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

FIRST SUPERVISORY NOTICE

To:	**BeAccount Ltd**
Reference Number:	**937539**
Address:	**One Canada Square Canary Wharf London E14 5AB**
Date:	**17 December 2025**

1 ACTION

1.1 For the reasons given in this First Supervisory Notice, and pursuant to regulation 11(1) of the Electronic Money Regulations 2011 (the "EMRs"), the Financial Conduct Authority (the "Authority") has decided to vary the authorisation granted to Be Account Ltd (the "Firm") pursuant to Part 2 of the EMRs by imposing the following requirements (the "Requirements") on the Firm with immediate effect.

The Requirements

Restrictions on business activities

1) The Firm must not, without the prior written consent of the Authority, carry out any electronic money services for which it is authorised by the Authority pursuant to Part 2 of the EMRs or conduct any payment services as defined under regulation 2(1) of the Payment Services Regulation 2017 ("the PSRs"). For the avoidance of doubt this includes not to onboard any new customers and to accept any new relevant funds (as defined in regulation 23 of the PSRs) ("Relevant Funds").

2) The Firm must return all Relevant Funds as soon as practicable and in any event by a date to be agreed with the Authority, except where funds are held to meet specific contractual obligations such as chargebacks.

Notification requirements

3) The Firm must by 24 December 2025 notify, in writing, all customers of the imposition and effect of these Requirements in a form to be agreed in advance with the Authority.

4) By 4pm, on 19 December 2025, the Firm must display, in a prominent place on its website [https://payine.com] and all other communication channels or contact method, e.g. mobile applications, other digital channels, etc, a notice setting out the terms and effects of these Requirements in a form to be agreed in advance with the Authority. This will include a link to the relevant website entry in the Authority's register relating to the Firm where the terms of the Requirements will appear. The font and size to also be agreed with the Authority in advance.

5) The Firm must provide written confirmation to the Authority that it is in compliance with these Requirements by 4pm, on 19 December 2025.

Retention of records

6) The Firm must secure and preserve all records and/or information (physical or electronic) relating to electronic money services from its systems in their original form, or in a copy proved to be identical to the source material. These must be retained in a form and at a location within the United Kingdom, to be notified to the Authority in writing by 4pm, on 19 December 2025, such that they can be provided to the Authority, or to a person named by the Authority, promptly on its request.

1.2 These Requirements shall take immediate effect and remain in force unless and until varied or cancelled by the Authority (either on the application of the Firm or of the Authority's own volition).

2 REASONS FOR ACTION

Summary

2.1 The Authority has concluded, on the basis of the facts and matters described below, that it is necessary to vary the Firm's authorisation by imposing the Requirements because it appears the Firm no longer meets, or it is unlikely to meet, the conditions for authorisation under regulation 6 of the EMRs and it is desirable in order to maintain trust in a payment system pursuant to regulation 11(1)(c) of the EMRs.

2.2 The Authority has identified serious concerns relating to the Firm and is not satisfied that the Firm has the operational effectiveness and adequacy required to be able to identify, manage, monitor and report the risk of its business being used to

facilitate financial crime, pursuant to regulation 6(5)(b) of the EMRs.

2.3 Specifically, the Authority has serious concerns that the Firm is not meeting its conditions for authorisation because it does not have effective procedures to identify, manage, monitor and report any risks to which it might be exposed, and which are comprehensive and proportionate to the nature, scale and complexity of electronic money to be issued and payment services to be provided by the institution.

2.4 As a "financial institution" whose permission enables it to conduct payment services and issue electronic money, the Firm is subject to the requirements of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("the MLRs"), and must comply with requirements to deter and detect financial crime, which includes money laundering and terrorist financing, pursuant to regulations 8(2)(b), 10(2)(a), 10(4) and Schedule 2 of the MLRs.

2.5 The Authority also has concerns that the Firm is unable to demonstrate that it is complying with the MLRs, specifically in relation to risk assessment (regulations 18(1) and (2)); policies, controls and procedures (regulation 19); CDD (regulation 27(1)); CDD measures (regulations 28(2), (4), (12) and (13)); and EDD: PEPs (regulation 35(1)) of the MLRs.

2.6 The Authority considers variation of the Firm's authorisation by imposition of the Requirements should take immediate effect because the matters set out in this First Supervisory Notice demonstrate that the Firm is unable to manage its affairs in a sound and prudent manner.

3 DEFINITIONS

3.1 The definitions below are used in this First Supervisory Notice:

"Act" means the Financial Services and Markets Act 2000;

"AEMI" means Electronic Money Institution;

"AML" means Anti-Money Laundering;

"Authority" means the Financial Conduct Authority;

"Bank A" means a bank with which the Firm held a safeguarding account;

"Bank B" means a bank with which the Firm currently holds a safeguarding account;

"Bank C" means the bank with which the Firm currently holds a safeguarding account;

"CDD" means Customer Due Diligence as set out in regulation 28 MLRs;

"Client Files" means the nine client files provided by the Firm to the Authority based on a customer list provided by the Firm on 12 May 2025;

"Conditions for Authorisation" means the conditions for authorisation set out in regulations 6(4) to (8) of the EMR;

"CRA" means Customer Risk Assessment;

"Customers 1 to 9" refer to the different customer files reviewed;

"DEPP" means the Authority's Decision Procedure and Penalties Manual, which is part of the Handbook;

"EDD" means Enhanced Due Diligence as set out in regulations 33 and 35 of the MLRs;

"EMR" means Electronic Money Regulations 2011;

"Firm" means BeAccount Ltd;

"Firm B" means an external compliance consultant;

"FATF" means Financial Action Taskforce;

"Handbook" means the Authority's online handbook of rules and guidance (as in force from time to time);

"JMSLG" means Joint Money Laundering Steering Group Guidance;

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

"MLRO" means Money Laundering Reporting Officer;

"Mr A" means the sole person currently with significant control of the Firm;

"PEP" means a Politically Exposed Person;

"POCA" means the Proceeds of Crime Act 2022;

"PSRs" means the Payment Services Regulation 2017;

"Relevant funds" has the meaning given to it by Regulation 20 of the EMR;

"Requirements" means the terms imposed on the Firm by this First Supervisory Notice as outlined in section 1 above;

"SARs" mean suspicious activity reports;

"SOF" means Source of Funds;

"SOW" means Source of Wealth;

"SUP" means the Supervision manual, which is part of the Handbook;

"Tribunal" means the Upper Tribunal (Tax and Chancery Chamber); and

"UBO" means the Ultimate Beneficial Owner of the Firm.

4 FACTS AND MATTERS

Background

4.1 The Firm was incorporated on 13 May 2020 and was authorised as an AEMI under the EMRs on 18 July 2021. The Firm also trades as "Payine". The Firm has four directors. The sole person currently with significant control is Mr A.

4.2 The Firm's permissions contain the following regulated activities:

(i) Services enabling cash to be placed on a payment account.
(ii) Services enabling cash withdrawals from a payment account.
(iii) Executing of payment transactions (not covered by a credit line).
(iv) Execution of payment transactions (covered by a credit line).
(v) Issuing and/or acquiring of payment instructions.
(vi) Money remittance.
(vii) Issuing electronic money.

4.3 On 20 September 2024, the Authority received a Change in Control ("CiC") application. The proposed controller firm already held a 9.99% shareholding in the Firm. The CiC application was to acquire the Firm's UBO's 90.01% stake. Mr A was the primary controller of the proposed controller firm, who held a 90.01% stake. The Authority approved the CiC application on 20 December 2024.

Failings and risks identified

4.4 On 8 April 2025, the Firm notified the Authority that its MLRO had received a letter from Bank A, which stated that Bank A had terminated its banking relationship with immediate effect and without warning. The Firm explained this meant the account was frozen and its customers could not access their funds.

4.5 On 10 April 2025, the Authority held a call with the Firm. On the call, the Firm stated that it holds safeguarding accounts with other providers (Bank B and Bank C). This mitigated the Authority's concerns that the Firm may be unable to hold 'relevant funds' in an appropriate safeguarding account which is a requirement under the EMRs.

4.6 On 23 April 2025, the Authority issued an information notice pursuant to section 165(1) of the Act, as modified by paragraph 3(a) of Schedule 3 of the EMRs, to the Firm. The Authority requested, by 30 April 2025, details of the Firm's clients, safeguarding accounts and the latest safeguarding and AML audits. The Firm acknowledged the request, and sought an extension to the deadline. The Firm also confirmed that Bank A had "unfrozen all client funds".

4.7 On 7 and 12 May 2025, the Firm provided the following documentation:

(i) Safeguarding audit, dated 27 September 2024,
(ii) Financial crime audit, dated 16 December 2024,
(iii) Client list, dated 12 May 2025,
(iv) MLRO report dated January 2025,
(v) Available liquidity dated 5 May 2025.

4.8 Having reviewed the responses, the Authority noted the following:

(i) The MLRO report dated January 2025 provided limited specific detail on the Firm and was drafted in generalised terms. The report made no recommendations for any system and control enhancements for the forthcoming year.

(ii) The external financial crime assurance review of client files by Firm B dated 16 December 2024, commented on a number of adverse triggers the Firm should have identified and scrutinised. It is unclear to the Authority if the sample of clients reviewed by Firm B should have been onboarded and if any mitigating controls were implemented to reduce the risk of financial crime.

4.9 On 28 August 2025, the Authority issued a further information notice pursuant to section 165(1) of the Act as modified by paragraph 3(a) of Schedule 3 of the EMRs to the Firm. The Authority requested that the Firm provide it with a copy of nine client files for review.

4.10 On 5 and 8 September 2025, in response to the Authority's 28 August 2025 request, the Firm provided copies of the Client Files. The Client Files were selected on the basis of the Firm's top clients by transactional volume and/or value data, whilst considering proportional representation among the risk ratings based on a list provided by the Firm on 12 May 2025. This ensured the review addressed areas of greatest risk and a split of high, medium and low risk clients so as to achieve a balanced and comprehensive evaluation of the Firm's systems and controls.

4.11 On 7 October 2025, the Authority requested that the Firm provide the additional client file transaction monitoring data, further to that which was received as part of the Client Files request. This additional request was made because the original data supplied in the original Client Files request was insufficient on its own to make a reasonable analysis.

4.12 The review of Client Files and transaction monitoring alerts was carried out against the relevant regulatory requirements, including those within the MLRs, and JMLSG, in relation to:

(i) CRA.
(ii) CDD.
(iii) PEP and sanctions screening.
(iv) EDD including SOW and SOF.
(v) Ongoing monitoring (periodic reviews).
(vi) Transaction monitoring.
(vii) Suspicious activity reporting.

4.13 Upon review, all client files were assessed as "inadequate" overall, failing to meet standards set out in the MLRs and JMLSG. The key findings of the review are set out below.

<u>CRA</u>

4.14 Regulation 28 of the MLRs requires a firm to take steps to identify the money laundering and terrorist financing risks posed by a particular customer. This includes identifying and verifying a customer's identity, beneficial owner, the purpose of the account and business relationship. In addition to the level of assets to be deposited and withdrawn and the value and volume of the transactions undertaken, a firm should undertake a CRA when establishing a business relationship with a customer and at other appropriate times for an existing customer on a risk-based approach.

4.15 All of the Client Files were rated as inadequate against this area of the assessment criteria. The CRA for each file provides no commentary on how the Firm has appropriately taken steps to assess the level of risk and rationale for onboarding.

4.16 There is also no evidence to suggest that the risk assessment carried out by the Firm aligns with its CRA methodology. For example, there is no reference in the files to sector specific vulnerabilities and no review of UBO's professional background, including historic and current ventures. The methodology requires that client forecasts are compared with industry benchmarks, and that the source of wealth and funds is supported by evidence from verified, reliable, and independent sources. There is no evidence this process is followed in practice, for example there is no evidence of open-source checks and where financial statements are provided there is no analysis provided to ensure they are reliable and independent. The CRA checklist is also applied inconsistently across client files and fails to include some of the assessment fields specified by the methodology.

4.17 Such inconsistencies may affect a customer's risk profile, which in turn influences the extent of due diligence required during onboarding and throughout ongoing monitoring. As a result, the necessary controls to reduce the risk of financial crime might not be adequately implemented.

4.18 For instance, Customer 1 should have remained high risk at its periodic review but was downgraded to low risk. The 2024 CRA checklist for this file did not contain the field about whether the client conducts business in a country assessed by the Firm as High Risk. This field alone would have rated the account as high risk.

4.19 In addition, the score for Customer 1 turnover was also incorrectly recorded as 25 instead of 250. This again would have automatically rated the customer high risk, in line with the risk rating methodology. Neither the change in risk rating nor incorrect scoring was identified at any stage. The MLRO approved the rating with no rationale provided. This has also impacted the periodic review cycle, which has changed from yearly (for high-risk customers) to every three years (for low-risk customers). As we have identified it should have been rated high risk, its 2025 review is therefore overdue.

4.20 The CRAs for 2023 and 2024 for Customer 2 were also inconsistent, with different scores for the same fields and other fields removed without explanation. An example is the adverse media field reflecting different responses (‘‘Yes’’ in 2023 and ‘‘No‘‘ in 2024).

4.21 Similarly, on the Customer 3 and Customer 4 CRA checklists, the score for turnover was left blank. This is evidence of a control failing as there is no explanation given as to why it is left blank. The scores generated by the turnover figure may have impacted the risk rating and should have been reviewed and analysed as part of CDD.

4.22 The Authority also notes that the CRA methodology failed to reference key jurisdictional assessment tools, such as HM Treasury lists for high-risk third countries. In seven of the nine files, Cyprus is a linked jurisdiction. Cyprus is not listed on the HM Treasury list or FATF (which is used by the Firm). However, it is rated medium risk by KnowYourCountry (which is one of the sources the Firm use). The CRA for the seven files rated Cyprus as low risk and no explanation was provided as to why the CRA methodology had been disregarded.

4.23 The UK National Risk Assessment 2025 also describes Cyprus as among the countries identified in UK law enforcement cases as a jurisdiction frequently part of complex, multi-jurisdictional corporate structures. These are linked to suspicious activities and offences such as fraud and corruption. Cyprus has also historically suffered weaknesses in relation to addressing AML risks arising in its real estate sector, as noted in the Mutual Evaluation Report 2019. This directly impacts the individual file of Customer 5, whose business ventures include real estate in Cyprus.

We did not see evidence of this risk raised or discussed in the Customer 5 file.

Business models

4.24 Regulation 28(13) of the MLR provides that a firm must assess the level of risk of a client. To obtain a level of comfort of a client's risk, regulation 28(2)(c) of the MLRs, as provided for in the JMLSG at paragraph 5.3.23, states that a firm must understand the purpose and intended nature of the business relationship. This relationship should be assessed on an ongoing basis and kept up to date as per regulation 28(11) of the MLRs, and this would include if a firm learned of new information about the client. Finally, to comply with regulation 33(3A)(e) of the MLRs, and specifically for high-risk customers, the business relationship requires approval of senior management.

4.25 Across all files, the client's business model is not clear, with high-level summaries provided that do not explain what the business is and why an account is needed. For all files, there is no evidence that the Firm fully understands the purpose and intended nature of the relationship. For example, the assessment for Customer 4 only comments that the business model "makes sense" It does not explain why it makes sense. This is not an assessment of the level of risk and potential harms.

4.26 In seven of the Client Files, it is unclear why the customers want to open an account with a UK authorised electronic money institution. For instance, in the case of Customer 6 there is no UK presence, no employees and the UBO is based in Peru. Similarly, for Customer 7, it was incorporated in Mauritius, the UBO is Israeli and resides in Cyprus. In these seven files the Authority could not see evidence that the Firm had sought to scrutinise and understand the reasons why the clients wanted to open accounts in the UK.

4.27 The file of Customer 8 did not clearly explain the business model and why the entity is required by its parent company to provide payment services. Two months after the onboarding of Customer 8, a transaction was queried. The customer explained that, in addition to the payment services it provides to the parent firm, it had sourced its own profit-making business. The client explained it would be supporting advertising/marketing services. Whilst the AML/Compliance officer rejected the transaction, there was no evidence that a recommendation was made to reject similar future transactions on the same basis or whether similar transactions took place subsequently. It is not clear what, if anything, the Firm has done to understand the new business and re-assess the risks. There is also no evidence of approval by senior management to continue the relationship. This is also contrary to its own CRA methodology when a change in customer profile should trigger a re-assessment.

4.28 A change in counterparties was identified for three customer files: Customer 7, Customer 1 and Customer 6. The payments were made through a crypto exchange, with the Firm receiving a fiat payment. The customers' used the same crypto exchange provider. Although the Firm did query the initial transactions, the customers' explanation is unclear and it was not challenged by the Firm. The MLRO approved the transactions and payments continued. There is no evidence that the Firm's senior management was made aware of these changes to the business relationship or gave approval to continue the relationship. There is also no evidence this triggered a re-assessment.

4.29 According to the Firm's Business Wide Risk Assessment ("BWR"), crypto transactions are outside its risk appetite, and the relationship should be terminated. The Firm does not explain its definition of a crypto transaction. The Authority cannot determine if receiving fiat through a crypto exchange is outside the Firm's risk

appetite.

4.30 The CRA methodology scores crypto transactions ''100'', which on its own merit rates a customer as low risk based on the Firm's CRA. However, it should reflect a prohibited score if outside the Firm's risk appetite. The crypto field is also inconsistently included as a risk to assess in the CRA checklists. The Firm's failure to clarify its own risk appetite, and apply consistent rules, heightens the risk of facilitating financial crime.

CDD

4.31 Regulations 27 and 28 of the MLRs require that a firm must apply CDD measures when it establishes a business relationship. This CDD must include identifying the customer, verifying the customer's identity, assessing and obtaining information on the purpose and intended nature of the business relationship. In addition to identifying the beneficial owner (if any) of the customer and taking reasonable measures to understand the ownership and control structure relating to the beneficial owner (if a legal person). Part I section 4.2 of the JMLSG also states that one of the broad objectives of the financial crime framework is for firms to understand their customers' expected level of activity. This allows a firm to manage and mitigate its risk.

4.32 All customer application forms in the Client Files were incomplete, and none were dated. Customer 3 left many fields on the application unanswered, including expected value and volume of transactions and counterparties. As insufficient information was captured on the expected account activity, it is unclear how the Firm assessed whether transactions were within the expected use of an account. The CRA methodology also explains that client profiles and transactional flows are evaluated by industry benchmarks. This should allow the Firm to identify client outliers in value and volume of transactions, but this was not evident in any of the files.

4.33 In Customer 5 file, the figures provided for expected outbound transactions were significantly different to the expected inbound transactions, with no evidence that the Firm had queried the shortfall. This suggests the Firm was not fully aware of its relationship with the customer.

4.34 In regulation 19 of the MLRs, firms must establish and maintain adequate and appropriate policies and procedures to mitigate the risk that the firm could be used to further financial crime. The screening of UBOs was inconsistent across all files. The application form requests details on UBOs with a share of over 10%, but the Firm has no document detailing what information is required to complete its due diligence.

4.35 In the Customer 5 file (an individual retail client), the Firm is aware of links to existing corporate clients. This is mentioned when seeking approval from senior management. However, any reliance on existing client information known to the Firm has not been documented. For instance, the Firm seems to be aware that Customer 5 has links to a particular firm, but this is not included in the individual's CV. On a review of the website for that particular firm, the Authority identified that the dialling code is for Brazil, despite that particular firm being based in Dubai. There is also no mention of any senior management on the website, including Customer 5.

4.36 A customer having no online presence presents a greater degree of risk and should require deeper scrutiny. Customer 2 did not have a website and there was no evidence of the Firm trying to understand the reason why, seeking alternative

verification of the business and explaining the concerns to the MLRO/AML officer.

4.37 For Customers 4, 7, 6 and 8, screenshots were taken of the website homepage. However, it was unclear if a holistic assessment of the full website took place as there was no commentary in the file as to why the Firm was comfortable as regard the legitimacy of the websites. Furthermore, upon review, the Authority found inconsistencies between the websites and Companies House information which should have been identified by the Firm. For example, an Irish address in Dublin is published on the Customer 6 website, whereas Companies House and the application form provide a UK address in London. Inconsistencies such as these can be indicators of the existence of shell companies which are not legitimate businesses and should be properly explored prior to on-boarding.

4.38 The Firm's scoring methodology for a client's online presence is too low and therefore often delivers a final overall 'low' client risk rating. Furthermore, the Firm seems to inconsistently apply this scoring methodology. The CRA methodology scoring gives a weight of fifty points for a customer with no online presence and twenty-five if there is a website, but issues detected. On review of the Firm's holistic scoring matrix, these scores would rate a client low risk which does not correctly reflect the limited understanding of the client and business model. Furthermore, in relation to Customer 2 and 3, despite both lacking an online presence, were each assigned a score of twenty-five in error.

4.39 While the Firm can demonstrate in part that it has obtained due diligence documents, such as bank statements or management accounts, there was no evidence in the Client Files that they had been reviewed or been considered as appropriate. An appropriate review is required to sufficiently identify the key risks a customer poses or whether further information is required.

EDD and SoW/SoF

4.40 Regulation 33 of the MLRs provides that a firm must apply EDD measures on a risk sensitive basis in any situation which, by its nature, can present a higher risk of money laundering or terrorist financing. This also includes obtaining appropriate information on the SoF and SoW of the client entity and UBO for enhanced due diligence purposes. Six of the nine Client Files were risk rated high, yet the Authority observed evidence of weak EDD.

4.41 The collection of SoF and SoW information from clients was inconsistent across the Client Files. There was no process to follow as to which documents should be requested, and this is evidence of weak formalised policies and procedures. This would also corroborate the findings above by not establishing adequate and appropriate policies. There was no evidence to suggest the Firm sufficiently reviewed and, if necessary, challenged the SoF/SoW documents to satisfy itself that such business did not constitute proceeds of crime.

4.42 For both SoW and SoF, the form included tick box options. The form does not ask for written detail to explain where the funds came from and how the wealth was generated. Furthermore, The SoW section was not included in Customer 5 application form. The SoF section was also missing from five of the nine Client File applications (three of these were high risk files).

PEP and sanction screening

4.43 The Firm must have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is a PEP or a family member or a known close associate of a PEP. This is a requirement of

regulation 35(1) of the MLR. It is in place so a firm can manage the enhanced risks arising from the connections.

4.44 All the Client Files were rated as inadequate against this area of the assessment criteria.

4.45 From late 2024, the Firm used a particular software to screen clients/corporate. Prior to this date the Firm used a new software.

4.46 For three customers (Customers 1, 3, and 4) the new software screening reports appear to be incomplete. The reports stated, "data is not received/verified". The Authority found no evidence in the files that further reports were generated.

4.47 There were at least 10 incidents across the files where the new software reports were completed by customers in another jurisdiction to where they are residing. There is no evidence of the Firm raising the mismatch with the customer in any of these ten incidents.

4.48 There is an overreliance on automated screening, notably for scanning adverse media. There is no evidence of the Firm undertaking manual open-source checks in any of the files. In at least three files, a search on Companies House would have provided more insight into the UBOs. For instance, open-source checks completed by the Authority showed that the UBO of Customer 6 previously held the same role at another firm which was incorporated in Cardiff. The UBO was also recorded as being resident in Egypt until their resignation in December 2022. However, the Customer 6 register recorded the UBO as being a resident in Peru from August 2022. That firm had also been subject to compulsory strike off twice while the UBO was a Director (April and September 2022) and again five months after his resignation (May 2023), which should have been identified at onboarding in October 2023. Customer 6 management accounts have also been overdue since 31 May 2025 which has not been identified.

4.49 Another example is that of the UBO of Customer 9. He is associated to thirty-five other companies, of which eight were current appointments. This may not impact an onboarding decision but understanding historic and current ventures is a key part of the screening process. We could not see any evidence of this being questioned by the Firm.

4.50 An open-source search on the customer file for Customer 5 suggests the customer should be identified as a PEP. The Firm should review the customer's reputation and any public material and how it affects the risk rating of the business relationship. The business industries risk rating on the CRA was low, however, open-source screening result would indicate that the Firm should have increased the score to at least high risk.

4.51 The Authority has also identified the UBO (Customer 5) as being involved in a Cypriot firm which is not disclosed to the Firm and shares the same address as other firms the UBO is linked to and named on the application. These findings were not identified during the automated screening process or through the Firm's transaction monitoring rules. This raises concerns about the quality of the Firm's assessments. The incomplete disclosures or omissions by the client is also evidence of heightened risks posed by this client.

Onboarding decisions and governance framework

4.52 The Firm does not appear to have a robust and formal governance structure in place to monitor and assess financial crime risks as per regulation 28(12)(i) of the MLRs.

The Firm also does not appear to be operating in compliance with regulation 33(3A)(e) of the MLRs, which requires that firms have clearly documented evidence of key decisions from senior management for establishing or continuing relationships. Without clear governance and management information in place, the Firm may not have sufficient information to ensure the prevention of financial crime.

4.53 According to the CRA methodology, the Board of Directors should review and approve high-risk customers. On review of the six high risk files, there is evidence of Board approval being sought in two files. However, the comments made do not make it clear if approval was agreed (for example in relation to Customer 5 and 1). The CRAs on the remaining four files indicate that Board approval was given through email, but there this is not evidenced. On review of the periodic reviews, there are comments on one file (Customer 2) to note Board approval was sought through email, but this is not evidenced. The remaining three files (Customer 1 was re-assessed as low risk, and Customer 5 has not met the yearly timeframe for review), comment N/A (not applicable) for Board approval.

4.54 On three occasions (Customers 8, 6, and 9), the onboarding team sent a summary email to the MLRO with the incorrect risk rating. This was not identified by the MLRO.

4.55 On all files, the MLRO response does not provide any rationale for approval. The decision is generally made in a relatively short period and with the one word ("approved"). It is not clear how the MLRO has had sufficient time to review the onboarding pack, nor is it clear on what basis the MLRO is approving the onboarding because there is insufficient narrative text. This means the Authority did not see evidence that the Firm is making an informed decision and ensuring customers' profiles meet its risk appetite. The MLRO also makes no reference to Board approval.

4.56 The decision to onboard Customer 2 raises concerns because of the significant adverse findings against the UBO. These are available on open-source searches. The US Commodity Futures Trading Commission took civil court action and the UBO was found guilty of illicit trading to US customers. The UBO, and his involvement in the collective firms known as Banc de Binary, were fined in excess of $11millon. At the time, the UBO was already involved with Customer 2.

4.57 The Firm onboarded the customer based on the UBO not having a criminal record and the customer confirming its involvement in the convicted activity was administrative only. The explanation suggests that the Firm does not recognise civil convictions. The Firm is also accepting the explanation of the UBO's involvement as administrative only, without recognising the multimillion dollar fine imposed on them and without interrogating the explanation. The judgement used to discount the civil action, and why seemingly only criminal action is considered, is not sufficiently explained to justify the decision to onboard. The onboarding team also requested approval by the MLRO without referring to the adverse finding and selected ''No'' on the CRA checklist for adverse findings, and this approach was also taken at the periodic review.

4.58 Additionally, as part of the conviction, the UBO was subject to a permanent ban on offering or trading certain contracts to US customers. There is a field on the CRA checklist ''Regulatory Sanctions'', and ''No'' was selected which is clearly incorrect. The CRA methodology acknowledges a response of ''Yes'' would be an automatic prohibition. Therefore, by not applying its own policies and procedures, the customer was onboarded when it should have been rejected.

Suspicious activity reporting and transaction monitoring

4.59 Section 28(11) of the MLRs requires that, as part of its ongoing monitoring of a client relationship, firms should scrutinise transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the Firm's knowledge of the customer, the customer's business and risk profile.

4.60 Regulation 19 of the MLRs requires a firm to establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in its financial crime risk assessment. Specifically, regulation 19(4)(d) requires this to include that anyone in a firm'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 (amongst other things) Part 7 of POCA.

4.61 Section 330 of POCA requires employees of the Firm to report to the nominated officer where they have grounds for knowledge or suspicion of money laundering. Section 331 of POCA and regulation 21 (5) of the MLRs requires the nominated officer to report to the National Crime Agency any transaction or activity that, after their evaluation, they know or suspect, or have 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.

4.62 Section 334 of POCA provides that where a person fails to comply with an obligation under POCA to make disclosures to a nominated officer and/or to the Nation Crime Agency as soon as practicable after the information giving rise to the knowledge or suspicion comes to the member of staff, a firm is open to criminal prosecution or regulatory censure.

4.63 Across all nine of the Client Files submitted for review, there was no evidence of any SARs having been submitted. There was also insufficient detail to determine whether SARs should have been submitted. This may create significant risk that the Firm's policies, controls and procedures in place to report suspicious activity either internally or externally may not be working effectively.

4.64 The review of the nine transaction monitoring alerts evidenced there was insufficient investigation or rationale to determine whether a SAR should have been submitted. This raises concern that the Firm is not be identifying and/or disclosing unusual or suspicious activity to the UK Financial Intelligence Unit within the National Crime Agency. A proper understanding and disclosure of suspicious activity reporting is paramount to ensuring firms are mitigating the risk of financial crime and contributing to maintaining integrity of the UK financial markets.

4.65 In the file for Customer 5, an alert was raised on a large transaction seeking approval from the MLRO. The MLRO requested source of wealth information to allow them to assess the transaction. Just 2 hours later with no evidence of actual information being provided to the MLRO, the transaction was given formal approval citing that the MLRO had "seen the tax return". There was no explanation as to where the tax form originated from, what it showed and the rationale for why this meant the transaction was suitable for approval.

4.66 In the file for Customer 2, the Firm reached out to the client after the transaction had been approved. There was no supporting evidence that the client responded. The Firm made further contact a month later querying the value comparative to the expected monthly turnover. There was no evidence of a response or any follow-up.

4.67 The transaction for Customer 3 was placed into a folder named ("out of the ordinary"). There was no further information in the folder apart from the alert report and no explanation of the folder's name.

4.68 In all of the files, the transaction monitoring reports were not generated in real time. It was also evident in two of the files that the transaction monitoring rules were generic rather than based on the client profile. For example, a transaction for Customer 9 related to a payment of wages. The account could have specific parameters to mitigate false positives for recurring salary payments. For Customer 4, the Firm was aware that the account would receive forty to forty-five incoming payments a month from a specific counterparty. The transaction was held as related to more than one transaction a day, though this was inevitable, based on the expected volumes. The transaction was approved within a minute and without any commentary to justify the decision. It was not clear how the transaction was reviewed in a relatively short period. If the rule was not generic but specific to the customer, it would be less likely to trigger an alert.

4.69 For the two transactions reviewed from Customer 8 and Customer 7, there was no evidence of a trigger report, which raises concerns about the quality of the Firm's record keeping and its transaction monitoring alerts.

4.70 In two other examples (Customers 1 and 7), the total score did not match the total score generated by the alert rules. The alerts were manually reviewed, and this was not picked up, suggesting inadequate reviews and potentially weak quality assurance.

4.71 In addition to the transaction monitoring reviews, as part of the Client File reviews, the Authority identified that the MLRO approved a transaction without full confidence. In the Customer 8 file, the MLRO responds with "I think I am satisfied". The comment suggests doubt and further information should have been sought from the customer.

4.72 Furthermore, according to the CRA methodology, all high-risk clients should be subject to strict monitoring for either 90 or 180 days. The CRA methodology does not explain what the monitoring entails, how it differs from enhanced due diligence, who is responsible for its compliance and possible outcomes following the expiration of the timeframe.

4.73 There are examples in the Client Files where is evident that the Firm is aware of the 90/180-day enhanced monitoring but has not actually applied it. On two of the five high risk files, (Customers 7 and 6) the MLRO approved the onboarding and attached a condition of strict ongoing monitoring for 180 days. On the CRA checklist for Customer 2, there is a comment by the onboarding team noting approval is subject to close monitoring, but the MLRO makes no reference to this condition. The files have no further reference to the control – we cannot see if or how it was applied.

4.74 In the case of Customer 6, its offboarding causes concern. On 25 June 2025, the client requested to close its account, citing a significant reduction in activity and business costs. However, in the preceding 10 months leading up to closure, the Firm had identified that the turnover, volume and value of transactions exceeded the customer's forecast. The customer had explained this is because of its success ''significant level of activity'' - a direct contradiction of its account closure justification. Customer 6 response to a periodic review questionnaire also confirmed it had no intention to grow. The Firm had requested account statements to reflect the increase in business and projected forecasts, but the Authority cannot

see evidence that audited accounts ever materialised. The Firm initially requested information in August 2024 and repeated the requests up until Customer 6 were offboarded in June 2025. This meant that 10 months elapsed and there is no evidence of mitigating controls being implemented while due diligence risk heightened. The Firm also suggested to the customer it might temporarily suspend the account, but this did not materialise either and no explanation was given as to why.

4.75 The client provided a goodstanding letter by a firm of chartered accountants. On review of this form of chartered accountants, the registered office address differs between Companies House in comparison to its website and the Institute of Chartered Accountants. The accountant/UBO is also involved in sixteen other firms according to Companies House. The goodstanding letter is vague, generic and did not provide the projected turnover that the Firm had requested. The Firm explained the goodstanding letter was not sufficient on 24 June 2025.There is, however, no evidence of internal escalation, or challenge on the content or the authenticity of the accountants.

4.76 Throughout this period (September 2024-June 2925), there is no evidence of the Board discussing the risks of continuing to provide services to this client, or whether additional controls should be implemented whilst transactions continued. As noted above, Companies House also confirmed its management accounts were outstanding, which would correlate with the Firm not receiving the accounts it was requesting.

4.77 The Firm closed the account the same day without any queries, escalation or Board discussion. There was also no documented consideration of whether a SAR should be raised. This raises material concerns around the Firm's governance and systems and controls.

4.78 Overall, we do not consider the Firm's financial crime framework to be effective or operationally workable.

5 CONCLUSION

5.1 The regulatory provisions relevant to this First Supervisory Notice are set out in the Annex.

Analysis of failings and risks

5.2 AEMI's, such as the Firm, are required to comply with the requirements of the MLRs to deter and detect financial crime, which includes money laundering and terrorist financing. As part of this, The Authority expect firms to demonstrate that they establish and maintain appropriate and risk-sensitive policies and procedures to counter the risk that they may be used to further financial crime. These policies and procedures should be proportionate to the nature, scale and complexity of the firm's activities and enable it to identify, manage, monitor and report any financial crime risks to which it may be exposed.

5.3 As a result of its review and assessment of the Client Files, The Authority has significant concerns with the adequacy and operational effectiveness of the Firm's financial crime controls. The Authority is concerned that the inadequacies observed in the Client Files, several of which may represent failures to comply with the MLRs and POCA, suggest that the Firm is currently failing to adequately identify, manage, monitor and report the risk of its business being used to facilitate financial crime. The extent and severity of the failings across all the Client Files and relating as they to different aspects of the financial crime control framework from across the client

lifecycle, suggests consistent issues indicative of risks across the Firm's financial crime systems and controls.

CRA

5.4 As stated above, the Authority found that the CRA for each of the Client Files provided no commentary on whether the Firm took appropriate steps to assess the level of risk and rationale for onboarding each client. The Authority considers that the presence of an inadequate CRA by the Firm, and/or the Firm's change to the CRA during the course of a relationship with a client with no supporting evidence or rationale give rise to possible breaches of regulation 18(1) and (2), and 28 of the MLRs as they suggest that the Firm:

(i) has failed to take appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject (regulation 18(1) of the MLRs).

(ii) has failed to take account of the information and risk factors outlined in regulation 18(2) of the MLRs.

5.5 The Authority's assessment is that this may indicate that the Firm does not have a clear view of the financial crime risk posed by its customer base.

CDD

5.6 As stated above, regulations 27 and 28 of the MLRs require that a firm must apply CDD measures when it establishes a business relationship. This CDD must include identifying the customer, verifying the customer's identity, assessing and obtaining information on the purpose and intended nature of the business relationship. In addition to identifying the beneficial owner (if any) of the customer and taking reasonable measures to understand the ownership and control structure relating to the beneficial owner (if a legal person).

5.7 From its review and assessment of the Client Files, The Authority found that all the customer application forms were incomplete, and none of them were dated.

5.8 The Authority is particularly concerned that the lack of adequate, sufficient and consistent CDD, including obtaining adequate explanation and understanding of intended nature and purpose of an account, may represent a breach of regulation 28(13) of the MLRs.

PEP and sanction screening

5.9 As stated above, regulation 35(1) of the MLRs requires the Firm have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is a PEP or a family member or a known close associate of a PEP. This is to ensure that the Firm manage the enhanced risks arising from the relevant person's business relationship or transactions with such a customer.

5.10 From its review and assessment of the Client Files, the Authority found that all the Client Files were rated as inadequate against this area of the assessment criteria.

5.11 The failings identified in respect of CDD means that the Firm may not have adequate information to determine whether its customer of the beneficial owner is a PEP, and to manage the risks accordingly is a possible breach of regulation 35(1) of the MLRs.

EDD including SOW and SOF

5.12 As stated above, regulation 33 of the MLRs provides that a firm must apply EDD to manage and mitigate the risks in circumstances including where there is a high risk of money laundering or terrorist financing and in any business relationship with a person established in a high-risk third country. The Firm's failures in respect of its CRA and CDD mean that not all clients have been correctly identified as high-risk clients, and therefore the review and assessment of the Client Files demonstrate a lack of consistent and adequate EDD at onboarding. The Authority considers that this suggests that the Firm may be in breach of regulation 33(1) of the MLRs.

SARs

5.13 As stated above, regulation 28(11) of the MLRs requires that, as part of its ongoing monitoring of a client relationship, firms should scrutinise transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, the customer's business and risk profile.

5.14 Regulation 19 of the MLRs requires a firm to establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in its financial crime risk assessment. Specifically, regulation 19(4)(d) requires this to include anyone in a firm'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 (amongst other things) Part 7 of POCA.

5.15 Across all nine of the Client Files, there was no evidence of any SARs having been submitted. There was also insufficient detail to determine whether SARs should have been submitted. This may create significant risk that the Firm's policies, controls and procedures in place to report suspicious activity either internally or externally may not be working effectively.

5.16 The Firm's Client File failings, coupled with the high-risk nature of many of its clients, create the significant risk that the Firm is unable to identify when SARs are required, and may not be stopping transactions as appropriate, or complying with its obligation to report suspicious activity. The Authority is concerned that in such circumstances, permitting the Firm to continue to service customers and to return customer funds without sufficient safeguards poses serious risks to trust in payment services. Further, the inadequacies across all the Client Files indicate serious concerns about the Firm's anti-money laundering systems and controls, such that The Authority is concerned that the Firm's conduct puts it at risk of being used for the purposes of financial crime.

Firm appears not to be meeting the conditions for authorisation: Regulation 6(5) of the EMRs

5.17 The Authority considers that the Firm does not appear to be meeting the conditions for authorisation as an AEMI under regulation 6(5)(b) of the EMRs because, based on the Client File review, the Authority has serious concerns about the operational effectiveness and adequacy of the Firm's financial crime controls, such that The Authority considers that the Firm may be currently failing to identify, manage, monitor and report the risk of its business being used to facilitate financial crime.

5.18 The Authority has concluded that it is necessary to vary the Firm's authorisation by imposing the Requirements which stop the Firm conducting any payment services

as defined under regulation 2(1) of the PSRs without the prior written consent of the Authority. For the avoidance of doubt this includes not to onboard any new customers and not to accept any new relevant funds (as defined in regulation 23 of the PSRs).

5.19 The Authority considers that variation of the Firm's authorisation by the imposition of the Requirements are a proportionate and appropriate means to address the current and immediate risks and are desirable in order to maintain trust in a payment system in accordance with the Authority's duties under regulation 11(1)(c) of the EMRs.

Timing and duration of the Requirements

5.20 It is necessary to impose the Requirements on an urgent basis given the seriousness of the risks and the need to protect consumers' funds.

5.21 The Authority considers that it is necessary for the Requirements to remain in place indefinitely.

6 PROCEDURAL MATTERS

Decision maker

6.1 The decision which gave rise to the obligation to give this First Supervisory Notice was made by an Authority staff member under executive procedures according to DEPP 2.5.7 and DEPP 2.5.7B.

6.2 This First Supervisory Notice is given to the Firm under regulation 11(6) of the EMRs and in accordance with regulation 11(7) of the EMRs.

6.3 The following statutory rights are important.

Representations

6.4 The Firm has the right to make written representations to the Authority (whether or not it refers this matter to the Tribunal). The Firm may also request to make oral representations but the Authority will only consider this in exceptional circumstances according to DEPP 2.3.1AG. The deadline for providing written representations and notifying the Authority that the Firm wishes to make oral representations is 14 days from the date of the FSN or such later date as may be permitted by the Authority. Any notification or representations should be sent to the Executive Decision Making Secretariat (EDMCaseInbox@fca.org.uk).

The Tribunal

6.5 The Firm has the right to refer the matter to which this First Supervisory Notice relates to the Tribunal. The Tax and Chancery Chamber is the part of the Tribunal which, amongst other things, hears references arising from decisions of the Authority. Under paragraph 2(2) of Schedule 3 of the Tribunal Procedure (Upper Tribunal) Rules 2008, the Firm has 28 days from the date on which this First Supervisory Notice is given to it to refer the matter to the Tribunal.

6.6 A reference to the Tribunal can be made by way of a reference notice (Form FTC3) signed by or on behalf of the Firm and filed with a copy of this First Supervisory Notice. The Tribunal's contact details are: Upper Tribunal, Tax and Chancery Chamber, 5th Floor, Rolls Building, Fetter Lane, London EC4A 1NL (telephone: 020 7612 9700; email: uttc@hmcts.gsi.gov.uk).

6.7 Further information on the Tribunal, including guidance and the relevant forms to complete, can be found on the HM Courts and Tribunal Service website: http://www.justice.gov.uk/froms/hmcts/tax-and-chancery-upper-tribunal

6.8 The Firm should note that a copy of the reference notice (Form FTC3) must also be sent to the Authority at the same time as a reference is filed with the Tribunal. A copy of the reference notice should be sent to the Executive Decision Making Secretariat (EDMCaseInbox@fca.org.uk).

Confidentiality and publicity

6.9 The Firm should note that this First Supervisory Notice may contain confidential information and should not be disclosed to a third party (except for the purpose of obtaining legal advice on its contents).

6.10 The Firm should note that section 391(5) of the Act, as applied by paragraph 8 of Schedule 3 of the EMRs, requires the Authority, when this First Supervisory Notice takes effect (and this First Supervisory Notice takes immediate effect), to publish such information about the matter to which the notice relates as it considers appropriate.

Authority contacts

6.11 For more information concerning this matter generally, contact the Executive Decision Making Secretariat (EDMcaseinbox@fca.org.uk).

Decision made under executive procedures

Head of Department, Resolution Strategy, Operations and CASS - Supervision, Policy and Competition

Annex

RELEVANT STATUTORY PROVISIONS

The EMRs

1. Regulation 6 of the EMRs state that:

   (1) The Authority may refuse to grant an application for authorisation only if any of the conditions set out in paragraphs (2) to (8) is not met.

   (5) The applicant must satisfy the Authority that, taking into account the need to ensure the sound and prudent conduct of the affairs of the institution, it has—
   (a)robust governance arrangements for its electronic money issuance and payment service business, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility;
   (b)effective procedures to identify, manage, monitor and report any risks to which it might be exposed; and
   (c)adequate internal control mechanisms, including sound administrative, risk management and accounting procedures,
   which are comprehensive and proportionate to the nature, scale and complexity of electronic money to be issued and payment services to be provided by the institution.

2. Regulation 7(1) of the EMRs provides that the Authority may include in the authorisation of an authorised electronic money institution such requirements as it considers appropriate. Regulation 7(2) of the EMRs provides that a requirement may, in particular, be imposed so as to require the person concerned to: 1) take a specified action, or 2) to refrain from taking a specified action.

3. Regulation 8(a) of the EMRs provides that the Authority may, on the application of an authorised electronic money institution, vary that person's authorisation by, among other things, imposing a requirement such as may, under regulation 7 of the EMRs, be included in an authorisation.

4. Regulation 11(1) of the EMRs provides that the Authority may vary the authorisation of an electronic money institution in any of the ways mentioned in regulation 8 if it appears to the Authority that:

   "[…]

   (a) The person no longer meets, or is unlikely to continue to meet, any of the conditions set out in regulation 6(4) to (8) of the EMRs.
   (c) The person would constitute a threat to the stability of a payment system by continuing to issue electronic money or provide payment services."

5. Regulation 11(2) of the EMRs provides that a variation takes effect immediately if the notice given under paragraph (6) states that this is the case, or on such date as may be specified. Regulation 11(3) of the EMRs provides that a variation may be expressed to take effect immediately or on a specified date only if the Authority, having regard to the ground on which it is exercising the power under paragraph (1), reasonably considers that it is necessary for the variation to take effect immediately or, as the case may be, on that date.

6. Regulation 11(6) of the EMRs provides that, where the Authority proposes to vary a person's authorisation, it must give the person notice.

7. Section 391 of the Act, as applied in modified form by paragraph 8 of Schedule 3 to the EMRs, provides that:

"[…]

(5) When a supervisory notice takes effect, the Authority must publish such information about the matter to which the notice relates as it considers appropriate.
(6) The Authority may not publish information under this section if, in its opinion, publication of the information would be: a) unfair to the person with respect to whom the action was taken (or was proposed to be taken), b) prejudicial to the interests of consumers, or c) detrimental to the stability of the UK financial system.
(7) Information is to be published under this section in such manner as the Authority considers appropriate."

The MLRs

8. Regulation 18 of the MLRs 18 provides that:

(1) 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.

(2) In carrying out the risk assessment required under paragraph (1), a relevant person must take into account—
(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.
[…]

9. Regulation 19 provides that:

(1) 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);

(b)regularly review and update the policies, controls and procedures established under sub-paragraph (a);

(c)maintain a record in writing of—

(i)the policies, controls and procedures established under sub-paragraph (a);

(ii)any changes to those policies, controls and procedures made as a result of the review and update required by sub-paragraph (b); and

(iii)the steps taken to communicate those policies, controls and procedures, or any changes to them, within the relevant person's business.

(2) 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.

(3) The policies, controls and procedures referred to in paragraph (1) must include—

(a)risk management practices;

(b)internal controls (see regulations 21 to 24);

(c)customer due diligence (see regulations 27 to 38);

(d)reliance and record keeping (see regulations 39 to 40);

(e)the monitoring and management of compliance with, and the internal communication of, such policies, controls and procedures.

(4) The policies, controls and procedures referred to in paragraph (1) must include policies, controls and procedures—

(a)which provide for the identification and scrutiny of—

(i)any case where—

(aa)a transaction is complex [or] unusually large, or there is an unusual pattern of transactions, [or]

(bb)the transaction or transactions have no apparent economic or legal purpose, and

(ii)any other activity or situation which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;

(b)which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity;

(c)which ensure that when [new products, new business practices (including new delivery mechanisms) or new technology are] adopted by the relevant person, appropriate measures are taken in preparation for, and during, the adoption of such [F4products, practices or] technology to assess and if necessary mitigate any money laundering or terrorist financing risks this new [product, practice or] technology may cause;

(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; or

(ii)Part 7 of the Proceeds of Crime Act 2002;

(e)which, in the case of a money service business that uses agents for the purpose of its business, ensure that appropriate measures are taken by the business to assess—

(i)whether an agent used by the business would satisfy the fit and proper test provided for in regulation 58; and

(ii)the extent of the risk that the agent may be used for money laundering or terrorist financing.

(5) 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.

10. Regulation 27 provides that:

(1) A relevant person must apply customer due diligence measures if the person—

(a)establishes a business relationship;

(b)carries out an occasional transaction that amounts to a transfer of funds within the meaning of Article 3.9 of the funds transfer regulation exceeding 1,000 euros;

(c)suspects money laundering or terrorist financing; or

(d)doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification.

11. Regulation 28 of the MLRs provides that:

(2) The relevant person must—
(a)identify the customer unless the identity of that customer is known to, and has been verified by, the relevant person;
(b)verify the customer's identity unless the customer's identity has already been verified by the relevant person; and
(c)assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction.

(4) 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.

(12) The ways in which a relevant person complies with the requirement to take customer due diligence measures, and the extent of the measures taken—

(a)must reflect—

(i)the risk assessment carried out by the relevant person under regulation 18(1);

(ii)its assessment of the level of risk arising in any particular case;

(b)may differ from case to case.

(13) In assessing the level of risk in a particular case, the relevant person must take account of factors including, among other things—

(a)the purpose of an account, transaction or business relationship;

(b)the level of assets to be deposited by a customer or the size of the transactions undertaken by the customer;

(c)the regularity and duration of the business

12. Regulation 35 of the MLRs provides that:

(1) A relevant person must have in place appropriate risk-management systems and procedures to determine whether a customer or the beneficial owner of a customer is—

(a)a politically exposed person (a "PEP"); or

(b)a family member or a known close associate of a PEP,

and to manage the enhanced risks arising from the relevant person's business relationship or transactions with such a customer.

RELEVANT REGULATORY PROVISIONS

SUP

13. The Authority's approach in relation to its own-initiative powers is set out in Chapter SUP 6B, certain provisions of which are summarised below.

14. The Authority considers that the powers under regulation 11(1) of the EMRs are similar to those under sections 55J and 55L of the Act and that the provisions of SUP 6B "Variation and cancellation of permission and imposition of requirements on the Authority's own-initiative and intervention against incoming firms" are applicable.

15. SUP 6B.1.1 states that the Authority will have regard to its statutory objectives and the range of regulatory tools that are available to it when it considers how it should deal with a concern about a firm. It will also have regard to: 1) the responsibilities of a firm's management to deal with concerns about the firm or about the way its business is being or has been run; and 2) the principle that a restriction imposed on a firm should be proportionate to the objectives the Authority is seeking to achieve.

16. SUP 6B.2.3 states that in the course of its supervision and monitoring of a firm or as part of an enforcement action, the Authority may make it clear that it expects the firm to take certain steps to meet regulatory requirements. In the vast majority of cases the Authority will seek to agree with a firm those steps the firm must take to address the Authority's concerns. However, where the Authority considers it appropriate to do so, it will exercise its formal powers under section 55J or 55L of the Act where the Authority considers it appropriate to ensure such requirements are met. This may include where, amongst other factors, the Authority has serious concerns about a firm, or about the way its business is being or has been conducted

or is concerned that the consequences of a firm not taking the desired steps may be serious.

17. SUP 6B.3.1 states that the Authority may impose a requirement so that it takes effect immediately or on a specified date if it reasonably considers it necessary for the requirement to take effect immediately (or on the date specified), having regard to the ground on which it is exercising its own-initiative powers.

18. SUP 6B.3.2 states that the Authority will consider exercising its own-initiative power where: 1) the information available to it indicates serious concerns about the firm or its business that need to be addressed immediately; and 2) circumstances indicate that it is appropriate to use statutory powers immediately to require and/or prohibit certain actions by the firm in order to ensure the firm addresses these concerns.

19. SUP 6B.3.3 states that it is not possible to provide an exhaustive list of the situations that will give rise to such serious concerns, but they are likely to include some of the following characteristics: 1) information indicating significant loss, risk of loss or other adverse effects for consumers, where action is necessary to protect their interests; and 2) evidence that the firm has submitted to the Authority inaccurate or misleading information so that the Authority becomes seriously concerned about the firm's ability to meet its regulatory obligations.

20. SUP 6B.3.4 states that the Authority will consider the full circumstances of each case when it decides whether an imposition of a requirement is appropriate and sets out a non-exhaustive list of factors the Authority may consider, these include: 1) the extent of any consumer loss or risk of consumer loss or other adverse effect on consumers; 2) the extent to which customer assets appear to be at risk; 3) the financial resources of the firm; 4) the nature of the false or inaccurate information; and 5) the impact that use of the Authority's own-initiative powers will have on the firm's business and on its customers.

21. SUP 6B.4.4 states that examples of requirements that the Authority may consider imposing when exercising its own-initiative power are: 1) a requirement not to take on new business; 2) a requirement not to hold or control client money; and 3) a requirement that prohibits the disposal of, or other dealing with, any of the firm's assets or restrict those disposals or dealings.

DEPP

6.12 The relevant entry in DEPP 2 Annex 1 for the exercise of powers under regulation 11(6) of the EMRs on the Authority's own-initiative provides that the decision will be taken under executive procedures.

6.13 DEPP 2.5.7G provides that an Authority staff under executive procedures will take the decision to give a supervisory notice exercising the Authority's own-initiative powers (by removing a regulated activity, by imposing a limitation or requirement or by specifying a narrower description of regulated activity), including where the action involves a fundamental requirement.

6.14 DEPP 2.5.7BG provides that an Authority staff of at least Director level will take the decision to give a supervisory notice exercising the Authority's own-initiative powers if the action involves a fundamental requirement. DEPP 2.5.8G provides that a fundamental requirement means: 1) removing a type of activity from an authorisation or registration; 2) refusing an application to include a type of activity; or 3) imposing or varying an assets requirement or refusing an application to vary or cancel such a requirement.