Administrative Measure Publication Notice

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

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

DATE OF IMPOSITION OF THE ADMINISTRATIVE MEASURE:

31 January 2023

RELEVANT ACTIVITY CARRIED OUT:

Virtual Financial Asset Service Provider (VASP)

SUBJECT PERSON:

Bequant Exchange Limited

SUPERVISORY ACTION:

Compliance review carried out in 2021

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of Euro 220,992 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 3.3.1 and 3.3.3 of the Implementing Procedures (IPs);
- Regulation 5(5)(a)(ii) of the PMLFTR, Sections 3.5.1, 3.5.1(a), 3.5.2 and 3.5.3 of the IPs Part I, and Section 2.1 of the Implementing Procedures, Part II, VFA Sector (IPs Part II);
- Section 2.2.1 of the IPs Part II;
- Regulation 7(1)(c) of the PMLFTR, Section 4.4.2 of the IPs Part I and Section 2.2.3 of the IPs Part II;
- Sections 4.3.1.1(i) and 4.3.1.2(i) of the IPs Part I;
- Regulation 11(1)(b) of the PMLFTR and Sections 4.9 of the IPs Part I;
- Regulation 7(2)(a) of the PMLFTR, Sections 4.5.1(a) and 4.5.2.3 of the IPs Part I and Section 2.2.5 of the IPs Part II.

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

<u>Business Risk Assessment – Regulation 5(1) of the PMLFTR and Sections 3.3.1 and 3.3.3 of the IPs</u>

The Committee considered the following shortcomings noted during the examination –

The BRA lacked sufficient consideration to risks to which the Company was or could potentially be exposed to. By way of example, the risks of VPN and proxy servers, as well as the risks pertaining to mixers or tumblers, are risks that although being synonymous to the VFAs' business, these have not been included in the assessment of the Company's business risks. This meant that even when the BRA was eventually adopted, this was still substantially inadequate. It was further noted that the methodology in the BRA was incorrect, failing to include the analysis of

risk scenarios, the likelihood of any risk materialising and the possible impact that such risks would have on the Company. The Company's residual risk rating was inadequate both because of the failure to assess material risks as above-mentioned but also because the residual risk rating in the BRA referred to an unrelated financial institution. It was also overall observed that apart from the serious inadequacies as abovementioned, The Company's BRA had been drafted late and at the time of the examination, had not been approved by the Board of Directors.

In its deliberations, the Committee considered that the Company had drafted its BRA late. Additionally, the BRA provided at the time of the examination was inadequate in that it lacked a proper assessment of pertinent risks the Company is exposed to. The CMC noted that the possibility of the usage of VPNs and proxy servers was something that companies offering services relating to VFAs could be easily exposed to. The same can be said for risks pertaining to mixers or tumblers, which are synonymous with VFAs. These risk factors were neither considered in the BRA submitted at the time of the examination, nor with the updated BRA submitted with the representations.

The Committee considered this failure to constitute a substantially inadequate assessment in relation to an important aspect of the Company's AML/CFT obligations. In view of the above, the Committee found the Company to be in serious and systematic breach of Regulation 5(1) of the PMLFTR, Sections 3.3.1 and 3.3.3 of the IPs Part I.

Customer Risk Assessment – Regulation 5(5)(a)(ii) of the PMLFTR, Sections 3.5.1, 3.5.1(a), 3.5.2 and 3.5.3 of the IPs Part I, and Section 2.1 of the IPs Part II

The Committee in its deliberations considered that at the time of the examination, the only document available was a Word document simply containing a risk rating pertaining to the customers sampled during the review, without any explanation or rationale as to how this risk rating was assigned. It was also noted that two CRA methodologies were being used. The issue was that the methodologies used by the Company for the purposes of conducting the CRA were inadequate in that they did not consider the four risk pillars: one of the risk methodologies did not consider the product/service risk and the interface risk and in fact, took into account, the customer type, the complexity of the business, the business model and jurisdiction. On the other hand, the other risk methodology mentioned in the MLRO's interview completely excluded reference to the customer risk, product/service risk, and interface risk and simply considered the nationality, residential address, and telephone number of the customer.

It was further noted that the Company also had deficiencies in its jurisdictional risk assessment. The Company advised it was making use of a renowned system to determine the risk rating of a jurisdiction. While this is acceptable, the Manual being used did not delineated the methodology being used by the Company to risk assess jurisdictions. Additionally, the Company was also required to consult different sources including the European Commission list of third countries having strategic deficiencies in their AML/CFT regimes, countries subject to sanctions, embargoes, or similar measures issued by international organisations such as the United Nations or the European Union, countries identified as having significant levels of corruption as per the Corruption Perception Index, countries that fail to implement effective beneficial ownership transparency measures, and other lists. This would have enabled a more comprehensive understanding of the risks posed by the jurisdictions exposed to.

The Company's as Customer Acceptance Policy (CAP) failed to provide the necessary considerations to take to determine the risks posed by the customers as well as importantly to consider the specific risks pertaining to the virtual asset sector (including the use of proxies and unverifiable IP locations). The CAP also failed to delineate the circumstances against which the Company is to refuse customers. While positive of the improvements done by the Company to enhance the CAP as evidenced in its representations, the Committee noted that additionally detail as to the factors for risk classification should have been included.

Shortcomings in regard to the CRA were also noted in specific files –

- In 12% files, the customer risk rating assigned was unjustified;
- In another 12% files, no risk rating was assigned at onboarding (and performed over one year from when the Company became a Subject Person);

- In 20% files, the customers logged from countries which were neither associated with their residential address nor with their nationality, yet the geographical risk exposure posed through such connections was not considered by the Company;
- In 44% files, adverse media screening was performed after the business relationship had been established and in another 16%, no adverse media screening was provided to the officials.

In its representations, the Company reiterated that it is has performed a number of remedial measures including updates to its risk assessment methodology including the considerations in risk assessing the jurisdiction risks as well as enhanced its CAP. While the Committee was positive of such remedial actions which the Company initiated before the Committee took this regulatory action, it also noted that additional enhancements are necessary. This shall be closely monitor as part of the Committee's follow up action. The CMC could also not ignore the fact that at the time of the compliance examination, the Company had the aforementioned shortcomings and thus concluded that the Company had systematically breached Regulation 5(5)(a)(ii) of the PMLFTR, Sections 3.5.1, 3.5.1(a), 3.5.2 and 3.5.3 of the IPs Part I, and Section 2.1 of the IPs Part II.

Information on the wallet address – Section 2.2.1 of the IPs Part II

The Report noted that the Company was not collecting information on the address from which the customer was receiving or sending VFAs. Additionally, the Company's system was unable to determine whether the wallet being used by the customer was a private or multi-signature wallet or a custodial wallet. In its submissions, the Company explained that it is faced with challenges to adhere to this requirement i.e. to verify whether a wallet is a private one or a multi-signature wallet. The Company also referred to the introduction of a well-known system to monitor customer activity, which was positively noted by the Committee.

However, the Committee noted that the Company was expected to ask the customer for information on the wallet address, including whether the wallet being used was a private or multi-signature wallet. Whilst the CMC acknowledges the issues faced by the Company, it pointed out that Section 2.2.1 of the IPs Part II clearly refers to the need to determine the nature of the wallets i.e. whether they are private wallets, multi-signature wallets or custodial wallets on the basis of information provided by the customer. Subject persons are also expected to corroborate the said information.

Purpose and Intended Nature of the Business Relationship – Regulation 7(1)(c) of the PMLFTR, Section 4.4.2 of the IPs Part I and Section 2.2.3 of the IPs Part II

In 36% files reviewed which had not yet transacted at the time of the examination, the Company had failed to collect adequate information or had collected inadequate information on the source of wealth / source of funds (SOW / SOF) and anticipated level and nature of the activity.

The CMC reiterated that upon it becoming clear that the Company was to be considered a subject person, the Company had to start applying AML/CFT requirements vis-à-vis any new business relationships formed from that date onwards. The Company was also equally obliged to assess the information it held on its customers and obtain the required missing information to meet its obligations under the PMLFTR, including any information on the purpose and intended nature of any business existing relationship, if necessary. The Committee also noted that, although the ML/FT risks were minimal in these cases where the customers had not yet transacted, the absence of any control by the Company over the said accounts led to it not being possible to exonerate the Company from obtaining the relevant information on the business and risk profile of the customer.

Although in its representations, the Company provided screenshots of accounts which had been disabled, the Committee noted that the majority of these customers had been disabled in 2021 or 2022, and therefore over a year from when the Company had become a subject person. Therefore, the Company's representations could not be accepted in this regard.

Moreover, the Company noted that basic accounts have a limit of USD 1,000 and that these would render the customer as posing low risk. The Committee noted that the transactional activity is one of the considerations for the determination of low risk. Nonetheless, from the screenshots available it became clear that there were no

actual limits in the system as abovementioned. For these reasons, the low-risk nature of the customers could not be confirmed.

The Committee also found the Company in breach of its obligations to obtain information on the purpose and intended nature of the business relationship in regard to another 12% customers, which had transacted at the time of the compliance examination.

In the taking of its decision, the Committee also considered that, the Company held no information to create a comprehensive customer profile and be able to monitor the customer activity. However, it also considered the extent of the risk materialising, observing that 36% of the customers had not transacted at all.

In view of the above reasons, the CMC determined that the Company had breached its obligations under Regulation 7(1)(c) of the PMLFTR, Section 4.4.2 of the IPs Part I and Section 2.2.3 of the IPs Part II.

Identification and Verification of the Customer – Sections 4.3.1.1(i) and 4.3.1.2(i) of the IPs Part I

The Report noted that the Company failed to verify the identification of 44% customers. In its representations, the Company attached documentation showing identification information of the customer. Nonetheless, the screenshots provided did not contain any evidence that verification documents were indeed obtained and retained. Consequently, the Committee did not accept the Company's submissions and determined that it was in breach of Sections 4.3.1.1(i) and 4.3.1.2(i) of the IPs Part I.

Enhanced Due Diligence – Regulation 11(1)(b) of the PMLFTR and Sections 4.9 of the IPs Part I

Shortcomings in relation to Enhanced Due Diligence (EDD) were noted in 4 files examined during the compliance examination.

In one particular file, the customer being serviced was resident in a country which at the time of the compliance examination was on the Financial Action Task Force (FATF) list of jurisdictions under increased monitoring. Despite the fact that the customer never traded, it was only blocked in February 2022. Thus, the customer could have traded whenever it wanted up until February 2022 and thus, the Company's representations that the customer never traded could not exonerate the Company from performing EDD.

In another file, the customer was receiving loans from another customer. The Committee could not understand the rationale behind these loans, something which the Company failed to query or investigate, despite the large values of transactions processed. Indeed, one of the transactions processed by the customer amounted to 29.4BTC (equivalent to over €1million). This extremely high amount was not queried by the Company. The Company failed to understand the purpose of these loans and whether there was an economic rationale for the same, ensuring their legitimacy. The amount being processed should have prompted the Company to obtain information and documentation on the transaction. In its representations, the Company clarified that it is carrying out updates on the KYC details of this customer, and consequently, applying the necessary EDD measures. While the Committee was positive of noting such a remedial action, it could not discount the risks observed by allowing such transactions to take place without performing the required EDD measures, including performing enhanced ongoing monitoring on the business relationship.

Consequently, the CMC concluded that the Company had failed to perform EDD in relation to 4 customer files in terms of Regulation 11(1)(b) of the PMLFTR and Sections 4.9 of the IPs Part I.

Transaction Scrutiny – Regulation 7(2)(a) of the PMLFTR, Sections 4.5.1(a) and 4.5.2.3 of the IPs Part I and Section 2.2.5 of the IPs Part II

The Committee noted that the Company had several shortcoming relating to transaction scrutiny. The Company stated to monitor transactions over €10,000 manually through Chainanalysis. However, considering the voluminous transactions being processed and the ease with which such transactions are processed, it is rather worrying that the Company did not have systems in place to monitor transactions. Such monitoring system not only had to include post transaction monitoring however also real-time monitoring for high risk situations such as large value transactions. Moreover it was noted that the detail as to when to conduct manual monitoring is not

reflected nor detailed in the Company's transaction monitoring policy which was considered to be rather generic and not tailor-made for the Company's business.

While noting the Company's manual monitoring measures, the effectiveness of the same considering the ease with which transactions are processed as well as the volume of the transactions passing through is highly questioned. This was further exacerbated through the fact that the Company had insufficient information on the risk profile of the customer, rendering monitoring of the customer relationship even more difficult in view of the inability to monitor the customer activity against its abilities and against that expected from the same. Moreover, the fact that the transaction monitoring policies were not sufficiently detailed rendered the carrying out of manual scrutiny more difficult and more subjective.

Moreover, the Committee proceeded to examine a transaction of 1,000,000 USDB (equivalent to €886,893). The amount being withdrawn to fiat was not within the usual withdrawal transactional pattern of the customer. Indeed, as per the transactional withdrawal history of the customer, it appears that the customer's highest withdrawal was in June 2020 for the amount of USDB300,300. The rest of the amounts withdrawn by the customer were all USB100,100 or under. Consequently, the withdrawal mentioned in the Report should have alerted the Company and prompted it to obtain further information on this transaction. In its representations, the Company acknowledged the fact that it should have collected more information on this transaction. This rendered the Company in breach of its transaction monitoring obligations.

In view of the above, the Committee determined that the Company was in breach of its transaction scrutiny obligations in terms of Regulation 7(2)(a) of the PMLFTR, Sections 4.5.1(a) and 4.5.2.3 of the IPs Part I and Section 2.2.5 of the IPs Part II.

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

After taking into consideration the abovementioned findings together with (i) the nature of the services and products offered by the Company including the size of the Company; (ii) the Company was overall cooperative during the compliance examination as well as the remedial action the Company had started to implement on its own motion before it was directed to do so by the FIAU (iv) the seriousness and at times systemic nature of the obligations breached; (iv) the fact that such breaches could have a large impact on the jurisdiction; (v) the Company's minimal regard to its AML/CFT obligations at the time of the examination, the Committee decided to impose an administrative penalty of two hundred twenty thousand, nine hundred, ninety-two euro (€220,992) in relation to the following breaches:

- Regulation 5(1) of the PMLFTR and Sections 3.3.1 and 3.3.3 of the Implementing Procedures (IPs);
- Regulation 5(5)(a)(ii) of the PMLFTR, Sections 3.5.1, 3.5.1(a), 3.5.2 and 3.5.3 of the IPs Part I, and Section 2.1 of the Implementing Procedures, Part II, VFA Sector (IPs Part II);
- Section 2.2.1 of the IPs Part II;
- Regulation 7(1)(c) of the PMLFTR, Section 4.4.2 of the IPs Part I and Section 2.2.3 of the IPs Part II;
- Sections 4.3.1.1(i) and 4.3.1.2(i) of the IPs Part I;
- Regulation 11(1)(b) of the PMLFTR and Sections 4.9 of the IPs Part I;
- Regulation 7(2)(a) of the PMLFTR, Sections 4.5.1(a) and 4.5.2.3 of the IPs Part I and Section 2.2.5 of the IPs Part II.

The Committee also considered that it could not proceed to impose a Directive to take remedial action on the Company, because it had filed for the surrender of its license.

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

Key take-aways

- The fact that the Company was not a subject person at the time when certain customers were onboarded did not exonerate the Company from applying the appropriate AML/CFT obligations in relation to such files / customers upon it becoming a subject person. In fact, upon an individual or entity becoming a

subject person, they are expected to adhere to the Prevention of Money Laundering Act, Prevention of Money Laundering and Funding of Terrorism Regulations, Implementing Procedures, and any other guidance issued by the FIAU. This including by having the necessary policies and procedures in place as well as ensuring that CDD is performed on customers on a risk sensitive basis

- The BRA and CRA of VASPs is to consider specific risks pertaining to this sector including, the risks emanating from the use of proxies, unverifiable IP addresses or geographical location, disposable email addresses or mobile numbers, and the use of different devices to conduct transactions by the customer to obscure actual locations (as per Section 2.1 of the IPs Part II).
- In the instance that customers are utilising IP addresses originating from jurisdictions which differ from those countries to which customers had declared that they were linked, subject persons are expected to query the reasons behind such divergence. Subject persons are expected to revise their CRA accordingly, including where applicable by taking the IP location as an additional risk indicator in the performance of the CRA.
- When a customer has material links to a jurisdiction (including the place of residency and the place from where the customer operates), subject persons are expected to assess the risks arising from that particular jurisdiction. If the jurisdiction is on the FATF list of jurisdictions under increased monitoring or on the EU lists as well as if jurisdictions are found to have risks emanating from other considerations, then the subject person is expected to apply EDD on a risk-sensitive basis in order to mitigate the high-risk associated with such a relationship.
- Obtaining information on the purpose and intended nature of the business relationship, including information on the SOW/SOF of the customer, the anticipated level and nature of the activity of the customer, as well as the customer's business/occupation/profession is crucial not only to build a comprehensive business and risk profile but also to be able to conduct efficient and effective transaction scrutiny.
- Products may have thresholds for customer activity and such threshold may indeed limit the risk exposure of the subject person. However, the carrying out of a comprehensive assessment on each customer is still necessary. Moreover, such thresholds should be clearly embedded in the measures implemented for monitoring customer activity through such products ensuring that such imposed thresholds could not be exceeded in any manner by the customer.

2 February 2023

APPEAL - On the 23rd of February 2023, the FIAU was served with a copy of the appeal application filed by the Company before the Court of Appeal (Inferior Jurisdiction), from the decision of the FIAU.

The Company states, *inter alia*, that the FIAU's methodology is unclear; that the administrative penalty imposed upon it is excessive and disproportionate and that it cannot exercise its right of appeal in an effective manner. It also states, among other things, that the legal basis of the FIAU's decision is defective; that the FIAU based its decision on considerations and conclusions which are subjective or erroneous and that the same decision has fundamental human rights implications. It also claims that considering it had surrendered its license four months prior to the FIAU's decision, it was no longer a subject person according to law.

The Company thus asked the Court to revoke and annul the decision of the FIAU in its regard, or alternatively, to modify and reform the said decision by reducing the penalty imposed upon it.

Pending the outcome of the appeal, the decision of the FIAU is not to be considered final and the resulting administrative penalty cannot be considered as due, given that the Court may confirm, vary or reject in whole or in part, the decision of the FIAU. As a result, the FIAU may not take any action to enforce the administrative penalty pending judgement by the Court.

This publication notice shall be updated once the appeal is decided by the Court so as to reflect the outcome of the same.

24 February 2023