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 Pro Limited

SUPERVISORY ACTION:

Compliance review carried out in 2021

DETAILS OF THE ADMINISTRATIVE MEASURES IMPOSED:

Administrative Penalty of Euro 242,243 and a Remediation 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 3.3.1 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;
- 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 Company's Business Risk Assessment (BRA) had been drafted late and at the time of the examination, had not been approved by the Board of Directors.
- The BRA lacked sufficient consideration to risks which the Company is exposed to.
- 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 is incorrect. It refers to the residual risk rating of an unrelated financial institution.

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 systematic breach of Regulation 5(1) of the PMLFTR, Sections 3.3.1 and 3.3.3 of the IPs Part I.

Csustomer 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 containing a risk rating pertaining to the customers, without any explanation or rationale as to how this risk rating was assigned. It was also noted that two CRA methodologies were allegedly being used. The fact that there were two methodologies differing for corporate customers and individual customers was not wrong in and of itself. 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.

The Company also had deficiencies in its jurisdictional risk assessment as well as in its Customer Acceptance Policy (CAP), and failed to consider the specific risks pertaining to the virtual asset sector (including the use of proxies and unverifiable IP locations).

The CMC also noted that in 10 files, the customers logged from countries which were neither associated with their residential address nor with their nationality. The CMC concluded that the Company should have sought an explanation from the said customers as to why there was this divergence.

In its representations, the Company reiterated that it is has performed certain remedial measures including updates to its CAP. Nonetheless, the CMC could 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 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 5 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.

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 8 customers, which had transacted at the time of the compliance examination. Thus for instance, in one particular case, the only information on file was a bank statement indicating the balance. The CMC determined that this was definitely not sufficient to establish the business and risk profile of the customer. The Company should have obtained information on the activity and business of the customer, any other source of wealth, its expected source of funds and its anticipated level and nature of transactions.

In view of the above reasons, the CMC determined that the Company was in breach of 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 at the time of the compliance examination.

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 2 files examined during the compliance examination.

The Committee noted that the customer was assigned a high-risk rating by the Company as it had been incorporated in a jurisdiction placed on the Financial Action Task Force (FATF) list of jurisdictions placed under increased monitoring and was involved in crypto trading and crypto business. Despite the links to this jurisdiction, the Company failed to conduct EDD on the customer.

It was also observed that the customer was processing a large amount of transactions within a very short period of time. The Committee indeed noted that hundreds of transactions were taking place every single day for this particular customer. Both the value and volume of transactions should have in and of themselves prompted the Company to conduct enhanced ongoing monitoring on this customer and ascertain that the transactions were not derived from ML/FT. One of such transactions amounted to €1.078million worth of cryptocurrency – the only supporting documentation found on file was a screenshot that the transaction was executed. No further information and documentation was furnished by the Company despite the fact that this was a high-risk customer. The Committee noted that the information found on file was definitely not sufficient to mitigate the ML/FT risks associated with this relationship. Given the high value of the transaction processed, the Company was expected to understand the source(s) funding the transaction, including by obtaining documentation to support the information provided by the customer.

Finally, the CMC also noted that the information found on file was not sufficient to determine the purpose and intended nature of the business relationship, and that this simply consisted in the Memorandum and Articles of Association of the customer, and the financial statement of another company. The Committee therefore determined that the Company not only failed to conduct EDD but also to obtain basic information on the purpose and intended nature of the customer.

Consequently, the CMC concluded that the Company had failed to perform EDD in relation to 2 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 namely –

- The failure to have a real-time or post-transaction monitoring system;
- The fact that transactions over €10,000 are manually checked through Chainanalysis and that this process is not mirrored in the Company's transaction monitoring policy;
- The generic nature of the Company's transaction monitoring policy and the fact that it is not tailor-made for the Company; and
- The Company's failure to adequately scrutinise the transaction (withdrawal) mentioned in 1 file of 1,000,000USDB (equivalent to €887,280).

The Committee considered that it is worrying that the Company did not have an automated system to monitor transactions, neither prior to the transaction being effected, nor after the processing of the same. This was further exacerbated through the fact that the Company had insufficient information on the risk profile of the customer as well as the fact that the transaction monitoring policies were not sufficiently detailed.

The CMC considered the Company's submissions which provided a screenshot of a note made by an employee of the Company stating: *'Withdrawal request update for 1Mil USD – Client replied and explanation makes sense. Also the date of the binance withdrawal and amount matches with CRM data*'. The CMC determined this note as insufficient; it cannot be considered as an adequate means to understand whether the transaction had originated from legitimate funds or otherwise. While it is especially important to understand how funds, be they in FIAT or VFA are generated when deposited with an institution, it is also important for subject persons to understand the reason behind particularly large transactions. Consequently, the Company was expected to understand the purpose behind this withdrawal especially considering the high value (USDB 1,000,000 equivalent to EUR 887,280) being processed. Therefore, the CMC determined that the Company had breached its obligations to conduct efficient and effective transaction scrutiny.

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 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 forty-two thousand, two hundred and forty-three euro (€242,243) 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;
- 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 served the Company with a Follow-up Directive (Directive) in virtue of the FIAU's powers under Regulation 21 of the PMLFTR. The purpose of this Directive is for the FIAU to assess whether the Company is fully compliant with the obligations imposed in terms of the PMLFTR and the Implementing Procedures issued thereunder, as well as to monitor the progress being achieved by the Company through the self-remediation project it has started. The Directive is also intended to ensure that the Company remedies all the AML/CFT breaches relayed throughout this letter.

In virtue of this Directive, the Company is expected to make available an Action Plan within eight weeks from the date of receipt of the letter which shall include:

i. Clear reference to the actions points that have already been completed together with a summary of the process carried out by the Company to implement said action points and any evidence to prove that these action items have actually been implemented in practice, including but not limited to:

    a) The latest version of the CRA adopted by the Company, CRA Methodology, updated AML/CFT Policy, Customer Acceptance Policy and Risk Appetite Framework, approved by the Board of Directors, as outlined in the Company's letter of 28 September 2022;
    b) New Customer Due Diligence matrix and updated onboarding form;
    c) Revision of the Company's policy framework, including the adopting of transaction monitoring specific documentation.
    d) Updates on the client file review remediation being performed by the Company; and
    e) Updating transaction monitoring policy.

The Action Plan shall as a minimum outline the action points intended to address the breaches highlighted in this letter, as well as any other additional enhancements being implemented by the Company, including but not limited to action points relating to:

a. The reassessment of the CRA of all 20 customer files, using the latest CRA adopted by the Company;
b. Updated policies and procedures in relation to obtaining information on the purpose and intended nature of the business relationship and the manner in which the Company intends to address the shortcomings pertaining to this obligation, through obtaining detailed and specific information on the business and risk profile of its customers, SOW and SOF; and
c. The manner in which the Company intends to address the shortcomings pertaining to Enhanced Due Diligence, including through the collection of sufficient and adequate information and documentation on the customer as well as the performance of enhanced ongoing monitoring.

Finally, the Committee stipulates that in the eventuality that the Company fails to make the abovementioned documentation and information available with the specified deadline, the Company's default shall 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 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.

<u>Key take-aways</u>

- 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.

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.

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