unit (FIAU) in terms of Article 13C of the Prevention of Money Laundering Act (PMLA) and in accordance with the policies and procedures on the publication of AML/CFT penalties and measures established by the Board of Governors of the FIAU.

This Notice provides select information from the FIAU's decision imposing the respective administrative measures and is not a reproduction of the actual decision.

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

29 September 2023

SUBJECT PERSON:

Alchemy Markets Limited (previously NSFX Limited)

RELEVANT ACTIVITY CARRIED OUT:

Investment Services

SUPERVISORY ACTION:

Compliance Review carried out in 2019

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

Administrative Penalty of €419,997 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) of the PMLFTR and Sections 3.3 and 8.1 of the Implementing Procedures (IPs)
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs
- Regulations 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.2.2, 4.3.1 and 4.3.1.2 of the IPs
- Regulations 5(5)(a)(i) and 11(1) of the PMLFTR
- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs
- Regulations 7(1)(d) and 7(2)(a)-7(2)(b) of the PMLFTR as well as Section 4.5.1(a)-(b) of the IPs
- Regulation 5(5)(a)(i) of the PMLFTR and Section 5.1.2(a) of the IPs

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment (BRA)- Regulation 5(1) of the PMLFTR and Sections 3.3 and 8.1 of the IPs

In reviewing the BRA, the Committee noted some systemic shortcomings pertaining to the methodology adopted by the Company at the time of the compliance examination, since it failed to:

- Adequately include qualitative elements in the assessment of its threats and vulnerabilities. By way of example, through outsourcing, the Company had to consider whether the entity it was outsourcing to had sufficient processes, controls and measures in place to meet legal requirements and whether there were potential ML/FT risks through such agreement. Yet, although reference to outsourcing was found in the BRA, there was no other evidence as to any assessment carried out by the Company.

- Include quantitative elements in the assessment of its threats and vulnerabilities. For instance, there was no indication of the volume of business, nor any information regarding the number of customers it has by risk category (e.g., low, medium, or high), or by customer type/customer activity (e.g. Pensioners, Unemployed, employment by sector etc.).

- Detail the jurisdictions with which the Company had established connections, and the risks these exposed it to. This given that the Company merely provided a list of jurisdictions indicating whether a country: (a) is/is not part of the European Economic Area; (b) listed on the European Union watch list or (c) is considered as not reputable jurisdiction and listed on FATF lists.

- Take into consideration the likelihood of the identified risks manifesting themselves and the impact of any such manifestation, which would have ultimately led to the determination of the level of risk the Company was exposed to.

- Detail as to how the CDD should vary depending on the risk observed. This since for all risk factors, the measures to be applied to address the risks are equally the same.

Moreover, prior to the compliance examination the Company was requested to provide the latest BRA following which it transpired that the BRA as detailed above was approved on 20 February 2019, i.e. more than a year following the introduction of this obligation.

Customer Risk Assessment (CRA) - Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs

1. CRA not carried out

During the compliance examination no evidence was found of the CRA carried out for 86% of files reviewed. Indeed, the Company explained that the CRA process was implemented in August 2018 since the requirement to carry out same was introduced with the 2018 PMLFTR. However, the Committee could not agree with this statement, reminding the Company that the obligation to carry out a CRA has been in place since 2008, by virtue of the PMLFTR, and that more detail as to the implementation of such risk assessments were explained in the FIAU's IPs which were first issued in 2011. The recording of the CRA in writing, has also been in place since August 2011.

2. CRA process did not consider the minimum risk indicators

It was noted that the CRA methodology adopted post August 2018 was not rigorous and comprehensive enough to enable the Company to understand the risks posed by customers and to effectively apply the risk-based approach. Hence the measures being applied did not include the identification and the assessment of all risks in relation to every business relationship that the Company entered into:

- It is still important to take into consideration those jurisdictions with which the customer has relevant personal links. While the mere fact that a customer was born in a high-risk jurisdiction should not itself mean that the business relationship is exposed to a heightened risk of ML/FT, the Company should assess whether there are any further links between that jurisdiction and the business relationship.

- Although channels through which a subject person establishes a business relationship and through which transactions are carried out may also have a bearing on the risk profile of a business relationship or a transaction, it became evident that the interface factor was not recorded by the Company.

- No considerations were made in relation to the product/service risk. To this effect, while comprehending that the product is one (i.e. a trading product), the Committee stressed that the details of the product offered by the Company such as the different investment opportunities vary and need to be factored in as a risk consideration.

Hence, although the Company had a risk assessment procedure in place, the risk rating process implemented was not widely effective to depict a correct risk image of the customer and to thus ensure the necessary control are taken.

Identification and Verification - Regulations 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.2.2, 4.3.1 and 4.3.1.2 of the IPs

The compliance examination revealed shortcomings by the Company in terms of its obligations which require the identification and verification of natural persons as required in 5 customer files:

- In one (1) file, only a front side copy of the identity card was found on file and therefore the verification of details concerning nationality, place of birth, and issue date were missing.

- The identification document for one (1) customer failed to indicate the nationality and place of birth, as well as the document expiry date. The Committee whilst acknowledging that the document issued by the Election Commission of India had no expiry date, stressed that the Company should have obtained additional documents to verify the place of birth and nationality.

- The bank statements obtained to verify the residential address for an additional three (3) customer files was limited to name, city, post code and a PO Box number. The Committee while appreciating the circumstances of certain countries, remarked that when resorting to exceptional means of verification, subject persons must appropriately document the reasons for reverting to these exceptional means of verification and the reasons for considering the documents and information used as reasonably reassuring to verify the customer's identity.

While these have been considered as breaches of the Company's legal obligations, the Committee considered that these are not serious and systemic failures and that indeed the majority of the files reviewed were found to be in compliance with the obligation to identify and verify the customer.

Enhanced Dur Diligence (EDD) - Regulations 5(5)(a)(i) and 11(1) of the PMLFTR

1. Lack of application of EDD measures on customers connected to high-risk jurisdictions

Although the Company had information in relation to the geographical connections of its customers, it nonetheless did not consider such information for the purpose of applying adequate mitigating measures to address the risk exposures. For instance, while customers had links with Syria, Iraq, Libya or Tunisia, no information was obtained by the Company in order to understand whether any part of their wealth was generated in these jurisdictions. Indeed, one (1) file the individual was born in Iraq and resided in South Africa however, from the bank statements held on file outward transactions with references such as mum and sister were noted. Likewise, an additional file involved a Syrian national living in the Netherlands yet in the account opening form declared that his source of wealth was from inheritance. This should have led the Company to enquiry further about the links to such jurisdictions and apply the necessary EDD measures

Concerns by the Committee in this regard were held in view of the fact that Syria was (and still is) included in the FATF lists of Jurisdictions under Increased Monitoring. Similarly, Libya, Tunisia and Iraq were featuring on the European Commission list of high risk third countries, (Syria remained listed to date), and thus are automatically considered as non-reputable jurisdictions. Therefore, the high-risk elements were evident and thus, the Company should have carried out EDD.

2. Lack of application of internal policies and procedures in relation to EDD

The Committee reviewed the AML Procedures Manual which was applicable to those customers that were on-boarded after August 2018. However, it was noted that the measures outlined do not adequately mitigate the ML/FT risks posed by a high-risk business relationship. This since most of the measures focused on obtaining verification documents or validating the customer's residential address, thereby failing to identify and address the risks emanating from each set of circumstances. While the aforementioned measures are good, these only address specific risks linked to a customer's identity or place of residence. No consideration was thus given to the need to gather more information and evidence to establish the profile of the customers in particular on matters related to their activities. Moreover, despite the fact that in line with its own policies and procedures, the Company should have applied EDD on those customers who reached a pre-determined score ,the Committee observed that this was in contradiction to what was happening in practice.

Purpose and Intended Nature of the Business Relationship - Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs

The compliance review revealed that the Company had failed on a number of occasions to adhere to its obligation to obtain sufficient information to establish the purpose and intended nature of the business relationships it maintained with its customers and to establish a comprehensive customer profile. As part of its deliberations, the Committee made the following considerations:

1. Information in relation to source and origin of funds, expected value of transactions and overall wealth of the customer

From the review of a sample of business relationships reviewed, it transpired that information obtained in relation to the purpose and intended nature of the business relationship was not sufficient. This is so because the Company did not obtain sufficient information in relation to:

(a) Source of Wealth of the customer

The customers' wealth was obtained through the fields concerning 'Source of Wealth', 'Nature of Employment' and 'Net Annual Income'. While it cannot be discounted that one's SoW will also be one's expected SoF, and that this could be exclusively derived from one's income through employment or business activities this cannot be taken for granted. A subject person should understand the source that generated one's wealth as well as understand which of such sources are expected to fund the activities through the established relationship. Therefore, as a minimum the Company must always establish the customer's SOW and then ask if the funds that are to be used throughout the relationship are to be generated by the same business/activity/employment or if the source is different/specific. In the latter case, the subject person would then have to obtain information, and if necessary, documentation on the expected SOF, in addition to that obtained for understanding the SOW.

(b) expected value and frequency of transactions (except for the initial deposit)

The Company establishes the expected value and frequency of transactions from the fields 'Approximate Amount of Investment', 'Source of Wealth', 'Net Annual Income' and 'Expected Monthly Trades'. The Committee, whilst acknowledging that this is good information suggested the inclusion of questions linked to investment prospects. This information will not only assist in building an appropriate customer business and risk profile, but it will also enable the Company to carry out meaningful monitoring of the customer's activity through the course of the business relationship.

(c) the expected source and origin of funds to be used during the course of the business relationship

Even though the products and services offered might appear to be simple, one must also consider the value and size of the product, service or transaction. The Company has to always bear in mind that the use of the product/ service offered will differ between customers and this in turn has a bearing on the risk the customer presents as well as the measures the Company implements to safeguard its operations. Hence the importance of obtaining information such as the source of wealth (SoW) and expected source of funds (SoF) that enable a thorough understanding of the business relationship entered into, and the expected level of its use.

2. Employment / Business Activity:

The file review also revealed that in 29% of the files reviewed, the information in relation to employment was found to be too generic (limited to an employment post held) as detailed below:

- In some files, the occupation field was marked ''employed'' without any information in relation to the said employment.

- In an additional file the on-boarding form indicated that this customer is employed as a leading specialist, without giving any information in relation to the area of expertise of this customer.

- Similarly, another customer indicated to be a self-employed engineer, however his industry was not indicated.

- For one (1) legal customer, it was indicated that the company provides general services, with the nature of services not being identified.

- Likewise where the customer indicated that he is self-employed company owner and where it was indicated that this customer is employed in general services sector there was no indication of the type of services offered by the business in which they are involved.

Transaction Monitoring - Regulations 7(1)(d) and 7(2)(a)-7(2)(b) of the PMLFTR as well as Section 4.5.1(a)-(b) of the IPs

1. No Evidence of transactional reviews carried out by the MLRO

The Committee noted that the Company's monitoring included a review of customer's transactions on the trading system in order to identify any unusual activity. Furthermore, it was indicated that the MLRO conducts ad-hoc checks on the client profiles. Nevertheless, no records were shown confirming the latter and no evidence of any transactional reviews carried out were made available by the Company either. In this respect, the Company was required to retain records of any information that is necessary to understand the customer, the business relationship entered into, and the activity being carried out. Indeed, the Company acknowledged that in hindsight it would have been in its own interest to do so. However, in the absence of any evidence to corroborate the Company's statement, the Committee could not consider that any form of transaction scrutiny was indeed being carried out.

Consideration was also given to Company's submission that irrespective of issues of timing and maintenance of records, the Company is confident that there are no issues of ML/FT with any of the clients mentioned. This since payments were received from Banks in reputable jurisdictions. However, this is not a sufficient justification due to the fact that as a subject person the Company required to conduct due diligence measures independently of those carried out by the Bank. Moreover, from a review of the files sampled, the Committee observed deposits being affected through Neteller as well as Skrill, which are not Banks, and which may increase the risk of anonymity.

2. Lack of scrutiny of transactions falling outside the customer's profile

The scrutiny of transactions consists in using the Company's knowledge of the customer to identify any transactions that are unusual, in other words, transactions that are inconsistent with the customer's profile or are significantly different to what is usually carried out or requested by the customer. On such occasions the Company should have reached out to the customers to obtain the necessary information and/or documentation. Yet, it was noted that the Company did not conduct sufficient transaction scrutiny in 36% of the customer files reviewed. Examples of which are being illustrated hereunder:

- In one (1) file, despite the account opening form indicating that the customer is a self-employed trader with a yearly income of €50,000-€100,000, deposits of approximately $1.7 million were effected between 2015 and 2018. Still, no clarifications were sought by the Company, nor any documentary evidence obtained to substantiate such transfers and such a deviation from account expectancy. Additionally, despite the Company making available a copy of two bank statements, none of these provided any clarity as to how this customer afforded such large deposits. This since the account activity consisted primarily of debit transactions with no specific transactions being traced to investment income. Moreover, even if the bank statements could have been considered as adequate for the deposits made in 2015, the same cannot be said for the exponential increase in deposits made in 2017 when compared to the previous years.

- In an additional file, a lump deposit of $149,946 was made in July 2017 as well as additional seven deposits made in three consecutive days in December 2017 amounting to $95,000. This despite the customer stating to have an annual income between €50,000-€100,000. The Committee considered that even if as stated by the Company, a self-employed engineer can earn far more, the Company had to obtain evidence on the employment income of the customer, or otherwise on the return on certain projects the customer was working on to ascertain that he could sustain the investments being made or otherwise whether other sources were funding such activity.

- In another file, the Committee was informed that as per account opening form, the customer was a self-employed kitchen equipment supplier with a yearly income between €25,000-€50,000. However, over a 20-day period the deposits affected by this customer amounted to $77,800. The Company therefore relied on generic statements provided by the customer as to source of funding and albeit having a trigger which should have required it to obtain more information/documentation to ensure that the source of funds as described by the customer could have funded such transactions, it failed to act on such trigger and allowed the activity to proceed.

In addition to the file specific observations, of concern was also the Company's statement that in particular instances, the discrepancy between the net annual income and the transactions carried out is due to customers under declaring their wealth. While this may be such, divergences between the transactions undertaken and the available information should be queried and verified and not taking such assumptions. Apart from this, such under-estimation could also be indicative of tax evasion, which is a ML predicate offence that should have been further analysed by the Company.

3. Lack of application of internal policies in relation to customer's activity monitoring

Although the Company stated that additional screening is carried out upon deposits of €50,000 and documentation confirming SoF is obtained from those who reach €100,000 deposit threshold, no evidence of this was noted. To this effect it was clarified that at on-boarding the Company collects the declaration of source of funds from the client as well as proof that the first deposit came from a bank account or is linked to a credit card. Moreover, when a client deposits (a) More than 25k further online checks are conducted (b) More than 50k an analysis is carried out to establish if there are any anomalies in the account movements and (c) More than 100k, an immediate block on any withdrawals is imposed, whilst requesting a bank statement or other form of proof showing the source of funds. However, as extensively relayed above, it is clear that such measures were not being implemented in practice.

4. Lack of measures in place to maintain customer's profiles valid and up to date

While no expired documents were found, from the findings relayed above, in particular the sections covering the obligation to obtain information in relation to source and origin of funds, expected value of transactions and overall wealth of the customer as well as to conduct on-going monitoring obligations, it became evident that the Company did not have measures in place to ensure that the information on its customers is complete and up to date. Accentuating this is that transactions being carried out were far from being in line with the little information available on the customers. Yet, this still didn't act as a trigger to obtain information and documentation form the customers with a view to both understand the customer's profile as well as the legitimacy of the transactions being undertaken.

The Money Laundering Reporting Officer (MLRO) - Regulation 5(5)(a)(i) of the PMLFTR and Section 5.1.2(a) of the IPs

The Company did not ensure that the MLRO it appointed had sufficient knowledge, expertise and time for such an onerous position. Indeed the MLRO was not dedicating sufficient time to meet his obligations at law due to multiple appointments held and due to lack of knowledge of the AML/CFT obligations. What is more worrying is that a number of cases which necessarily merited further action by the MLRO were identified during the review, but nonetheless no action was taken by the MLRO. The Committee deemed relevant to point out that, when an employee is acting as the MLRO for two or more subject persons, it has to be ensured that these multiple appointments still allow the MLRO to fulfil his/her functions in an effective manner. Time commitment is key to ensure as much. While there is no set number of appointments that one may accept as MLRO, the more appointments one holds and the more complex or voluminous the activities of the subject person concerned, the more difficult it will inevitably become for the MLRO to meet his obligations at law in a satisfactory manner.

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, particularly that the Company not only lacked a comprehensive understanding of the risks it was exposed to but was making little to no use of the information about its customers to monitor and scrutinise the activity taking place. 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 also in light of the transactions that were being processed were also considered.

The Committee was overly concerned about the Company's effective actions in enhancing its AML/CFT measures through time, and particularly when it had on earlier occasions already been made aware by the FIAU of the need to address ineffective measures it was applying to safeguard its operations. The Committee also considered the Company's size and the impact that the subject person's failures may have had on both its operations and on the local jurisdiction. The level of cooperation portrayed by the Company throughout the supervisory process was also factored in, including the Company's statement that it is committed to remediate its failures.

In view of this, the Committee decided to impose an administrative penalty of four hundred nineteen thousand, nine hundred and ninety-seven Euro (€419,997) in relation to the following breaches:

- Regulation 5(1) of the PMLFTR and Sections 3.3 and 8.1 of the Implementing Procedures (IPs)
- Regulation 5(5)(a)(ii) of the PMLFTR and Section 3.5 of the IPs
- Regulations 7(1)(a) and 7(1)(b) of the PMLFTR and Sections 4.2.2, 4.3.1 and 4.3.1.2 of the IPs
- Regulations 5(5)(a)(i) and 11(1) of the PMLFTR
- Regulation 7(1)(c) of the PMLFTR and Section 4.4.2 of the IPs
- Regulations 7(1)(d) and 7(2)(a)-7(2)(b) of the PMLFTR as well as Section 4.5.1(a)-(b) of the IPs
- Regulation 5(5)(a)(i) of the PMLFTR and Section 5.1.2(a) of the IPs

The Committee ascertained that these are proportionate to the circumstances and risks presented through the established relationship as well as effective in ensuring that the Company increases its level of regard to ML/FT risks. In particular those to ensure that risks are well and thoroughly understood both at the business and customer levels, the necessary level of due diligence is carried out at all times, customer relationships and transactions are adequately monitored and evidenced as necessary.

Moreover, in terms of Regulation 21(4)(c) of the PMLFTR, the FIAU 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:

- An updated BRA clearly outlining how the Company has tackled the shortcomings identified by the Committee. This shall also include the provisions implemented by the Company to assess jurisdiction risks, including the criteria considered to risk assess the same.

- 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 EDD procedures to ensure that: (1) the necessary information is obtained to mitigate the heightened ML/FT risks identified and (2) the inclusion of the documentation necessary to be obtained in such circumstances;

- The procedure relating to the collection of information and/or documentation on the purpose and intended nature of the business relationship and the measures the Company plans to implement in order to ensure that all necessary information is collected.

- The procedure and measures adopted or planned to be adopted in relation to the scrutiny of transactions. The Company is required to enhance the measures it has in place to monitor the customer activities to be able to determine instances where the activity is not in line with the

information available on the customer or otherwise where there are material deviations from the patterns of usual trading activity.

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. Such action plan shall be closely monitored by the FIAU to ensure the Company achieves tangible progress in the implementation of effective AML/CFT safeguards. This may also include the interviewing of Company officials to ensure that there is sound knowledge of the AML/CFT legal obligations as well as knowledge of the Company's own measures to manage and control ML/FT risks. A sampling of customer files may also be necessary.

The administrative penalty hereby imposed is not yet final and may be appealed before the Court of Appeal (Inferior Jurisdiction) within the period as prescribed by the applicable law. It shall become final upon the lapse of the appeal period or upon final determination by the Court.

Key Take aways:

- Subject persons need to assess the risks that they are exposed to because of the business relationships they engage in. This needs to be done by assessing the inherent risk which depends on the identification of the existent threats and vulnerabilities as specified by Regulation 5(1) of the PMLFTR.

- The geographical risk assessment is not merely about having a rating but rather it is about understanding where the risk derives from in order for the subject person to be able to mitigate the same. Therefore, it is not enough to provide a list without understanding and be able to explain and evidence the rationale behind it

- The CRA is one of the pillars of a sound AML/CFT compliance program, as well as a measure which is necessary both to determine the level of due diligence required to build comprehensive customer profiles, as well as to ascertain the degree of on-going monitoring necessary. Therefore, the CRA is one where all the risk criteria are exhaustively considered, and an understanding of risk is obtained. Documenting this process is at all more important both to confirm when the assessment was done, as well as the considerations taken to arrive at the final risk score
- Where the customer presents higher risk elements (including links with non-reputable jurisdictions), 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 customer and the customer's source of funds and source of wealth.

- Understanding the purpose and intended nature of a business relationship is an essential AML/CFT obligation which enables a subject person to perform effective transaction scrutiny. Without an adequate business and risk profile, subject persons are unable to identify deviations from normal behaviour or patterns and may result in subject persons failing to file a SAR or STR where required to do so.

- Subject persons are to have effective transaction monitoring procedures in place. It is only through the monitoring of customer transactions or activities that subject persons can (a) identify that the customers' behaviour/transactions are not in line with their profile, (b) identify suspicious and anomalous transactions or activity, and (c) determine whether the initial risk assessment requires updating.

- Subject Persons appointing MLROs who either hold multiple positions within the same entity or else multiple MLRO appointments, have to ensure that these multiple appointments still allow the MLRO to fulfil his/her functions in an effective manner. Time commitment is key to ensure as much.

29 September 2023