FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

DECISION NOTICE

Zeux Limited

3 January 2024

ACTION

1. By an application dated 24 June 2022 ("the Application"), Zeux Limited ("Zeux") applied under Regulation 57 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "MLRs") for registration as a cryptoasset business to perform the following activities in the UK:

    a. The exchange of fiat currency for cryptoassets.

    b. The exchange of one cryptoasset for another.

2. For the reasons listed below, the Authority has decided to refuse the Application.

SUMMARY OF REASONS

3. By its Warning Notice issued on 16 November 2023 the Authority gave notice that it proposed to refuse the Application and that Zeux Limited was entitled to make representations about that proposed action by a deadline of 14 December 2023. As of the date of this Decision Notice the Authority had not received any representations in response to the Warning Notice.

DEFINITIONS

4. The following definitions are used in this Notice:

"the AML Policy" means Zeux's Anti Money Laundering Policy dated May 2022;

"the Application" means Zeux's application dated 24 June 2022 referred to in paragraph 1 above;

"the Authority" or "FCA" means the Financial Conduct Authority;

"BWRA" mean Business-wide Risk Assessment;

"CDD" means Customer Due Diligence;

"CRA" means Customer Risk Assessment;

"DAML" means Defence Against Money Laundering;

"EDD" means Enhanced Due Diligence;

"Executive Decision Maker" means the member of the Authority's staff acting under executive procedures as described in Chapter 4 of the Decision Procedure and Penalties Manual ("DEPP") in the Authority's Handbook;

"KYC" means Know Your Customer;

"JMLSG" means Joint Money Laundering Steering Group;

"MLRs" means the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017;

"Nominated Officer" means the Nominated Officer under Regulation 21(3);

"NRA" means National Risk Assessment;

"PEPs" means Politically Exposed Persons;

"POCA" means Proceeds of Crime Act 2002;

"SARs" means Suspicious Activity Reports as required under sections 337(1) and 338(4) of POCA and section 21B the Terrorism Act;

"Regulation" means a regulation under the MLRs unless stated otherwise;

"the Relevant Obligations" means the obligations under the MLRs 2017, Part 3 of the Terrorism Act 2000, or Parts 7 and 8 of POCA;

"the Risk Overview" means Zeux's "Risk Management Overview";

"the Risk Register" means Zeux's "Financial Crime and AML Risk Register June 2022". This document is the primary basis for the BWRA;

"TM" means Transaction Monitoring;

"the Tribunal" means the Upper Tribunal (Tax & Chancery Chamber), and

"Zeux" or "the Firm" means Zeux Limited.

FACTS AND MATTERS

5. On 10 January 2020, the Authority became the anti-money laundering and counter terrorist financing supervisor for businesses carrying out certain cryptoasset activities under the MLRs. Since that date, existing cryptoasset businesses (operating before 10 January 2020) carrying on cryptoasset activity in the UK had to comply with the requirements set out in the MLRs and needed to register with the Authority.

6. Zeux applied to the Authority for registration under the MLRs on 24 June 2022. It operates a crypto exchange. The director of Zeux is Mr Jiayi ZHOU; he is also the proposed senior manager responsible for compliance with the MLRs under Regulation 21(1)(a). Mr "A" is the proposed Nominated Officer under Regulation 21(3) of the MLRs.

Failings in Zeux's Business-wide Risk Assessment ("BWRA")

7. Regulation 18 of the MLRs requires a relevant person to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject. The BWRA must consider the size, complexity, and nature of the business.

The size, complexity, and nature of Zeux's business

8. Zeux provides a mobile-device platform for use on android or iOS devices that allows users to manage their finances, make and receive payments and to make it easier to invest in a range investment products. The platform is available to download from the Apple App Store and its website.

9. Zeux is authorised and regulated by the FCA for the following activities: Arranging deals in investments; making arrangements with a view to transactions in investments; agreeing to carry on a regulated activity; account information services and; payment initiation services. Zeux plans to offer a cryptocurrency service whereby customers can purchase or sell cryptocurrency directly with Zeux.

10. Its target customers will be wealthy middle-class individuals but those who are not sufficiently wealthy to qualify for the services provided by private banks, as well as small and medium sized enterprises. Zeux expects these customers to be based in the United Kingdom and in Europe. Its marketing plan uses social media to target members of the Chinese expatriate and student community in the United Kingdom.

11. At the time of the Application, Zeux had approximately 500 active customers and expected to grow to 1000 customers within 12 months, rising to 1650 active customers by the end of Year Three.

12. Zeux estimates that in "Year One" it would have 12 staff and a revenue of £0.5million; in "Year Two" it would have 18 staff and a revenue of £1 million and; "Year Three" it would have 24 staff and a revenue of £1.7 million.

13. Zeux's BWRA is primarily set out in the "Risk Register".

14. On assessment of the BWRA, the Authority found several key concerns that evidence Zeux's failure to comply with Regulation 18 of the MLRs. These are described immediately below.

Failure to note all the risk factors

15. There was a failure to note all the risk factors that are outlined in Regulation 18 of the MLRs.

16. Limited consideration was given to the Firm's inherent risks under the customer's risk factor throughout in the "Risk Register". The Firm should have assessed all the risks posed by their potential customers (retail and corporate) for example the risk that a retail client is subject to international sanctions or corporate customers utilising bearer shares etc. Understanding their customer risk would ultimately enable them to ensure they have the appropriate controls in place to help mitigate or manage their risks.

17. No consideration was given to the risks posed by the products or services offered by the Firm. Products and services would include, for example, the exchange of fiat currency for cryptoassets (and vice versa), and the swap of cryptoassets to cryptoassets. An example of an associated inherent risk would be cryptoassets being used to transfer or disguise funds obtained from criminal activities.

18. Only high-risk jurisdiction nationals were mentioned when considering the countries or geographic areas in which the Firm operates. The Firm should have assessed all geographical risk posed, for example a customer's funds are derived from personal or business links to jurisdictions associated with higher money-laundering or terrorist financing risks.

19. The inherent risks for transactions are inaccurate and incomplete throughout the "Risk Register". This part of the risk assessment should identify the types of transactional risks the Firm could face e.g., risks around using blockchains and their decentralized and distributed nature which can facilitate a greater degree of wallet anonymity.

20. The "delivery channels" risk factor, i.e., the methods of how they will engage with their customer is not factored within the BWRA.

Failings in BWRA methodology

21. There is no evidence of a BWRA methodology that complies with the requirements of Regulation 18 of the MLRs. The assessment only provides a guidance matrix showing how the scorings have been developed, i.e., Impact x probability. Whereas the methodology should list out all the steps taken by the Firm in order to deliver the BWRA (e.g., sources used, how to test the effectiveness of controls and how a residual risk is calculated).

Failure to understanding how to perform a BWRA

22. There is no evidence of control effectiveness testing in place to help derive the overall residual risk rating.

23. The BWRA shows a table that notes a score for probability and a score for impact which result in a "residual risk" (the impact of an inherent risk multiplied by the probability). However, this is incorrect, as the calculation Zeux has performed is to calculate an inherent risk score **not** a residual risk score. Thus, there is no evidence of residual risks being calculated.

24. The inherent risks are clustered and not easy to follow throughout the "Risk Register". The Authority would expect a clear linear mapping of inherent risks, the applicable controls and the residual risk rating.

25. It appears that a lot of information has been lifted straight from the "AML Policy" without appropriate application to business scenarios.

Failure to understand, identify, differentiate and document risks

26. There is a failure to understand, identify, differentiate and document risks. For example, "Transaction Monitoring" is considered an inherent risk. There is a detailed description of the Firm's TM processes but the nature of the risk is described as *"a lack of a robust TM…."*; in fact, this is a control failing, not an inherent risk.

27. "EDD Requests" are noted in the BWRA as an inherent risk; in fact, this is a control not an inherent risk.

28. The inherent risks appear to be articulating what the policy does, as opposed to acting as a starting point for the Firm's AML framework, i.e., a BWRA typically will come first and identify all the risks, and the policy and all that is within it are designed to help mitigate these risks.

29. The BWRA notes PEPs as an inherent risk and categorises them as either high, medium or low risk explaining the different types and generic risks PEPs pose. However, the firm would not be able to assess the level of risk a PEP poses until they have undergone due diligence, which is a control. Furthermore, this type of narrative on PEPs in not what is expected in a BWRA.

The BWRA should list the risks posed by PEPs to the Firm – such as the risk of the Firm handling the proceeds of corruption, and the likelihood and impact of that based on the Firm's business model and target customers.

30. The inherent risk "SAR" is not a risk, it just describes SARs and the need to report. Again, this would be a control.

Failure to consider the National Risk Assessment ("NRA")

31. There is no evidence that the BWRA gives any, or any adequate, consideration to the NRA. Regulation 18(2)(a) of the MLRs states that a relevant person must consider:

> "Information made available to them by the supervisory authority under Regulations 17(9) and 47".

32. This references the NRA which has a specific section on cryptoassets. One of the risks it highlights as a medium risk is cryptoassets being used to finance terrorist activity (8.18 of the NRA). This risk should be included as a specific risk in the BWRA. Additionally, under "jurisdiction risk" the NRA identifies uneven regulatory requirements (or regulatory arbitrage) as a vulnerability. This is not mentioned in the Firm's BWRA, albeit these are listed under CDD and TM in the AML Policy.

33. The Authority considers that the Firm has not complied with Regulation 18 of the MLRs. The Firm has demonstrated a lack of understanding on how to complete a BWRA and that it has insufficient controls in place to identify, assess, mitigate and prevent the risks of money laundering and terrorist financing.

<u>Customer Risk Assessment ("CRA") failings</u>

34. Regulations 28, 33 and 35 of the MLRs encompass the requirements of a CRA. A CRA is an evaluation made when a new business relationship or transaction is to be initiated with a customer. It is a critical process by which the firm explores the potential risks that a new business relationship may create. Depending on the risk posed by a new business relationship, the firm will use this customer risk rating to drive the appropriate level of due diligence and ongoing monitoring to ensure the customer's risk is being managed, monitored, and mitigated.

The key risk factors that should be considered as part of this exercise are:

a. Customer risk.

b. Jurisdiction risk.

c. Product/Services risk.

d. Transaction risk.

e. Delivery channel risk.

35. Section 17 of the AML Policy sets out the Firm's CRA.

36. This section highlights three customer risk ratings: High, Medium and Low.

37. Various scenarios/examples of customer attributes are noted below each risk rating in bullet point format. For example, if customers deposit less than £10,000, they would be classified as low risk (amongst other contributing factors). However, this is not assessing the customer in its entirety/holistically. There is no evidence of an actual assessment. Instead, there are scenarios under each risk category. The Authority would expect the Firm to have a specific tool and methodology that assesses a customer against all attributing risk factors noted in the MLRs and JMLSG (e.g., industry and geography). The tool or methodology should have appropriate scoring and weighting to derive the overall score or risk rating for a customer in order to understand the level of due diligence and monitoring required.

38. No evidence of a customer risk rating methodology.

39. There is a lack of risk lists to accompany the customer risk assessment. For example, product risk would usually be accompanied by a list of all products and their associated assessment of risk.

40. It is the view of the Authority that the CRA is inadequate as there is an inaccurate/incomplete tool with no accompanying methodology. Therefore, the Firm cannot appropriately identify and

manage/mitigate the risks of money laundering, terrorist financing and sanctions evasion that a customer may pose. The Authority considers, on reasonable grounds, that the Firm will breach the requirements in Regulation 28, 33 and 35 of the MLRs and the JMLSG Chapter 4.

Enhanced Due Diligence ("EDD") failings

41. Regulation 33(1)(f) of the MLRs requires a firm to apply EDD measures and ongoing monitoring to manage and mitigate the risks arising in any case where:

> "A transaction is complex and unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic legal purpose, …".

42. In cases where Regulation 33(1)(f) of the MLRs applies, Regulation 33(4) of the MLRs states that a firm must:

> "As far as possible, examine the background and purpose of the transaction, and increase the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or relationship appears to be suspicious."

43. Section 18 of the AML Policy sets out Zeux's EDD procedures for its customers and notes several measures to be taken where a customer is required to undergo EDD. One such measure is:

> "Requesting further information from the customer for reasons for source of funds and source of wealth if required. All deposits that are over £10,000 or equivalent require source of funds. Larger value transactions or total deposits require source of funds and source of wealth."

44. However, Regulation 33(5) of the MLRs and JMLSG 4.62(b) state that, where EDD applies, both Source of Funds and Source of Wealth must be identified, regardless of the amount deposited, i.e., if a person are deemed to be high risk, their Source of Funds and Source of Wealth must be identified.

45. With respect to "Red flags", section 21 of the AML Policy, gives 8 examples of potential red flags involving customer behaviours and activities that would require an employee to notify the Nominated Officer immediately to facilitate further investigation.

46. Whilst the examples given are appropriate, the section fails to include one important scenario, namely, omitting where a customer is established (or where a party to a transaction is established) in a high-risk third country, as specified in Schedule 3ZA of the MLRs. As a result, the Authority considers that section 21 of the AML Policy is inadequate.

47. The Authority is concerned that the Firm's EDD measures fail to demonstrate an awareness of all EDD triggers and fail to capture all requirements under the Regulations, specifically Regulations 33(4) and 33(5) of the MLRs.

Suspicious activity reports ("SARS")

48. Regulations 19(4) and 21(5) of the MLRs require a firm to establish and maintain policies, controls and procedures to mitigate effectively the risks of money laundering and terrorist financing identified in any risk assessment undertaken by the firm. This includes where a disclosure is made to the Nominated Officer, that officer must consider it in the light of any relevant information which is available to the relevant person and determine:

> "Whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing and creation of a SAR".

49. Part One of the JSMLG Guidance sets out that:

> 6.33 The Firm's nominated officer must report to the NCA any transaction or activity that, after their evaluation, they know or suspect, or has reasonable grounds to know or suspect, may be linked to money laundering or terrorist financing, or to attempted money laundering or terrorist financing. Such reports must be made as soon as is reasonably practicable after the information comes to them.

50. The purpose of the SAR is to alert law enforcement (the NCA) that certain customer activity is in some way suspicious and might indicate money laundering or terrorist financing.

51. The primary test whether a report needs to be made to the NCA is whether the Nominated Officer 'knows' or 'suspects' or has reasonable grounds for 'knowing' or 'suspecting' that a customer is engaged in money laundering. Failure to disclose would be a breach of Section 331 of POCA.

52. Section 29 of the AML Policy sets out the Firm's SAR procedures, the relevant part of which states that:

> "Where there is serious suspicion, evidence or reasonable grounds for suspecting, that a transaction may be deemed suspicious, employees are required to report their suspicions **in accordance with the Firm's procedures on Suspicious Transaction Reporting**.
>
> "The Nominated Officer will receive any reports or concerns relating to any suspected or actual money laundering and will record, investigate, and report this to the relevant authorities, …" [Emphasis added]. …"

53. The Firm refers to "Suspicious Transaction Reporting", a term relating to a report made to the FCA. A "Suspicious Activity Report" or SAR is the required vehicle for reports made to the NCA.

54. Despite the reference above to the Firm's "procedures on Suspicious Transaction Reporting", no such procedures were submitted with the Application.

55. Accordingly, the Authority considers that the AML Policy fails to adequately set out the process by which an employee would report their suspicions to the Nominated Officer, specifically the method of by which they would report such concerns (whether by email or orally) or any prescribed information required when doing so. Nor does the AML Policy set out the procedure by which a SAR is reported by the Nominated Officer to the relevant authorities.

56. The Authority is also concerned that there is no mention of a DAML. A DAML can be requested from the NCA where a reporter has a suspicion that property, they intend to deal with is in some way criminal, and that by dealing with it they risk committing one of the principal money

laundering offences under POCA. The Authority would expect the Firm to reference DAML and explain that a person does not commit one of those offences if they have received "appropriate consent" (aka, a DAML) from the NCA. The NCA is empowered to provide these criminal defences in law under s335 of POCA.

57. The SAR guidance is too high-level and lacks detail as to what the Firm would consider raising with the NCA. The SAR guidance does not set out the internal procedures for dealing with a SAR in any detail. It does not detail what record keeping is in place around decision making in relation to SARs (Regulation 19(4)(d) of the MLRs and Section 330(5) of POCA.

58. A Warning Notice was issued to the firm on 14 November 2023 by the Authority and given 28 days to make representations to its contents. As of 18 December 2023, the Authority has received no response.

Conclusion

59. On the basis of the facts and matters described above, the Authority suspects, on reasonable grounds, that Zeux will fail to comply with its obligations under the MLRs.

60. Therefore, the Authority has decided to refuse the Application in accordance with Regulation 59(1) of the MLRs.

PROCEDURAL MATTERS

Decision maker

61. The decision which gave rise to the obligation to give this Decision Notice was made by the Executive Decision Maker.

62. This Decision Notice is given under Regulation 59(4)(b) of the MLRs. The following statutory rights are important.

The Tribunal

63. Zeux Limited has the right to refer the matter to which this Decision Notice relates to the Upper Tribunal. Under paragraph 2(2) of Schedule 3 to the Tribunal Procedure (Upper Tribunal) Rules

2008, Zeux Limited has 28 days from the date on which this Decision Notice is given to Zeux Limited to refer the matter to the Tribunal.

64. A reference to the Upper Tribunal is made by way of a signed reference notice (FormFTC3) filed with a copy of this Decision Notice. The Tribunal's contact details are:

The Upper Tribunal, Tax and Chancery Chamber
Fifth Floor
Rolls Building
Fetter Lane
London
EC4A 1NL
(tel: 020 7612 9730; email: uttc@hmcts.gsi.gov.uk).

65. For further information on the Tribunal, Zeux Limited should refer to the HM Courts and Tribunal Service website. Guidance on making a reference to the Tribunal and the relevant form to complete (Form FTC3) can be accessed from the following link: https://www.gov.uk/government/collections/upper-tribunal-tax-and-chancery-chamber

66. A copy of Form FTC3 must also be sent to Peter Jones, Manager, Digital Assets Team at the Financial Conduct Authority, 12 Endeavour Square, London E20 1JN at the same time as filing a reference with the Upper Tribunal.

67. Once any referral is determined by the Upper Tribunal and subject to that determination, or if the matter has not been referred to the Upper Tribunal, the Authority will issue a final notice about the implementation of that decision.

Access to evidence

68. The person to whom this Notice is given has the right to access the material upon which the Authority has relied in deciding to give this Notice.

Confidentiality and publicity

69. Zeux Limited should note that this Decision Notice may contain confidential information and, unless it has been published by the Authority, should not be disclosed to a third party (except for the purpose of obtaining advice on its contents). Zeux Limited should also note that, under regulation 84 of the MLRs, a person whom a Decision Notice is given or copied may not publish

the Notice or any details concerning it unless the Authority has published the Notice or those details. This notice may contain confidential information and should not be disclosed to a third party (except for the purpose of obtaining advice on its contents).

70. Zeux Limited should also note, however, that the Authority must, under regulation 84 of the MLRs, publish such information about the matter to which a Decision Notice or Final Notice relates as it considers appropriate. A Decision Notice or Final Notice may contain reference to the facts and matters contained in this Notice.

Authority contacts

71. For more information concerning this matter generally, contact Peter Jones, Manager, Digital Assets Team, Authorisations at the Authority (direct line: 020 70665472 / email: Peter.Jones@fca.org.uk).

Val Smith
Executive Decision Maker

ANNEX A – REGULATORY PROVISIONS RELEVANT TO THIS DECISION NOTICE

Relevant Statutory Provisions

The MLRs 2017

Requirement for cryptoasset firms to be registered

1. The requirement for cryptoasset exchange providers (as defined by Regulation 14A of the MLRs 2017), acting in the course of business carried on by them in the United Kingdom, to be registered, is set out in Regulation 8 and Regulation 9 of the MLRs 2017.

Risk assessments and controls

2. Chapter 2 of Part 1 of the MLRs 2017 sets out the requirements regarding risk assessments and controls (Regulations 16 – 25).

3. Regulation 18(1) (Risk assessment by relevant persons) states that: "A relevant person must take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject."

4. Regulation 18(2) sets out the factors which a relevant person must take into account when carrying out the risk assessment required under Regulation 18(1), which are:

    (a) information made available to them by the supervisory authority under regulations 17(9) and 47, and

    (b) risk factors including factors relating to—

        (i) its customers;

        (ii) the countries or geographic areas in which it operates;

        (iii) its products or services;

        (iv) its transactions; and

        (v) its delivery channels.

5. Regulation 18(3) states that in deciding what steps are appropriate under Regulation 18(1) the relevant person: "must take into account the size and nature of its business".

6. Regulation 18(4) states that a relevant person must keep an up-to-date record in writing of all the steps it has taken under paragraph (1) […].

7. Regulation 19(1) (Policies, controls and procedures) states that a relevant person must— (a) establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any risk assessment undertaken by the relevant person under regulation 18(1); […]

8. Regulation 19(2) states that the policies, controls and procedures adopted by a relevant person under paragraph (1) must be— (a) proportionate with regard to the size and nature of the relevant person's business, and (b) approved by its senior management.

9. Regulation 19(4) states that the policies, controls and procedures referred to in paragraph (1) must include policies, controls and procedures— […] (d) under which anyone in the relevant person's organisation who knows or suspects (or has reasonable grounds for knowing or suspecting) that a person is engaged in money laundering or terrorist financing as a result of information received in the course of the business or otherwise through carrying on that business is required to comply with— (i) Part 3 of the Terrorism Act 2000(1); or (ii) Part 7 of the Proceeds of Crime Act 2002 ("POCA") [see provisions relating to the making of an authorised disclosure under section 338 of POCA]; […].

10. Regulation 19(5) states that in determining what is appropriate or proportionate with regard to the size and nature of its business, a relevant person may take into account any guidance which has been— (a) issued by the FCA; or (b) issued by any other supervisory authority or appropriate body and approved by the Treasury.

11. Regulation 21(5) states that where a disclosure is made to the nominated officer, that officer must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

12. Regulation 24(1) (Training) states that a relevant person must:

    (a) take appropriate measures to ensure that its relevant employees […] are—

(i) made aware of the law relating to money laundering, terrorist financing and proliferation financing, and to the requirements of data protection, which are relevant to the implementation of these Regulations; and

(ii) regularly given training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering, terrorist financing or proliferation financing;

(b) maintain a record in writing of the measures taken under sub-paragraph (a), and in particular, of the training given to its relevant employees […].

(i) identification or mitigation of the risk of [F5money laundering, terrorist financing and proliferation financing] to which the relevant person's business is subject; or

(ii) prevention or detection of money laundering, terrorist financing and proliferation financing in relation to the relevant person's business.

13. Regulation 24(3) states that:

> "In determining what measures are appropriate under paragraph (1), a relevant person— (a) must take account of— (i) the nature of its business; (ii) its size; (iii) the nature and extent of the risks of money laundering, terrorist financing and proliferation financing to which its business is subject; and (b) may take into account any guidance which has been— (i) issued by the FCA; or (ii) issued by any other supervisory authority or appropriate body and approved by the Treasury."

Customer due diligence

14. Part 3 of the MLRs 2017 sets out the requirements regarding customer due diligence, enhanced customer due diligence and simplified customer due diligence (Regulations 27 -38).

15. Regulation 27(1)(a) (Customer due diligence) states that a relevant person must apply customer due diligence measures if the person [amongst other situations] establishes a business relationship.

16. Regulation 27(7D) states that a cryptoasset exchange provider of the kind who operates a machine which utilises automated processes to exchange cryptoassets for money, or money for cryptoassets, must also apply customer due diligence measures in relation to any such transaction carried out using that machine […].

17. Regulation 28 (Customer due diligence measures) applies when a relevant person is required by regulation 27 to apply customer due diligence measures. Regulation 28(2) states that the relevant person must (a) identify the customer, (b) verify the customer's identity and (c) assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction.

18. Regulation 28(3) states that where the customer is a body corporate—

    (a) […]

    (b) subject to paragraph (5) [which disapplies the requirement where the customer is a company which is listed on a regulated market] the relevant person must take reasonable measures to determine and verify—

        (i) the law to which the body corporate is subject, and its constitution (whether set out in its articles of association or other governing documents); […]

19. Regulation 28(4) states that subject to paragraph (5), where the customer is beneficially owned by another person, the relevant person must—

    (a) identify the beneficial owner;

    (b) take reasonable measures to verify the identity of the beneficial owner so that the relevant person is satisfied that it knows who the beneficial owner is; and

    (c) if the beneficial owner is a legal person, trust, company, foundation or similar legal arrangement take reasonable measures to understand the ownership and control structure of that legal person, trust, company, foundation or similar legal arrangement.

20. Regulation 28(11)(a) states that the relevant person must conduct ongoing monitoring of a business relationship, including scrutiny of transactions undertaken throughout the course of the

relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, the customer's business and risk profile.

21. Regulation 33(1) (Obligation to apply enhanced customer due diligence) states that a relevant person must apply enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the customer due diligence measures required under regulation 28, […], to manage and mitigate the risks arising in specified circumstances.

22. Under Regulation 33(1)(f) and (g) [the obligation to apply enhanced customer due diligence] includes any case where (i) a transaction is complex or unusually large, (ii) there is an unusual pattern of transactions, or (iii) the transaction or transactions have no apparent economic or legal purpose; and in any other case which by its nature can present a higher risk of money laundering or terrorist financing.

23. Under Regulation 33(3A) the enhanced due diligence measures taken by a relevant person, where there is a business relationship with a person established in a high-risk third country, or in relation to any relevant transaction where either of the parties to the transaction is established in a high-risk third country, must include (amongst other measures):

> "… (c) obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner; …"

24. Under Regulation 33(4) the enhanced customer due diligence measures taken by a relevant person for the purpose of paragraph (1)(f) must include—

> (a) as far as reasonably possible, examining the background and purpose of the transaction, and
>
> (b) increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appear to be suspicious.

25. Regulation 33(5) states that depending on the requirements of the case, the enhanced customer due diligence measures required under paragraph (1) may also include, among other things—

(a) seeking additional independent, reliable sources to verify information provided or made available to the relevant person;

(b) taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction;

(c) taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;

(d) increasing the monitoring of the business relationship, including greater scrutiny of transactions.

Applications for registration

26. Regulation 57 (Applications for registration in a register maintained under regulation 54 or 55) states that a person applying for registration under the MLRs 2017 must make an application in such manner as the registering authority may specify.

Fit and proper test: cryptoasset businesses

27. Under Regulation 59(1) of the MLRs 2017, the Authority may refuse to register an applicant for registration if:

a) any requirement of, or imposed under, regulation 57 has not been complied with; […]

b) the registering authority suspects, on reasonable grounds—

(i) that the applicant will fail to comply with any of its obligations under—

(aa) these Regulations;

(bb) Part 3 of the Terrorism Act 2000; or

(cc) Parts 7 and 8 of the Proceeds of Crime Act 2002;

(the "relevant obligations");

(ii) that any person whom the applicant has identified as one of its officers or managers will fail to comply with any of the relevant obligations.

28. Regulation 59 of the MLRs 2017 states:-

59.— Determination of applications for registration under regulations 54 and 55

(1) Subject to regulation 58 and regulation 58A, the registering authority may refuse to register an applicant for registration in a register maintained under regulation 54 or 55 if—

(a) any requirement of, or imposed under, regulation 57 has not been complied with;

(b) it appears to the registering authority that any information provided pursuant to regulation 57 is false or misleading in a material particular;

(c) the applicant has failed to pay—

(i) a penalty imposed by the authority under Part 9;

(ii) a charge imposed by the authority under Part 11; or

(iii) a penalty or charge imposed by the authority under regulation 35(1) or 42(1)

of the Money Laundering Regulations 2007;

(d) where the registering authority is not the applicant's supervisory authority, the

supervisory authority opposes the application for registration on reasonable grounds; or

(e) the registering authority suspects, on reasonable grounds—

(i) that the applicant will fail to comply with any of its obligations under—

(aa) these Regulations;

(bb) Part 3 of the Terrorism Act 2000; or

(cc) Parts 7 and 8 of the Proceeds of Crime Act 2002;

(the "relevant obligations");

(ii) that any person whom the applicant has identified as one of its officers or managers will fail to comply with any of the relevant obligations.

(2) Where the Commissioners are the registering authority, they must within 45 days beginning either with the date on which they receive the application or, where applicable, with the date on which they receive any further information required under regulation 57(3), give the applicant notice of—

(a) the decision to register the applicant; or

(b) the following matters—

(i) their decision not to register the applicant;

(ii) the reasons for their decision;

(iii) the right to a review under regulation 94; and

(iv) the right to appeal under regulation 99.

(3) Where the FCA is the registering authority, it must within the period specified in paragraph (3A) beginning either with the date on which it receives the application or, where applicable, with the date on which it receives any further information required under regulation 57(3), give the applicant notice of—

(a) its decision to register the applicant; or

(b) the following matters—

(i) that it is minded not to register the applicant;

(ii) the reasons for being minded to refuse to register the applicant; and

(iii) the right to make representations to it within a specified period (which may not be less than 28 days).

(3A) The period specified in this paragraph is—

(i) where the applicant is a cryptoasset exchange provider or custodian wallet provider, 3 months, or

(ii) in any other case, 45 days,

beginning either with the date on which it receives the application or, where applicable, with the date on which it receives any further information required under regulation 57(3).

(4) After the expiry of the period referred to in paragraph (3)(b)(iii), the FCA must decide, within a reasonable period, whether to register the applicant and it must give the applicant notice of—

(a) its decision to register the applicant; or

(b) the following matters—

(i) its decision not to register the applicant;

(ii) the reasons for its decision; and

(iii) the right to appeal under regulation 93.

(5) The registering authority must, as soon as practicable after deciding to register a person, include that person in the relevant register.

29. Regulation 84 of the MLRs 2017 states:

(1) Where a warning notice is given by the FCA under regulation 81(2), neither the FCA nor any person to whom it is given or copied may publish the notice or any details concerning it.

(2) Where the FCA gives a decision notice under regulation 81(6), the FCA must publish on their official website such information about the matter to which the notice relates as it considers appropriate, subject to paragraphs (3) to (9).

(3) Where the FCA publishes information under paragraph (2) or (4) about a matter to which a decision notice relates and the person to whom the notice is given refers the matter to the Upper

Tribunal (see regulation 93), the FCA must, without undue delay, publish on its official website information about the status of the appeal and its outcome.

(4) Subject to paragraph (5), (6) and (9) where the FCA gives a final notice, it must, without undue delay, publish on its official website information on the type and nature of the breach and the identity of the person on whom the sanction or measure is imposed.

(5) Subject to paragraph (8) and (9), information about a matter to which a final notice relates must be published in accordance with paragraph (6) where—

(a) the FCA considers it to be disproportionate to publish the identity of a legal person on whom the sanction or measure is imposed following an assessment by the FCA of the proportionality of publishing the person's identity;

(b) the FCA considers it to be disproportionate to publish the personal data of the individual on whom the sanction or measure is imposed following an assessment by the FCA of the proportionality of publishing the personal data; or

(c) the publication of information under paragraph (4) would jeopardise the stability of the financial markets or an ongoing investigation.

(6) Where paragraph (5) applies, the FCA must—

(a) defer the publication of the information about a matter to which a final notice relates until such time as paragraph (5) ceases to apply; or

(b) publish the information on an anonymous basis if publication on that basis would ensure the effective protection of any anonymised personal data in the information.

(7) Where paragraph (6)(b) applies, the FCA may make such arrangements as to the publication of information (including as to the timing of publication) as are necessary to preserve the anonymity of the person on whom the sanction or measure is imposed.

(8) The FCA may make arrangements for the postponed publication of personal data that is anonymised in information it publishes under paragraph (6)(b) if—

(a) the publication of the data is postponed for a reasonable period of time; and

(b) the FCA considers that paragraphs (5)(b) and (6)(b) will no longer apply in respect of that data at the time of the postponed publication.

(9) Information about a matter to which a final notice relates must not be published if publication in accordance with paragraph under paragraph (6) is considered by the FCA insufficient to ensure—

(a) that the stability of the financial markets would not be put in jeopardy; or

(b) that the publication of the information would be proportionate with regard to sanctions or measures which are considered by the FCA to be of a minor nature.

(10) Where the FCA publishes information in accordance with paragraphs (2) to (8), the FCA must ensure that the information remains on its official website for at least five years, unless the information is personal data and the data protection legislation requires the information to be retained for a different period.

(11) For the purposes of this regulation, "personal data" has the same meaning as in Parts 5 to 7 of the Data Protection Act 2018 (see section 3(2) and (14) of that Act).

30. Section 330 of POCA states: Failure to disclose: regulated sector

(1) A person commits an offence if the conditions in subsections (2) to (4) are satisfied.

(2) The first condition is that he—

(a) knows or suspects, or

(b) has reasonable grounds for knowing or suspecting,

that another person is engaged in money laundering.

(3) The second condition is that the information or other matter—

(a) on which his knowledge or suspicion is based, or

(b) which gives reasonable grounds for such knowledge or suspicion,

came to him in the course of a business in the regulated sector.

(3A) The third condition is—

(a) that he can identify the other person mentioned in subsection (2) or the whereabouts of any of the laundered property, or

(b) that he believes, or it is reasonable to expect him to believe, that the information or other matter mentioned in subsection (3) will or may assist in identifying that other person or the whereabouts of any of the laundered property.

(4) The fourth condition is that he does not make the required disclosure to—

(a) a nominated officer, or

(b) a person authorised for the purposes of this Part by the Director General of the National Crime Agency

as soon as is practicable after the information or other matter mentioned in subsection (3) comes to him.

(5) The required disclosure is a disclosure of—

(a) the identity of the other person mentioned in subsection (2), if he knows it,

(b) the whereabouts of the laundered property, so far as he knows it, and

(c) the information or other matter mentioned in subsection (3).

(5A) The laundered property is the property forming the subject-matter of the money laundering that he knows or suspects, or has reasonable grounds for knowing or suspecting, that other person to be engaged in.