Administrative Measure Publication Notice

This Notice is being published by the Financial Intelligence Analysis Unit (the FIAU) in terms of Article 13C of the Prevention of Money Laundering Act (the 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:

1 April 2025

SUBJECT PERSON:

OKCoin Europe Limited

RELEVANT ACTIVITY CARRIED OUT:

Virtual Asset Service Provider (VASP)

SUPERVISORY ACTION:

Onsite compliance examination carried out in April 2023

DETAILS OF THE ADMINISTRATIVE MEASURE IMPOSED:

An administrative penalty of €1,054,269 and a Follow-Up Directive in terms of Regulation 21 of the Prevention of Money Laundering and Funding of Terrorism Regulations (the PMLFTR)

LEGAL PROVISIONS BREACHED:

The following breaches, as determined by the Committee, took place up to April 2023 and in the preceding years:

- Regulations 5(1) and 5(4) of the PMLFTR, Sections 3.2, 3.3 and 8.1 of the IPs – Part I, and Section 2.1 of the IPs – Part II for the VFAs Sector
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.4 and 3.5 of the IPs – Part I
- Regulation 7(1)(c) of the PMLFTR and Sections 3.4 and 4.4.2 of the IPs – Part I
- Regulations 7(1)(d), 7(2)(a), 7(2)(b), 11(1)(b) and 11(9) of the PMLFTR, Sections 4.5.1, 4.5.2, 4.5.3 and 4.9 of the IPs – Part I, and Section 2.2.1 of the IPs – Part II for the VFAs Sector
- Regulation 15(3) of the PMLFTR and Section 5.5 of the IPs – Part I
- Regulations 5(5)(b) and 5(5)(e) of the PMLFTR and Section 7.3 of the IPs – Part I

REASONS LEADING TO THE IMPOSITION OF THE ADMINISTRATIVE MEASURE:

Business Risk Assessment (BRA) – Breach of Regulations 5(1) and 5(4) of the PMLFTR, Sections 3.2, 3.3 and 8.1 of the IPs – Part I, and Section 2.1 of the IPs – Part II for the VFAs Sector

At the time of the compliance examination in 2023, the Company had compiled a BRA in an attempt to identify the threats and vulnerabilities it is exposed to. Notwithstanding, deficiencies were noted within the Company's BRA methodology, making it unable to properly assess the risks of ML/FT it was exposed to and to adequately apply the required mitigating measures to manage them. Some of the deficiencies identified include:

- Failing to adequately assess the ML/FT risks emanating from its product offerings. As despite not being expected to include an assessment for every coin being offered, the Company was required to categorise such offerings and assess the ML/FT risks of specific categories of coins/product related features. Including assessing the ML/FT exposure emanating from the potential use of mixers/tumblers, privacy coins, use of tokens on decentralised exchanges and stablecoins. Also, the Company was expected to assess the nature of risks prevalent in the services it was offering, distinguishing between for example custody and exchange services.
- It is acknowledged that the Company had quantitative data at its disposal and had the means to extract the same from its systems. What it lacked, however, was a consideration of such data in order to statistically form a clearer opinion of the threats and vulnerabilities its business was exposed to. Without such statistical information, it is impossible to truly understand risks and ensure that resources are effectively targeting the areas of highest concern. For example:
    - To establish material links with jurisdictions, the Company was required to consider any ties with jurisdictions through the sources funding the customers' activity and through the location of service providers hosting the customers' wallets. This would have ensured that any material exposures to jurisdictions were identified and each of such jurisdictions were adequately and comprehensively assessed.
    - Quantifying the number of customers per product cluster reveals concentrations of ML/FT risks. This including distinguishing between products involving potential anonymity as well as understanding the types of services mostly used and any risks exposed through the same. Even the type of trades undertaken by customers should be well understood. Also, understanding the volume per product and service will indicate where best to focus the controls required. Indeed, by understanding the average transaction volume of specific product clusters, the Company could have set more appropriate transaction monitoring thresholds for each product or service.
- Despite the Company's strategy adopted to only service European-based customers, it was essential to also consider the potential ML/FT exposure emanating from other jurisdictions, including from where the sources of the customers' funding originated.

Notwithsdating the above deficiencies, the proactive remediation undertaken by the Company following the compliance examination was also acknowledged, this including:

- The Company's BRA enhancements to employ more rigorous considerations, including specific ML/FT risk factors per risk pillar as required in terms of the IPs.
- A combination of qualitative and quantitative methods to evaluate the severity and likelihood of each identified risk factor within its BRA.
- Updating of the Company's jurisdiction risk assessment to include additional considerations.

Customer Risk Assessment (CRA) – Breach of Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.4 and 3.5 of the IPs – Part I

Failures were identified in relation to the Company's CRA methodologies adopted to assess the ML/FT risks emanating from its customers, both natural persons and legal entities. This since:

- While positively acknowledging that the Company was undertaking adverse media screening on its customers, the results of the screening undertaken did not feature as part of the CRA methodology adopted by the Company, this as required in line with Section 3.5.1(a) of the IPs – Part I.

- The Company's CRA methodology classified the assessment across two types of coins being '*High Risk Coins*' vs '*Low Risk Coins*'; however, parameters to identify which token clusters are to be classified into such risk categories were not established nor recorded.

- While the considerations adopted do provide for some information as to the customers' source of funds, as evident in practice, this was not sufficient. While conscious of the fact that the drop-down menus cannot include all different types of industries, the Company was required to ensure that the ML/FT risk emanating from specific industries was adequately taken into account in assessing its customers. Moreover, the sources funding the customers' activities should have been first, more adequately understood, and second, comprehensively factored in assessing the customers' risks.

- Despite the Company having a set token listing process and assessment undertaken prior to each listing, it was still required, as part of its CRA, to distinguish between specific characteristics of its product offerings (as already referenced under the BRA section).

Moreover, the Company was found to have failed to carry out a CRA upon establishing a business relationship for around 50% of the customer files reviewed as part of the compliance examination. Despite the Company's submissions that a CRA was conducted at onboarding for these customers, the evidence collected indicates that such clients had deposited thousands of dollars before a CRA was completed, with such assessment being conducted several months following onboarding.

Notwithstanding the above-mentioned deficiencies, the enhancements implemented by the Company to remediate its shortcomings identified during the compliance examination were positively acknowledged, this including:

- Migrating the CRAs pertaining to both legal and natural persons onto one automated system.
- Enhancing the list of industries to cater for other ML/FT factors across different industries to which its customers may be exposed to.
- Including additional funding methods to cater for specific ML/FT risks.
- Other enhancements in line with the shortcomings identified during the compliance examination.

Purpose and Intended Nature of the Business Relationship and the Customer's Business and Risk Profile – Breach of Regulation 7(1)(c) of the PMLFTR and Sections 3.4 and 4.4.2 of the IPs – Part I

According to the compliance examination report, at the time of the compliance examination in 2023, the Company obtained the information needed to formulate business and risk profiles for its customers by requiring them to populate certain details through a drop-down menu selection as part of the account registration process, with the type of information varying based on whether the client was a natural or a legal person. Amongst other data points, information collected for natural persons included the purpose of the account, occupation, source of funds, and expected deposit volume. For legal persons, details such as the customer entity type, industry, source of funds, and anticipated transaction volumes were gathered. The drop-down menu options were limited, offering only a few selections per data point. Some examples included: (a.) "*health and social care*", "*legal and social professionals*", and "*information and communication technology services*" for occupation; (b.) "*professional service provider*", "*financial service business*", and "*crypto exchange company*" for customer type; and (c.) "*employment*", "*savings*", "*investments*", "*business*", and "*invest with the company's user funds*" for source of funds (as applicable to natural or legal persons, respectively).

The aforementioned information was considered overly generic and insufficient for appropriately understanding and managing the specific risks pertaining to the source of wealth (SOW) and expected source of funds (SOF) to be used by the customer during the course of the business relationship, as well as for gaining insights into the client's occupation or business activity and any risks associated with the same. This failure was especially concerning given that no additional information or clarifications were sought from customers, which became increasingly important as the relationships progressed and the clients' activity grew more prominent. The above approach is also in line with Section 4.4.2 of the IPs – Part I, which stipulates that subject persons are not to restrict the acquisition of information to generic terms such as "*business*", "*employment*", or "*inheritance*", but should ensure that such information is relevant and adds value to the business and risk profile of the customer.

The compliance examination report went on to highlight a number of specific customer files in respect of which the Company failed to collect information on the customers' anticipated level of activity and occupation. Through its representations, the Company rebutted this observation, stating that each of these clients had opted for a basic account at the onboarding stage, as deposits were not expected to exceed €1,000. Therefore, in light of this, the clients in question were automatically assigned a low risk rating and, in turn, subjected to simplified due diligence (SDD) measures, resulting in certain information, such as the anticipated level of activity and occupation, not being obtained. During its discussions, the Committee confirmed that, in the case of each customer file where such deficiency was observed, the Company had breached its AML/CFT obligations by failing to gather the necessary information regarding the anticipated level of activity and occupation at any point during the business relationship. Further supporting this decision is the fact that the lifetime deposits of each of these customers greatly surpassed the €1,000 mark, with the majority of clients reaching this threshold from their very first deposit. Notwithstanding the above, the Committee positively acknowledged that, following the completion of the compliance examination, the Company reviewed most of the customer files involved and took remedial action, either by acquiring the required information or freezing accounts due to non-cooperation. The Committee also gave positive consideration to the fact that the Company has since discontinued the offering of the basic account, with any clients wishing to continue their relationship needing to undergo re-onboarding, which includes full CDD measures and a comprehensive risk assessment.

In view of the above, the Committee determined that the Company had repeatedly failed to obtain the requisite information and, on a risk sensitive basis, supporting documentation to establish

business and risk profiles that accurately reflect the actual transactions and activities of its customers. Despite this decision, the Committee commended the fact that, after the compliance examination, the Company enhanced its internal processes by introducing more granularity in the information collected for the purpose of building business and risk profiles for its clients. Such granularity should undoubtedly result in a deeper understanding of the customers, as well as more effective ongoing monitoring throughout the business relationships.

Ongoing Monitoring and Enhanced Due Diligence (EDD) – Breach of Regulations 7(1)(d), 7(2)(a), 7(2)(b), 11(1)(b) and 11(9) of the PMLFTR, Sections 4.5.1, 4.5.2, 4.5.3 and 4.9 of the IPs – Part I, and Section 2.2.1 of the IPs – Part II

The next section of this document will focus on concerns raised in the compliance examination report regarding the Company's non-compliance with its obligations related to ongoing monitoring and EDD. A summary of the findings identified in relation to these two distinct obligations can be found below:

a.) Ongoing monitoring

- Transaction monitoring – For around 80% of the customer files reviewed, it was noted that the Company failed to adequately scrutinise the transactions being executed, which collectively amounted to more than $20 million. Although at the time when the compliance examination took place, the Company had an automated transaction monitoring system in place configured on the basis of detection rules which generated alerts when certain thresholds or criteria were met, these alerts were not being properly reviewed or followed-up on, and were often discounted without sufficient justification. In each instance, there were evident risk factors and red flags which necessitated more comprehensive scrutiny of the transactions, including:
    - Transactions not in line with the customer's established profile, with stark discrepancies identified between the client's expected and actual activity.
    - Lack of adequate scrutiny of substantial transactional activity, encompassing regular, high-value individual deposits, accumulated large lifetime deposits, or both.
    - Deposits made in fiat currency or cryptocurrency, which are then exchanged into other currencies and rapidly withdrawn within a short timeframe, sometimes in just hours or even minutes.
    - Unexplained or high spikes in deposits over short periods, either occurring over a certain number of days or an extended period of time (e.g. a month).
    - Sudden surge in activity following a period of dormancy, which was not noticed at all or flagged.
    - Inadequate SOW/SOF information and supporting documentation collected that failed to substantiate the customer's voluminous activity and large transaction values passing through the account. There were also cases where, although certain documents were collected by the Company, these were not properly reviewed for consistency or relevance. Had proper scrutiny been carried out, it would have become even more apparent that there was a mismatch between the activity undertaken and the available information/documentation, thereby meriting further scrutiny.
    - Supporting documentation, such as bank statements, which only showed the flow of funds across accounts, not the actual origin of the funds.
    - Inadequacies in the limited customer file reviews carried out, which failed to yield a concrete understanding of the customer, or the funding sources used. EDD requests

appeared to be more of a procedural formality rather than a genuine attempt to gather the necessary information and documentation in order to understand its implications.
    - Inappropriate discounting of transaction monitoring alerts, involving the discounting of alerts without sufficient rationale or follow-up action taken to ensure that the flagged activities were indeed legitimate.
    - Issues with the quality and calibration of transaction monitoring alerts, as customers with relatively low activity often triggered a large number of alerts, while those engaging in high value and high-volume transactions generated only a handful of alerts. Ultimately, none of these alerts were properly reviewed and assessed.

- Keeping information, data, and information held on the customer up-to-date – In a few customer files, all rated as high risk, periodic reviews were found to be overdue, with the pre-defined frequency of review not being adhered to, which failure could have led to customer-related information, data or documents becoming outdated. Moreover, in a small number of cases, identity verification documents, such as identity cards and passports, were discovered to have been expired for as long as two years, meaning that the Company had not taken the necessary steps to re-obtain up-to-date and valid documents from these clients.

b.) EDD

- Application of EDD measures – With respect to around 15% of the customer files under review, either classified as high risk or assigned a different risk rating but exhibiting high risk elements, the Company neglected to implement EDD measures, which include not collecting appropriate SOW/SOF information and documentation, as well as not conducting enhanced transaction scrutiny. By failing to employ such EDD measures, the Company was not in a position to ensure that the higher risks presented by certain customers, products, services, and transactions were being monitored and managed in an effective manner.

- Control over the wallet address – As stipulated in Section 2.2.1 of the IPs – Part II for the VFAs Sector, if a customer utilises a private wallet to send VFAs to the VFA service provider, the latter has to establish that the former has control over the address from which the VFAs originate. While this requirement is not mandatory in all instances, it must be applied on a risk sensitive basis, notably in scenarios involving significant amounts of VFAs being processed. Regarding a number of high risk customers forming part of the compliance examination sample and making use of a private wallet, it was observed that the Company did not gather any proof of control over the wallet addresses, even though the cryptocurrency deposits made by these clients over the lifetime of their business relationships were of a significant value, ranging from $160,000 to $1.3 million.

It is important to note that all customer files in which shortcomings pertaining to the application of EDD measures were noted also featured deficiencies in transaction monitoring. Therefore, when analysing the portion of customer files reported under the transaction monitoring obligation, the Committee took a holistic approach for files that also had EDD failings, considering breaches related to both obligations in its assessment. Some examples illustrating transaction monitoring and EDD breaches, as applicable, are presented hereunder.

- Customer file A – This customer, a natural person, was onboarded in June 2019 and held a low risk rating at the time of the compliance examination. The only information obtained at onboarding from a customer profiling perspective was that such client worked within the information technology industry, had investments as their source of funds, and was estimated to deposit €100,000 a month. During the years 2019 and 2020, the customer engaged in limited activity, with total deposits not exceeding $50,000. However, in 2021, over a period of less than four months, the client made cryptocurrency deposits amounting to approximately $1.8 million. In this case, not only was the declared anticipated activity of the client substantial, warranting further questioning, but there were months where the deposits made significantly surpassed the €100,000 threshold. At the point in time when the client was engaging in high-value deposits, these transactions were not being scrutinised by the Company, save for one instance where the Company reached out to the customer to query the purpose of the account and the funding sources for the deposits, to which the client provided short, generic replies that were not corroborated. In October 2022, more than a year after the customer was last active, a risk ad-hoc review was conducted, and an EDD documentation request was made. However, this request went unanswered, resulting in the account being frozen.

- Customer file B – Here, the customer is once again a natural person who was onboarded in March 2021 and classified as medium risk at the time of the compliance examination. The only information collected at onboarding from a customer profiling perspective was that such client worked within the health and social care industry, had savings as their source of funds, and was estimated to deposit €25,000 a month. In this case, the client's typical transactional pattern involved depositing cryptocurrency and withdrawing the equivalent amount in USD on the same day, sometimes within just a few hours, a technique commonly used to obfuscate the origin of funds through multiple transactions. Activity began a few days following onboarding and continued for over a year and a half, during which almost $490,000 were deposited. Most of the deposits did not exceed the $40,000 mark, but there was a spike towards the end of 2021, when deposits of nearly $100,000 were made in a single day. A risk ad-hoc review only took place in March 2022, at which point it was recommended that a bank statement be requested from the client; however, this request was not followed-up. A total of 50 transaction monitoring alerts were generated for this customer, but they were discounted with insufficient rationale, with only the aforesaid risk review being taken as a follow-up action.

- Customer file C – The customer in question consists of a legal person onboarded in May 2021 and designated as high risk at the time of the compliance examination. At onboarding, the information gathered regarding the customer's business and risk profile indicated that this customer entity was a professional service provider, with business as its source of funds, and anticipated volumes of €10 million a year. However, no documentary evidence was obtained to substantiate such expected level of activity. Initially, the client did not exhibit any activity, with the first deposit occurring a year post-onboarding. Nevertheless, in the nine months following this date, the customer made nearly $980,000 in deposits. During the second half of 2022, the customer entity consistently affected high value deposits, often ranging in the tens of thousands of dollars, with one even exceeding $200,000, which was immediately withdrawn. Yet, such transactions were not corroborated to ensure their legitimacy. A payslip from the second quarter of 2022, pertaining to the entity's beneficial owner, which displayed a year-to-date salary of around AUD $115,000, was acquired. However, this document was deemed insufficient to justify the amounts being transacted, not only because the declared

salary amount was smaller than the transactional activity, but also since there was no tangible evidence of the extent to which the beneficial owner was providing financing to the customer. A total of 90 transaction monitoring alerts were generated for this client, but they were all discounted on the grounds that no unusual activity was detected, with limited follow-up actions taken.

Notwithstanding the concerns relayed above, the Committee positively recognised the general enhancements made by the Company to its transaction monitoring framework post-compliance examination, which now includes the integration of several robust transactions monitoring systems, notably one specific system for the monitoring of fiat and off-chain cryptocurrency transactions and a separate system for the monitoring of on-chain cryptocurrency transactions. The Committee is also aware of the fact that the Company has now implemented robust audit and quality control checks to ensure that the alerts generated are being discounted appropriately and that adequate and comprehensive justification is maintained; otherwise, the alert is escalated if necessary. According to the Committee, the improvements made by the Company represent a considerable advancement over the transaction monitoring framework in place at the time of the compliance examination, with such upgrades expected to facilitate the identification of unusual and suspicious transactions, as well as augment the process surrounding the discounting of alerts. Further to the above, in terms of the EDD process, refinements have been implemented to ensure the standardisation and streamlining of document requests at the appropriate stages in the business relationship, as needed.

External Reporting – Breach of Regulation 15(3) of the PMLFTR and Section 5.5 of the IPs – Part I

The Committee was informed that, in relation to one specific customer file, the Company failed to submit a Suspicious Transaction Report (STR) with the FIAU, despite a number of red flags being present throughout the business relationship. By way of background, this customer was onboarded in April 2021 and assigned a high risk rating by the Company at the time of the compliance examination. The only information obtained by the Company at onboarding was that the source of funds of this client was derived from investments and that the purpose of the account was trading. However, no details were collected in relation to the customer's occupation, anticipated level of activity, or the specific investments that would be funding his trading activity.

In terms of activity, the customer's transactional pattern involved making cryptocurrency deposits and subsequently withdrawing funds in fiat currency within a short period of time, usually, a few hours. Within the first three months following the commencement of the business relationship, the client's deposits amounted to almost $1.2 million, while withdrawals exceeded $1.4 million.

In response to an EDD documentation request made in May 2021, the customer provided, amongst other documents: (a.) a bank statement showing numerous incoming and outgoing transfers involving a variety of individuals and entities, the client's relationship with which was unknown; (b.) a private purchase agreement documenting the customer's purchase of certain cryptocurrency tokens for a consideration equivalent to less than $50,000; (c.) a declaration stating that he was the owner of two companies.

Given the client's voluminous activity and transaction pattern not being in line with the stated profile, additional requests were made to the customer, who either failed to provide the required clarifications and documentation or, when he did respond, offered contradictory information. This prompted one of

the Company's risk investigators to file an internal report, which outlined several concerns. Despite this, the internal report was closed shortly after, with no further action taken.

In passing its deliberations, the Committee held that, considering the array of red flags identified over the course of the business relationship, some of which had serious implications, it is evident that the Company was obligated to submit an external report with the FIAU. The specifics of these red flags are elaborated below:

- The customer engaged in significant transactional activity, exceeding $1 million in deposits within a three month timeframe. Several large amounts were deposited, which notably includes an initial deposit of $170,000 made just a few days after onboarding.
- The transactional pattern, which involved cryptocurrency deposits from private wallets owned by the customer, followed by rapid withdrawals of funds in fiat currency soon thereafter.
- Almost 30 alerts were generated by the Company's transaction monitoring system during the period of activity; however, these alerts were not properly looked into by the Company and were inappropriately discounted.
- The supporting documentation collected by the Company, consisting of a bank statement and a private purchase agreement, were insufficient to justify the customer's overall activity as well as the large transactions involved.
- Various different risk investigators flagged the activity exhibited by the customer as suspicious and inconsistent with his profile; however, these concerns did not translate into the submission of an external report with the FIAU.
- The customer was non-cooperative, refusing to provide any additional documentary evidence beyond what was submitted in response to the first EDD documentation request.

Training and Awareness – Breach of Regulation 5(5)(b) and 5(5)(e) of the PMLFTR and Section 7.3 of the IPs – Part I

While positively acknowledging that the Company's employees were provided with training pertaining to AML/CFT matters, this was not tailored to the Company's own AML/CFT policies and procedures as required in terms of Section 7.3 of the IPs. The Company's commitment to enhance its training material and provide its employees with additional, detailed AML/CFT training within subsequent months was positively acknowledged.

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

The Committee commends the Company on the significant improvements undertaken and implemented over the past 18 months, through a self-imposed remediation exercise. This includes the enhancements made by the Company to its BRA and CRA methodologies, customer profiling processes, and transaction monitoring framework. The Committee observed the unwavering commitment from the Company's top management and at the Group level. All the improvements carried out by the Company and those which are in process of implementation are considered positive; however, the Committee could not ignore that the Company had past failures as identified during the compliance review of 2023, some of which were deemed to be serious and systematic, thereby requiring the imposition of an administrative penalty. Specifically, the Committee expressed greater concerns pertaining to the Company's past failure to undertake an adequate assessment of the ML/FT risks emanating from its business and its customers, its inability to establish an adequate customer profile, in inadequately monitoring and scrutinising the activity of the majority of the files reviewed, and in failing to report to the FIAU suspicion of ML/FT in one of its customers. All such past administrative breaches could have potentially led to the unintentional facilitation of ML/FT. As part of reaching

its final decision, the Committee considered the nature, size, and operations of the Company. Further to this, the Committee also factored in the level of cooperation exhibited by the Company throughout the entire process, highlighting that the Company and its officials were cooperative, both during the compliance review with the supervisory officials, as well as during the in-person meetings with the Committee members, where additional clarifications were provided as needed. Lastly, the Committee ensured that the administrative penalty imposed for the breaches identified during the 2023 compliance review is effective, dissuasive, and proportionate to the failures identified and the ML/FT risk exposure that was not effectively mitigated.

When taking all the above factors into consideration, the Committee decided to impose an administrative penalty of one million fifty-four thousand two hundred sixty-nine euro (€1,054,269) in relation to the following breaches:

- Regulations 5(1) and 5(4) of the PMLFTR, Sections 3.2, 3.3 and 8.1 of the IPs – Part I, and Section 2.1 of the IPs – Part II for the VFAs Sector
- Regulation 5(5)(a)(ii) of the PMLFTR and Sections 3.4 and 3.5 of the IPs – Part I
- Regulation 7(1)(c) of the PMLFTR and Sections 3.4 and 4.4.2 of the IPs – Part I
- Regulations 7(1)(d), 7(2)(a), 7(2)(b), 11(1)(b) and 11(9) of the PMLFTR, Sections 4.5.1, 4.5.2, 4.5.3 and 4.9 of the IPs – Part I, and Section 2.2.1 of the IPs – Part II for the VFAs Sector
- Regulation 15(3) of the PMLFTR and Section 5.5 of the IPs – Part I

The Committee also served the Company with a Follow-Up Directive (the 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 IPs issued thereunder, as well as to monitor the progress being achieved by the Company through the self-remediation project it has embarked upon. The Company's approach to take remedial action out of its own volition is synonymous to a sustainable compliance culture and the Follow-Up Directive is intended to give additional impetus to its actions in this regard. The Directive is also intended to ensure that the Company remedies all the AML/CFT breaches relayed throughout this document. By virtue of this Directive, the Company is expected to make available an Action Plan, which shall include:

- The Company's latest BRA, as approved by the Board of Directors.
- The enhancements undertaken by the Company to cater for the breaches identified in relation to its CRA Methodology, both for natural persons and legal entities.
- The information and supporting documentation currently being collected by the Company at onboarding and subsequently during the course of the business relationship to formulate business and risk profiles for its customers.
- The Company's existing transaction monitoring framework, including the systems utilised for both on-chain and off-chain transaction monitoring, the alerts handling process, the methodology adopted in relation to the fine-tuning of detection rules, as well as the quality control procedures in place.
- The ongoing monitoring processes employed to ensure that client-related information, data and documents are reviewed and updated on a regular basis through periodic reviews and in response to certain trigger events.
- The EDD measures currently applied by the Company, including the various points in the business relationship when EDD requests are made. Furthermore, an explanation of the trigger events for refreshing the initial EDD information and documentation.
- The remediation undertaken to ensure that AML/CFT training provided by the Company to its staff is in line with Section 7.3 of the IPs – Part I.

The Follow-Up action shall also include the carrying out of a number of meetings to discuss the implementation of the above-mentioned action items, as well as the sampling of a number of customer relationships and the review of new measures/systems implemented by the Company.

Finally, the Committee stipulates that in the eventuality that the Company fails to make the above-mentioned 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 the applicable law. It shall become final upon the lapse of the appeal period or upon final determination by the Court.

Key take-aways

- When assessing the ML/FT risks emanating from their product offerings both within the context of the BRA and CRA, VASPs are not expected to include an assessment on each and every coin being offered, instead they are required to categorise such offerings and assess the ML/FT risks of specific categories of coins/product related features. This includes assessing:
    - The potential use of mixers/tumblers – such exposure increases the likelihood of obscuring transaction origins, making tracing more challenging, thereby heightening ML/FT risk.
    - Privacy coins - such tokens are designed for enhanced anonymity and accordingly pose a heightened risk of ML/FT.
    - Use of tokens on decentralized exchanges increase the risk of ML/FT due to lack of centralised controls and KYC/AML procedures.
    - Stablecoins (e.g. tokens pegged to a fiat currency) – these can be used to facilitate large-scale fund transfers, making them attractive for laundering large sums of money.

- When establishing the business and risk profile of a customer at the onset of the business relationship, it may be reasonable to start by collecting basic information regarding this client's business/occupation/employment, SOW, SOF, and anticipated level of activity, this since such information is usually sufficient to provide an initial understanding of the customer during onboarding. However, it is essential that the said information is then enhanced and expanded upon as the business relationship progresses and the client continues to engage in more and more activity, or otherwise when the client is identified as presenting a higher level of risk at any point in the relationship. Thus, in these circumstances, there is a greater need for more granular details to truly understand the customer's evolving profile. By way of example, in the case of an actively trading customer or one who executed a particularly substantial one-off transaction, simply selecting "*education*" as an occupation does not provide sufficient clarity on the type of activity to expect, as the client could either be in a top management position within an educational institution or a lower-level administrative staff member, and these distinctions have a considerable impact on the expected transactional activity and deposits.

- Building on the point above, at times, the necessity for increased granularity in information may sometimes become apparent from the very first deposit, especially if this deposit is of a significant value or portrays immediate divergence from the anticipated activity. Furthermore, there may be situations where supporting documentation is required in order to substantiate the information submitted by the customer and ensure that the transactions being executed are justified by the client's SOW/SOF.

- Proper scrutiny of transactions necessitates vigilant monitoring to identify those transactions that deviate from the customer's established profile, as well as those transactions that, *prima facie*, appear to be unusual or suspicious, or lack a clear business or economic rationale. Subject persons must ensure that they have an effective transaction monitoring framework in place, capable of promptly detecting behaviours such as substantial transactional activity within a short period of time, recurring or one-off large individual transaction amounts, and sudden spikes in deposits. On a risk sensitive basis, the transactions being processed may need to be further corroborated through the collection of relevant information and supporting documentation, this to ascertain their legitimacy.

- In the specific context of the virtual financial assets space, one potentially concerning transactional pattern involves deposits made in fiat currency or cryptocurrency, which are then exchanged into other currencies and rapidly withdrawn within a short timeframe, sometimes within days, but in some cases, even within hours or minutes. Although this pattern may be a legitimate trading strategy, it should still warrant further investigation to understand the underlying reason for the transactions. Ultimately, subject persons have the responsibility to ensure that their services are not exploited for illicit purposes by bad actors.

- When a customer is escalated for review, it is of utmost importance that such a review entails a proper deep dive into the client's activity and funding sources, taking into consideration all available information and documentation in a holistic manner. Hence, customer file reviews should not be a mere procedural formality or a checkbox exercise, but rather, they should aim to gain a comprehensive understanding of the customer's profile and behaviour. Additionally, when documentary evidence is acquired, it must be adequately scrutinised as well as assessed for relevance and consistency.

- Transaction monitoring alerts generated need to be reviewed and investigated thoroughly, with follow-up actions taken as necessary, including escalation through an internal report when deemed appropriate. Consequently, any discounting of alerts should be based on a sufficient and well-founded rationale, which is duly documented.

- As part of their ongoing monitoring efforts, subject persons are obligated to ensure that they have the resources needed to keep client-related information, data, and documents up-to-date. It is, however, pertinent to clarify that, as per Section 4.5.3 of the IPs – Part I, there is no prescribed information monitoring method, with suggested methods including periodic reviews, updating prompted by trigger events, or a combination of both. With respect to periodic reviews, the regulations do not specify the required frequency for such reviews – what is important is that reviews occur with sufficient regularity to ascertain the timely updating of information, data, and documents.

3 April 2025