

---

## **FINAL NOTICE**

---

To: Monzo Bank Limited

Reference  
Number: 730427

Address: Broadwalk House, 5 Appold Street, London, EC2A 2AG

Date: 7 July 2025

### **1. ACTION**

- 1.1. For the reasons given in this Notice, the Authority hereby imposes on Monzo Bank Limited a financial penalty of £21,091,300 pursuant to section 206 of the Act.
- 1.2. Monzo agreed to resolve this matter and qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £30,130,475 on Monzo.

### **2. SUMMARY OF REASONS**

- 2.1. Monzo is one of several digital challenger banks which have increased competition in the banking sector through the use of technology and more up-to-date IT systems. Monzo was authorised in August 2016 and granted full banking permissions in April 2017.

- 2.2. Since obtaining its full banking permissions, Monzo's customer base has substantially increased, growing from approximately 250,000 customers in early 2017 to over 12 million personal and business customers by April 2025. Likewise, Monzo's product offering, which was originally centred around the provision of pre-paid payment cards, has expanded from the provision of personal current accounts to business banking, overdrafts, loans and money transfers. However, rapid customer growth must not come at the detriment of compliance with the requirement to maintain adequate systems and controls to counter the risk that the firm might be used to further financial crime.
- 2.3. Because of the significant risks of their services being used to facilitate financial crime, in particular money laundering, banks are required to maintain robust systems to counter this risk. These systems must be proportionate to the nature, scale and complexity of their activities.
- 2.4. Key elements of Monzo's financial crime framework, particularly with regard to customer risk assessments and the collection of customer information, did not keep pace with the Firm's expansion and, during the Pre-VREQ Period, the Authority considers that they were inadequate to counter actual and potential financial crime risks effectively.
- 2.5. For a substantial part of the Pre-VREQ Period, Monzo operated a more limited approach to gathering customer information ("customer due diligence" or "CDD") at the point of onboarding. While this facilitated account opening processes, it meant that Monzo did not obtain and/or assess sufficient information about prospective customers. In particular, the Firm failed to obtain information about the purpose and nature of the proposed customer relationship and, at times, failed to review adverse media hits for a customer unless another risk factor was present. In respect of business customers, Monzo's CDD procedures did not provide, as required by the MLRs, for verification of the identity of all beneficial owners and persons of significant control ("PSCs").
- 2.6. This meant that Monzo was at the time unable to assess all the financial crime risks which its customers presented and unable effectively to monitor whether their use of Monzo's services was consistent with its knowledge of them.
- 2.7. Furthermore, Monzo's policy, upon which its financial crime risk appetite was based, was only to service customers based in the UK. However, for most of the Pre-VREQ Period Monzo stopped verifying customer addresses for certain personal banking customers and therefore was unable to ensure that its customer base did

not exceed its risk appetite. Monzo subsequently identified instances of customers using PO Boxes, foreign addresses with UK postcodes or obviously implausible UK addresses, such as well-known London landmarks. Monzo subsequently accepted that it was unable to confirm that all customers were UK-based.

- 2.8. The lack of effective onboarding controls during most of the Pre-VREQ Period also enabled some customers to open multiple accounts without Monzo being aware, including 2 customers whose accounts had previously been closed as a result of financial crime concerns. In the absence of full knowledge of the customer's activities, Monzo was unable effectively to assess the money laundering risks associated with the customer.
- 2.9. Where banks identify customers as presenting higher risks of money laundering, they are required to conduct enhanced customer due diligence ("EDD"). Until August 2020, Monzo's EDD processes for most categories of personal banking customers did not provide for the circumstances in which EDD would be necessary, nor as to how, when and where an EDD review needed to be documented. This meant that, in respect of some higher-risk personal banking customers, no EDD was carried out.
- 2.10. While Monzo did maintain processes designed to identify politically exposed persons ("PEPs"), who may present higher money laundering risks, it had no clear internal definition of what constituted a PEP, meaning that indicators may not have been consistently applied in some cases and in other instances, some PEPs were not identified at onboarding. Further, Monzo's processes enabled potential PEPs to open accounts and transact while the identification process, and any resulting EDD, was ongoing. This weakness was exacerbated by consistent backlogs in the assessment of PEP flags.
- 2.11. The weaknesses in Monzo's financial crime controls resulted from incorrect assumptions about the nature of many of its customers and products and about the effectiveness of Monzo's transaction monitoring systems to mitigate the lack of customer data gathered at onboarding. Monzo's failure to gather sufficient customer data, meant the Firm was unable effectively to assess whether transactions were consistent with expected activity or were suspicious. In addition, there were weaknesses in Monzo's transaction monitoring processes, including a lack of adequate procedural guidance being provided to staff on how to investigate transaction monitoring alerts and key transaction monitoring tasks being performed by insufficiently experienced or trained staff.

- 2.12. By the end of the Pre-VREQ Period, external data referred to in an internal Monzo document indicated that the Firm was the recipient bank for a higher proportion of fraudulent transactions reported to the external data provider by participating firms relative to the proportion of UK current accounts it operated for customers.
- 2.13. Principle 3 of the Authority's Principles requires a firm to take reasonable steps to ensure that it has organised its affairs responsibly and effectively, with adequate risk management systems.
- 2.14. By failing to design, implement, and maintain adequate systems and controls to mitigate financial crime risks (in particular in relation to the onboarding and risk assessment of customers), Monzo breached Principle 3 during the Pre-VREQ Period.
- 2.15. In August 2020, the Authority required Monzo to appoint a Skilled Person to undertake a full and substantive review of the state of its financial crime risk management. In addition, at the request of the Authority, Monzo applied for requirements to be imposed upon it, principally to prevent it from accepting or processing new or additional account applications for high-risk customers ("VREQ"). A detailed categorisation of what defined high risk was included within the sub-requirements of the VREQ, which the Authority imposed on Monzo's Part 4A permissions from 5 August 2020 (i.e. the first day of the Relevant VREQ Period).
- 2.16. When the Authority imposes a requirement on an authorised firm's Part 4A permissions, the firm must correctly implement all necessary changes to its systems and controls to ensure that the terms of the requirements are met immediately and on an ongoing basis, until the requirements are varied or cancelled by the Authority.
- 2.17. Monzo failed to properly implement all of the VREQ's underlying requirements and sub-requirements and did not adequately monitor or test its compliance with the terms of the VREQ following its imposition. As a result, over the Relevant VREQ Period, Monzo opened 33,039 accounts in breach of the VREQ; 26,325 of these accounts were for high-risk customers.
- 2.18. Separately, at times during the Relevant VREQ Period, Monzo failed to apply certain of its VREQ controls to new or additional account applications and at times applied its VREQ controls to incorrect information. These instances were connected to 167,444 accounts opened by Monzo during the Relevant VREQ

Period. The Firm estimates that these instances may have led to the onboarding of 34,262 high-risk customers.

- 2.19. Monzo therefore contravened the VREQ during the Relevant VREQ Period which was a relevant requirement imposed under section 55L of the Act.
- 2.20. The Authority therefore imposes on Monzo a financial penalty of £21,091,300, pursuant to section 206 of the Act.
- 2.21. In conjunction with the VREQ and the appointment of a Skilled Person, Monzo has made progress in remediating and enhancing its financial crime framework. The Authority acknowledges Monzo's commitment to ensuring, on an ongoing basis, that it has an effective financial crime framework in place.
- 2.22. Monzo has cooperated fully with the Authority throughout the course of its investigation.

### **3. DEFINITIONS**

- 3.1. The definitions below are used in this Notice:

"2016 AML Review" means the review of Monzo's AML policies and procedures conducted by an external consultant on Monzo's behalf;

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

"AML" means anti-money laundering;

"the Authority" means the Financial Conduct Authority;

"CDD" means customer due diligence;

"CIFAS" means the company formerly known as Credit Industry Fraud Avoidance System, a UK fraud prevention service with over 250 members across the financial industry and other sectors. For further information, see [www.cifas.org.uk](http://www.cifas.org.uk);

"CRA" means customer risk assessment;

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

"EDD" means enhanced customer due diligence;

"FCC" means Monzo's Financial Crime Compliance Team;

"FCRA" means Financial Crime Risk Assessment, the assessment made by Monzo of the financial crime risks to which it is exposed;

"Fincrim Compliance Review" means Monzo's Financial Crime Compliance Review of Duplicate User Controls in October 2020;

"the Handbook" means the Authority's Handbook of rules and guidance;

"IDV" means identification and verification, the process of identifying, and verifying the identity of, a customer or potential customer;

"Legal Firm" means the Legal firm instructed by Monzo in 2021 to conduct an independent review of its implementation of the VREQ.

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

"MLRO" means Money Laundering Reporting Officer;

"MoF" means Misuse of Facility;

"Monzo" or "the Firm" means Monzo Bank Ltd (FRN: 730427);

"NRA" means the UK's 2020 National Risk Assessment of money laundering and terrorist financing;

"Part 4A permissions" means the regulatory permissions given by the Authority or the PRA under Part 4A of the Act (Permission to carry on regulated activities), or having effect as if so given;

"PEP" means Politically Exposed Person;

"PRA" means the Prudential Regulation Authority;

"Pre-VREQ Period" means 1 October 2018 to 4 August 2020 inclusive;

"Principles" means the Authority's Principles for Businesses as set out in the Handbook;

"PSCs" means people with significant control;

"Relevant Period" means 1 October 2018 to 30 June 2022 inclusive (i.e. the Pre-VREQ Period and Relevant VREQ Period combined);

“Skilled Person” means the person appointed under section 166 of the Act following a requirement notice dated 14 August 2020;

“the Tribunal” means the Upper Tribunal (Tax and Chancery Chamber);

“VREQ” means the requirements (as modified) which the Authority imposed on Monzo’s permissions under section 55L(5)(a) of the Act from 5 August 2020 until 26 February 2025; and

“Relevant VREQ Period” means 5 August 2020 to 30 June 2022 inclusive.

## **4. FACTS AND MATTERS**

### **Background**

- 4.1. Monzo was originally authorised by the PRA on 10 August 2016 and granted a UK banking license with restrictions. Since that date, the Firm has been regulated by the Authority and the PRA. In 2017, Monzo received full banking permissions and thereafter offered, and continues to offer, a variety of services to its customers, including the provision of personal current accounts, business banking, overdrafts, loans and money transfers.
- 4.2. Monzo is a digital challenger bank. Challenger banks are a sub-sector of retail banks that aim to reduce the market concentration of traditional high street banks through the use of technology and more up-to-date IT systems. Digital challenger banks have the following common features in their business models: they primarily offer personal current accounts, they operate without a branch network, and they provide financial services through smartphone apps.
- 4.3. The Authority has identified challenger banks as an important part of the UK’s retail banking sector. Specifically, the Authority has identified good practice in relation to their innovative use of technology to identify and verify customers at speed, allowing for quick and easy account openings. However, in its 2022 financial crime review (see paragraph 4.23 below for further details), the Authority found that the challenger bank sub-sector as a whole needed to do more in relation to their financial crime controls.
- 4.4. In recent years, challenger banks have experienced significant growth both in their revenue and the numbers of customers opening accounts with them. When a financial institution undergoes such growth, it must continue to ensure it can effectively counter the risk that it might be used to further financial crime. In

doing so, such institutions must comply with applicable regulatory rules (including the Authority's Principles and the MLRs).

- 4.5. The following table details Monzo's growth between February 2018 and March 2023:

	<b>February 2018</b>	<b>February 2022</b>	<b>March 2023</b>
<b>Number of customers</b>	590,000	5.8m	7.4m
<b>Customer deposits</b>	£71.3m	£4.4bn	£6.0bn
<b>Lending</b>	£0.2m	£259m	£800m
<b>Revenue</b>	£2.7m	£154m	£355.6m

- 4.6. Over the course of the Relevant Period, Monzo's customer base grew significantly, including the Firm taking on business banking customers, initially on a pilot basis, from 2019. In parallel with its growing customer base, Monzo diversified its product offering, adding several new features to its current account and introducing a Lending product. Monzo's expansion of its business broadened the range of actual and potential financial crime risks which it could have been exposed to. Monzo recognised the importance of taking a "*proactive approach*" to addressing such risks.
- 4.7. Monzo is subject to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "MLRs"). Firms subject to the MLRs have an overarching obligation to take specified steps to detect and prevent money laundering, terrorist financing and, since 2022, proliferation financing. Furthermore, the Authority expects firms to have effective systems and controls which can identify, assess, monitor, and manage money laundering risk. These controls must be appropriate and proportionate to the nature, scale and complexity of a firm's activities.
- 4.8. Monzo's specific obligations under the MLRs include customer due diligence (i.e. "CDD"). Monzo's CDD obligations include the requirement to identify and verify



customers. Monzo must also assess, and where appropriate obtain information on, the purpose and intended nature of its business relationships and its customers' transactions. In relation to business customers, this includes ascertaining the nature of the customer's business and establishing how it will use Monzo's services. Establishing this information at the outset of a customer relationship enables Monzo to assess the money laundering risks (amongst other risks) a customer presents against its own risk appetite and tolerance thresholds.

- 4.9. Moreover, where it identifies that a customer may present a high inherent risk of money laundering (as well as in other cases set out in the MLRs), Monzo must apply appropriate and risk based enhanced customer due diligence ("EDD") measures to manage and mitigate that heightened risk. This includes circumstances where Monzo has determined that a customer or potential customer is a politically exposed person ("PEP"), or a family member or known close associate of a PEP. The Authority published guidance in July 2017 which set an expectation that all firms should apply an individualised approach to each of these customers and where such a customer was a UK PEP, or a family member or close associate had no additional risk factors, then they should be treated as a lower risk customer to whom a lower level of EDD would apply.
- 4.10. Likewise, as an authorised firm, Monzo is required, amongst other things, to implement and maintain policies and procedures to identify, assess, monitor and manage its money laundering risk. Such controls must be appropriate to, amongst other factors, its size, product and service offering, geographical business locations and customer typologies.

### **Monzo's historical AML systems and controls**

#### *2016 AML Review*

- 4.11. In 2016 (i.e. prior to the Relevant Period when Monzo was still operating under restricted regulatory permissions), in advance of launching current account services, Monzo's AML policies and procedures were assessed by an external consultant (the "2016 AML Review"). In particular, the 2016 AML Review considered the adequacy of Monzo's policies in light of its proposed future business model and applicable AML rules and regulations. At that time, the external consultant found that Monzo's policies and procedures were "*adequate based on the size and complexity of the bank.*"

*The Authority's 2017 supervisory review*

4.12. In November 2017, the Authority's financial crime supervision team reviewed Monzo's AML and financial sanctions systems and controls. Subsequently, the Authority wrote to Monzo in December 2017 providing its high-level feedback on the review. While noting some positive elements, the Authority's feedback suggested areas of improvement within Monzo's financial crime control framework to be addressed as soon as practicable. The matters highlighted in the Authority's letter included, but were not limited to, the following:

- (1) limited evidence of Monzo seeking to understand, from the outset, the nature of its customer relationships including a failure to collect details on a customer's expected financial activity and obtain essential information to understand a customer's profile (without having information on customers expected activity, the Authority queried how Monzo could derive meaningful results from its transaction monitoring system);
- (2) insufficient clarity regarding both the risk rating ascribed to customers' at onboarding and the consequent level of due diligence required as well as a need for Monzo to develop a more "*holistic risk assessment*";
- (3) no provision for Monzo to conduct EDD on high-risk customers other than customers identified as PEPs or having high-risk third party links; and
- (4) evidence of Monzo's customers being able to transact prior to the completion of due diligence checks.

4.13. Monzo responded to the supervisory letter on 18 January 2018. The Firm explained that the Authority's feedback had been shared with its Board and that appropriate action was being taken. Amongst other things, Monzo's response asserted that:

- (1) Given the Authority's concerns, and as part of an ongoing commitment to review and enhance its processes, Monzo would revisit the balance between information it received when onboarding new customers and information gathered as part of its ongoing risk assessment;
- (2) Monzo performed CDD and EDD checks on all customers at onboarding before they could transact; and

- (3) Monzo labelled customers as high-risk for factors other than PEP status (Monzo cited the example of adverse media checks being run on all customers).

*Monzo's MLRO Function*

- 4.14. In October 2018 (i.e. the start of the Relevant Period), Monzo's MLRO departed the Firm. Thereafter, until April 2020, MLRO responsibilities were held on an interim basis by other senior staff members. In early 2020, Monzo's second line of defence produced an initial report which concluded that Monzo's financial crime framework was not fully effective. The report noted, as a primary issue, that the Firm's controls had onboarded too many customers about whom it had insufficient information, which had necessitated additional work in the form of investigations, reporting and customer exits.

*Skilled Person Review*

- 4.15. In June 2020, the Authority raised concerns about the adequacy of Monzo's financial crime risk management with a particular focus on the Firm's customer onboarding controls. Thereafter, on 14 August 2020, the Authority required Monzo to formally appoint a Skilled Person to undertake a full and substantive review of the state of financial crime risk management. Specifically, the Skilled Person was required to:

- (1) Assess the adequacy of the Firm's financial crime systems and controls and the adequacy of customer due diligence against the requirements of the MLRs and Authority's rules and guidance;
- (2) Provide recommendations for improvements to address any weaknesses in the Firm's plans to improve its financial crime systems and controls;
- (3) Undertake quality assurance testing of the Firm's remediation of impacted customer files and report on whether the due diligence undertaken for this purpose was appropriate and adequate;
- (4) Determine the adequacy of the Firm's plans to address any weaknesses in its financial crime systems and controls as identified by the Skilled Person; and
- (5) Test, evaluate and report on the Firm's implementation of the remediation work carried out in conjunction with its plans for improvement of its financial crime systems and controls.

- 4.16. As required by the Authority, the Skilled Person conducted its review and reported its findings on a phased basis. On 18 September 2020, the Skilled Person produced an initial report concluding that Monzo's CRA, CDD and EDD controls did not fully align with the MLRs and industry guidance in a number of key areas which required urgent resolution. On 14 December 2020, the Skilled Person produced a further report which, inter alia, assessed the effectiveness of Monzo's transaction monitoring systems and controls and provided a number of recommendations based on the findings documented in its initial report.
- 4.17. Thereafter, Monzo took steps to address the weaknesses identified across its financial crime controls, and the Skilled Person produced a series of reports on the steps taken. In August 2024, the Skilled Person produced a final report which recorded, among other matters, that all but one of its recommendations had been fully met and that, going forward, Monzo should be equipped to manage financial crime risk commensurate to the size scale and complexity of its business. The final recommendation was fully met shortly afterwards, in November 2024.

#### *Imposition of VREQ*

- 4.18. In tandem with the appointment of a Skilled Person and at the request of the Authority, Monzo voluntarily applied for requirements to be imposed upon how it carried out its business, with a particular focus on its onboarding of new customers. Accordingly, the Authority imposed the VREQ on Monzo's Part 4A permissions from 5 August 2020 (i.e. the first day of the Relevant VREQ Period).
- 4.19. In particular, the VREQ included the following requirement:
- "The Firm must not accept or process any new or additional account applications (whether for personal use, business use or otherwise) from new or existing high risk customers."*
- 4.20. In the absence of Monzo having a clear definition of high-risk customers, the VREQ included 19 sub-requirements defining specific activities and characteristics which Monzo was required to consider as high-risk factors. For certain sub-requirements, the VREQ required Monzo to take additional steps before deciding to onboard customers and ensure that its rationale for such onboarding decisions, along with relevant evidence, had been appropriately documented.
- 4.21. Following its implementation, the Authority kept the requirements of the VREQ under review in light of, amongst other matters, the Skilled Person's assessment

of Monzo's financial crime systems and controls. The VREQ remained in force until February 2025, subject to certain modifications. Such modifications included the Authority agreeing in December 2021 for Monzo to apply its updated customer risk assessment tool ("CRA") to 50% of new personal banking customer applications and from June 2023, to 100% of new personal banking applications.

- 4.22. On 26 February 2025, the Authority agreed to the immediate lifting of all remaining VREQ requirements. By that date, significant progress had been made by Monzo in relation to enhancing its financial crime controls.

*Authority's review of challenger banks financial crime controls following the Pre-VREQ Period*

- 4.23. In December 2020 (i.e. during the course of the Skilled Person's review and after the imposition of the VREQ), the NRA raised the risk that criminals may be attracted to the faster onboarding process offered by challenger banks when compared to traditional high street banks. In 2021, the Authority undertook a review of the financial crime controls at a sample of challenger banks, including Monzo. The findings of the review were published on 22 April 2022.
- 4.24. In May 2021, the Authority issued a "Dear CEO" letter to Monzo (and other relevant firms) summarising some of the common control failings it had identified during the course of its review. Within the letter, the Authority set out its expectation that Monzo complete a gap analysis against each of the common control failings and take steps to close any gaps identified.
- 4.25. Monzo, through its Financial Crime Compliance team ("FCC"), completed the gap analysis in September 2021. The work carried out by FCC culminated in 16 recommendations being made across the control areas covered by the Authority's review. These recommendations included making necessary enhancements to Monzo's CRA and EDD procedures to ensure compliance with the MLRs.

**Remediation and enhancement of financial crime framework**

- 4.26. In conjunction with the imposition of the VREQ and appointment of a Skilled Person, Monzo has worked to remediate and enhance its financial crime framework. This work has included:
- (1) Establishing and completing a Financial Crime Change Programme intended to fully resolve known weaknesses and incorporate the Skilled Person's

recommendations on areas including customer due diligence, customer risk assessments and transaction monitoring.

(2) Conducting a comprehensive back-book customer remediation exercise to collect required due diligence information from existing customers and exit relationships with customers falling outside of its risk appetite.

(3) A significant investment in its recruitment and resourcing of key financial crime roles across its first and second lines of defence. Between August 2020 and April 2021, Monzo significantly increased its headcount in its financial crime collective and financial crime compliance team, and saw an even greater increase in its financial crime team focused on customer operations.

4.27. The Authority acknowledges Monzo's commitment to ensuring, on an ongoing basis, that it has an effective financial crime framework in place.

#### **Monzo's assessment of Money Laundering Risk**

4.28. Pursuant to the MLRs, a firm must take appropriate steps to identify and assess the risks of money laundering (and terrorist financing) to which its business is subject. Such assessments must take into account risk factors relating to customers, countries or geographical areas of operation, products or services, transactions, and delivery channels.

4.29. Monzo assessed its business-wide exposure to financial crime risks, including money laundering risks, through its Financial Crime Risk Assessment ("FCRA"). Monzo finalised its first comprehensive FCRA in early 2020 and completed another in September 2020. The FCRA's stated purpose was to provide a "*baseline*" for assessing Monzo's risk profile over time across customers, products, geographies and channels.

4.30. The FCRA was comprised of, among other things, a risk scenario register which recorded and explained the relevance of the different financial crime risks faced by Monzo, a controls library which catalogued Monzo's existing controls and their assumed effectiveness, and individual risk assessments for each category of financial crime identified in the FCRA.

4.31. The financial crime category with the most comprehensive coverage in the 2020 FCRA was "*Money Laundering*". Monzo's risk scenario register and individual risk assessments recorded numerous actual and potential risks associated with customer activity and the relevant mitigating controls that Monzo had in place to

reduce those risks. The FCRA recorded that a significant number of these risks were managed and mitigated by Monzo's customer verification; CRA; CDD; EDD and PEP screening controls. The FCRA found that Monzo's controls, if operating effectively, would reduce the risk of potential money laundering being facilitated.

- 4.32. In addition, Monzo utilised an overarching risk appetite statement which was approved by the Monzo Board in May 2020 and articulated, among other matters, that it had low tolerance for financial crime and accepted that certain categories of customers were considered to be outside of its risk appetite. The risk appetite statement referred explicitly to Monzo's CRA and due diligence measures and controls processes (including EDD and PEP screening) for the purpose of understanding and evaluating customer risk and setting appropriate risk thresholds.

### **Customer Due Diligence (CDD)**

- 4.33. Under the MLRs, a core purpose of CDD is the identification and verification ("IDV") of a firm's customers and, where applicable, their beneficial owners. CDD also entails a requirement to appropriately obtain information on the purpose and intended nature of its business relationships and customers' transactions.
- 4.34. CDD was therefore crucial to Monzo's understanding, both initially and on an ongoing basis, of who its customers were, their financial behaviour and ultimately, the money laundering risk (and other financial crime risks) they presented. Relatedly, Monzo relied upon CDD measures to identify financial crime risks (including money laundering risk), not least for providing a basis for the Firm's customer monitoring activities.
- 4.35. Throughout the Pre-VREQ Period, Monzo's approach to CDD was inadequate as the Firm did not obtain, nor assess, any information to establish the purpose and intended nature of its customer relationships. Notably, the lack of customer information being gathered by Monzo had already been raised as an issue by the Authority in its December 2017 feedback letter. Specifically, the Authority referred to having seen "*limited evidence*" of the Firm seeking to understand the intended nature of customer relationships from the outset to determine more accurate customer risk ratings.
- 4.36. However, Monzo's CDD procedures did not require the Firm to obtain and assess information from its personal and business customers relating to the following key factors expressly set out in the MLRs, namely:

- (1) The purpose of an account, transaction or business relationship;
- (2) The level of assets to be deposited by a customer or the size of the transactions undertaken by the customer; and
- (3) The regularity and duration of the business relationship.

- 4.37. In specific regard to prospective business customers, up until August 2020, Monzo's CDD procedures did not provide, as required by the MLRs, for verification of the identity of all beneficial owners and PSCs. During the Relevant VREQ Period, Monzo carried out a remediation exercise to verify the identity of the beneficial owners and PSCs of existing business customers. Notably, the remediation exercise necessitated the identity verification of approximately 19,198 beneficial owners/PSCs which Monzo had not previously completed.
- 4.38. Furthermore, although required by the MLRs, during the Pre-VREQ Period, Monzo's business banking CDD procedures did not require the Firm to report to Companies House any material discrepancies between Companies House records and IDV information which Monzo had gathered from a prospective business customer.
- 4.39. Monzo's CDD processes also failed to incorporate reviews of existing customer records to ensure they remained up to date and did not define the circumstances where CDD measures would be re-applied to existing personal and business customers. These gaps meant the Firm could not comply with the MLRs nor its own internal requirement to repeat CDD measures on a risk-sensitive basis.

*Monzo's overall approach to CDD*

- 4.40. The Firm's more limited approach to CDD during a substantial part of the Pre-VREQ Period was driven by several factors. Firstly, the approach was built upon assumptions about the nature of Monzo's customers and products. In particular, the Firm assumed that its product range was ordinary and that its customers would use their accounts in the same way. Such assumptions conflicted with the Firm's actual knowledge of how customers were, at times, using their accounts. Indeed, Monzo's customer monitoring activities identified that customers were using their accounts in different ways, including as salary accounts, secondary accounts and travel accounts.
- 4.41. Secondly, the Firm's onboarding controls, including its CDD measures, entailed limited information gathering and assessment to facilitate customer onboarding



with minimal “*friction*” (i.e. minimal controls were applied to ensure that customers could be onboarded at speed and begin using the Firm’s products/services).

- 4.42. Thirdly, early in the Pre-VREQ Period, Monzo conducted a review to assess the sufficiency of the customer information it was gathering at onboarding. The review determined, subject to a number of “*caveats*”, that the information being gathered was sufficient and commensurate with Monzo’s “*assessed financial crime exposure*”. In addition, the review concluded that customers’ transactional behaviour and connections to other suspicious customers, rather than onboarding checks on their own, were more useful indicators of potential criminal activity.
- 4.43. The report highlighted that Monzo collected “*limited data*” when onboarding customers compared to more traditional banks, but that this was mitigated by its post-onboarding controls, particularly transaction monitoring rules. Further, the report expressly recorded that a number of specific findings were based upon reviews of “*small*” samples of customers and, moreover, that certain findings were worth revisiting or required further work, in order to draw more definitive conclusions.
- 4.44. As Monzo’s customer base and product range grew, subsequent internal reviews during the Pre-VREQ Period raised the need to obtain more information from customers prior to onboarding. For example:
- (1) In December 2018, a Monzo compliance monitoring report noted that information gathered by the Firm did not take into account the nature of the business relationship, which would become “*increasingly important*” as Monzo diversified its product offering. The same report recorded that Monzo gathered no information about customer occupation or planned account usage at the onboarding stage and that obtaining such information “*could help in assigning a more accurate risk rating*”;
- (2) A 2019 MLRO report recorded as a “*particular concern*” that Monzo was not asking how customers intended to use their current account at onboarding or using existing information to ascertain the purpose and nature of the business relationship. Importantly, the absence of information regarding intended account usage was seen as making it difficult to “*contextualise subsequent account activity*” as out of character or unusual (i.e. for transaction monitoring purposes);

(3) A 2019 compliance assurance report concluded Monzo's approach to assessing the nature of the customer's relationship constituted a "*regulatory breach*" and that no information was obtained regarding the intended nature for a customer having a current account.

- 4.45. Despite these findings, which pointed to repeated calls for Monzo's CDD processes needing to be augmented to capture information regarding customers' intended purpose and usage of their Monzo account, such information was not captured during the entirety of the pre-VREQ Period. Consequently, a customer file review exercise conducted by the Skilled Person (which assessed 18 personal banking customer files and 12 business customer files) found no evidence of Monzo having obtained any information regarding the intended purpose of accounts, expected activity or duration of the business relationship.

#### **Additional weaknesses in onboarding controls**

- 4.46. In addition to the flawed CDD process, certain other control weaknesses exacerbated the risk of Monzo onboarding and servicing customers outside of its financial crime risk appetite:

##### *Address verification*

- 4.47. During the Pre-VREQ Period, Monzo's IDV procedure involved Monzo obtaining and comparing a prospective customer's selfie video and date of birth with a photograph of a government-issued photo identification. Prospective customers were also subject to a "*2+2 check*" whereby Monzo obtained name, date of birth and residential address which was compared against data held by credit reference agencies. However, for almost all of the Pre-VREQ Period, to sign up for an account, customers were only required to successfully pass the selfie IDV procedure and not the 2+2 check.
- 4.48. The consequence of Monzo relying solely on its selfie IDV procedure for almost all of the Pre-VREQ Period was that address verification was not a requirement for onboarding a customer. This element had been withdrawn as an IDV control in early 2019 following Monzo concluding that it was not a reliable indicator of criminal propensity. Monzo made this decision having found that approximately "*20%*" of existing current account customers had previously failed the check. Notably, the Firm also found that "*47%*" of current account customers considered at the time to be higher risk, had failed address verification checks.

- 4.49. Monzo's risk appetite and business proposition were predicated on customers (both personal and business) having a legitimate UK address and "*only providing services to individuals residing within the UK*". Whilst the absence of address verification as an onboarding prerequisite for almost all of the Pre-VREQ Period was not contrary to prevailing guidance on the MLRs, it impacted the Firm's ability to ensure its business was aligned with its risk appetite.
- 4.50. Whilst Monzo's internal systems had been calibrated to only accept UK postcodes, the lack of independent address verification during almost all of the Pre-VREQ Period allowed customers to provide obviously implausible UK addresses when applying for an account, such as well-known London landmarks including "*Buckingham Palace*" and "*10 Downing Street*", and even Monzo's business address. Monzo's decision not to verify, or otherwise monitor, customer addresses also gave rise to other issues (all of which heightened the risk of Monzo having onboarded, and continued a business relationship with, non-UK resident customers outside of its risk appetite):
- (1) Customers using PO Box addresses, mail-forwarding addresses and addresses of customers who had been previously offboarded by Monzo;
  - (2) Customers providing invalid UK addresses containing non-UK details or foreign addresses with UK postcodes;
  - (3) Customers using a UK address when applying for an account and then subsequently re-ordering their account card to a non-UK address (sometimes in very short order); and
  - (4) Multiple customers using the same address in circumstances where Monzo had not fully assessed the risk of criminal activity (e.g. money muling).
- 4.51. These control weaknesses, and Monzo's resulting exposure to financial crime, were compounded by the fact that, for most of the Pre-VREQ Period, Monzo had promoted the lack of address verification on its website and online media channels. Furthermore, in that same period, Monzo offered its customers a "*Same day Monzo*" service whereby customers were able to transact before receiving their physical account card at the address provided at onboarding. By the end of the Pre-VREQ Period, Monzo held concerns that lack of address verification had impacted the number of customers accepted by Monzo intending to use the Firm for financial crime purposes. Monzo reincorporated address verification into its

IDV procedure in July 2020 and its same day Monzo service was reintroduced around the same time.

- 4.52. Further, in May 2020, Monzo submitted its annual Financial Crime Report to the Authority (a regulatory requirement under rule SUP 16.23.4R of the Handbook). The report required Monzo to provide, amongst other details, its total number of relationships with UK based customers. However, the combined lack of address verification and the above-mentioned monitoring issues led Monzo to “*doubt the accuracy of reporting all customers as UK customers*”. Consequently, the Firm submitted the report with an accompanying explanation to the Authority of its concerns with declaring all customers as UK based.

#### *CIFAS checks*

- 4.53. Members of CIFAS can check details against its databases for matches to individuals whose behaviour appears to be consistent with known fraudulent conduct. Whilst membership of CIFAS is not itself a regulatory requirement, CIFAS serves as a vital source of information, enabling firms to identify and manage customer risk in adherence to relevant UK AML guidelines and international standards of good practice. Relevant guidance on the MLRs cites CIFAS as a useful source of information in the context of IDV checks.
- 4.54. In August 2018, Monzo tested the benefits of CIFAS membership whereupon a random sample of 69,685 existing customers was screened against CIFAS’s National Fraud Database. The screening results revealed an overall match rate of 8.72%, which CIFAS classified as high risk. This was considered by CIFAS standards to be a “*high match rate*” and indicated that 8.72% of sampled customers had been flagged by other CIFAS members as posing a high financial crime risk.
- 4.55. In March 2020, Monzo’s Board gave approval for the Firm to become a member of CIFAS. Notably, the discussion drew attention to Monzo’s awareness, since 2018, that it would “*significantly benefit*” from joining CIFAS. Moreover, in the absence of CIFAS membership, Monzo’s ability to identify potential customers who had previously engaged in financial crime or fraud was significantly limited.
- 4.56. Monzo identified that 5,038 of the 69,685 sampled customers had been exited as outside of Monzo’s risk appetite. A significant percentage of the exited customers were positive matches in CIFAS’s database and Monzo acknowledged that, had it

been a member of CIFAS, it would have prevented those accounts from being opened and the associated operational costs and any incurred fraud losses.

- 4.57. CIFAS was implemented as an onboarding control in July 2020, in the form of Misuse of Facility ("MoF") checks. These checks are designed to identify the misuse of an account, policy or product by a genuine account holder for fraud purposes. The MoF checks were introduced as part of a suite of new onboarding controls following concerns raised by the Authority on the adequacy of Monzo's financial crime framework and customer onboarding controls.
- 4.58. In January 2021, Monzo produced a report titled "Fincrim Initial Customer Remediation Approach and Plan" ("Fincrim Customer Approach and Plan"). The report set out Monzo's strategy for reviewing its existing customer population to identify customers exhibiting specific risk factors which were outside of Monzo's risk appetite. The purpose of the plan was to allow Monzo to remediate its customer population in line with its new onboarding controls and assess whether customers should be retained or exited. Monzo prioritised customers who were solely flagged by the MoF check on the basis it was "*the most predictive risk indicator*".
- 4.59. Monzo's Fincrim Customer Approach and Plan from January 2021 recorded that approximately 53,600 customers, most of whom were onboarded in the Pre-VREQ Period, failed CIFAS screening. The Firm envisaged exiting its relationship with, and closing the accounts of, over half of those customers.

*Failure to identify duplicate users*

- 4.60. Throughout the Pre-VREQ Period, Monzo failed to implement effective controls to identify instances where customers were able to open multiple accounts. This was despite Monzo confirming to the Authority in July 2020 that duplicate user controls, which identified previously exited users or sign-ups from existing account holders, were in place.
- 4.61. The Skilled Person conducted tests of Monzo's controls in relation to duplicate users and in its findings, established that a population of 4,213 active customers had been onboarded more than once and 36 of these customers had been onboarded more than four times. In its September 2020 report, the Skilled Person highlighted 2 examples of customers who had previously been offboarded by Monzo for financial crime reasons, still having a current active account with a risk rating of "*No Risk Identified*".

- 4.62. In October 2020, Monzo undertook its own review of its duplicate user controls. The “Financial Crime Compliance Review of Duplicate User Controls” (“Fincrime Compliance Review”) determined its manual process for reviewing duplicate user flags was prone to human error and that quality assurance was not conducted on duplicate user tasks.

### **Customer Risk Assessment**

- 4.63. Customer risk assessments are required by the MLRs and should form a fundamental part of a firm’s business-wide assessment of the money laundering risks (among other risks) which they are subject to. A firm’s treatment of each of its customers, for the purposes of the MLRs, should depend upon an assessment of the money laundering risk which each customer presents.
- 4.64. Throughout the Pre-VREQ Period, Monzo’s CRA was insufficient to comprehensively assess its customers (both personal and business), pursuant to both the MLRs and its own risk appetite. Consequently, Monzo could not accurately determine the risks its customers posed and, relatedly, the appropriate level of ongoing monitoring and due diligence they required.
- 4.65. Monzo placed significant emphasis on the customer experience being streamlined and efficient. Consequently, limited initial information was gathered and evaluated during a substantial part of the Pre-VREQ Period and Monzo instead relied upon ongoing transaction monitoring processes, to help manage financial crime risks (see paragraphs 4.79 to 4.90 below). This was initially considered appropriate in light of Monzo’s product offerings and customer base, but became inadequate as Monzo’s product offerings and customer base grew over time.

### *Risk assessment of personal banking and business customers*

- 4.66. During the Pre-VREQ Period, the Firm’s documented approach to risk-assessing personal banking customers was based upon its IDV processes, adverse media searches, PEPs, Sanctions checks, EDD, duplicate user detection, source of wealth and source of funds reviews, and immigration and residency checks.
- 4.67. Monzo utilised four risk categories for the purpose of rating a prospective customer’s financial crime risk at the onboarding stage: No Identified Risk; Low Risk; Potential Risk and Likely Risk. However, Monzo’s procedures during the Pre-VREQ Period stipulated “*No Identified Risk*” as the “*default*” risk category to be applied at onboarding to all personal banking customers.

- 4.68. In relation to its personal banking customers, whilst the procedures outlined the corresponding level of suspicion for each risk category, Monzo gave no adequate guidance or methodology for assessing the risk factors stipulated by the MLRs (see paragraph 4.28 above) including the weightings to be given to each risk factor, in accordance with Monzo's risk appetite). The central cause of this was the lack of relevant data points captured and thus, not assessed, at onboarding.
- 4.69. In respect of personal banking customers, information pertaining to a customer's occupation, expected transactional activity and, for most of the Pre-VREQ Period, geographic location, did not feed into the CRA. For business customers, whilst country of residence and nationality data of directors and PSCs were factored into the CRA, insufficient information was assessed in regard to the customer's exposure to high-risk third countries or sanctioned countries in connection with its business activities. Moreover, given the lack of comprehensive verification of beneficial owners and PSCs (see paragraph 4.37 above), the CRA did not consider the full extent of business customers' links to high-risk industries/sectors.
- 4.70. The only risk factors expressly stipulated to be applied for the purpose of risk-rating personal banking customers at onboarding during the Pre-VREQ Period were PEP exposure and adverse media concerns. However, at times during the Pre-VREQ Period, Monzo would not review adverse media hits identified for a personal banking customer unless another risk factor (a PEP flag or subsequent transaction monitoring alert) was also identified. This decision was based upon Monzo's screening process producing a high rate of "*false-positives*" and notwithstanding the Firm's documented awareness of a risk that potentially serious adverse media was not always being considered, both initially and during the customer relationship, when assessing customer risk in relation to its personal banking customers.
- 4.71. Separate customer file reviews undertaken by the Skilled Person and the Authority identified a small number of examples of adverse media screening not being assessed as part of the CRA.
- 4.72. In consequence of the limitations to Monzo's CRA during the Pre-VREQ Period the majority of personal banking customers were categorised with the financial crime risk rating of "*No Identified Risk*". This painted a misleading picture of the risk of financial crime which the bank could have been exposed to in relation to the MLRs' inherent risk factors and, in turn, the robustness of Monzo's financial crime framework in 2020.

- 4.73. Moreover, Monzo was unable to determine the appropriate levels of CDD, EDD and ongoing monitoring to be applied during the customer lifecycle to ensure customers remained within its risk appetite.
- 4.74. By the end of the Pre-VREQ Period, external data referred to in an internal Monzo document indicated that the Firm was the recipient bank for a higher proportion of fraudulent transactions reported to the external data provider by participating firms, relative to the proportion of UK current accounts it operated for customers.

*Awareness of CRA information shortcomings*

- 4.75. Throughout the Pre-VREQ Period, Monzo recognised the limitations of the CRA and its failure to capture and consider certain customer information which was required by the MLRs and/or highly relevant to its risk appetite. Critical observations recorded during the Pre-VREQ Period within internal Monzo documents regarding the CRA included:
- (1) Although Monzo was unable to determine exactly how other UK banks used information collected from customers at onboarding, it became clear that, during the Pre-VREQ Period, Monzo may have collected less information from customers at onboarding for the purpose of its CRA. In particular, Monzo considered it fair to assume that other banks designated information such as employment status, expected account turnover and geographical location as higher risk criteria in their customer risk assessments;
  - (2) Notwithstanding non-UK based customers fell outside of its risk appetite, Monzo's CRA did not consider the potential of non-UK based customers seeking to open a current account.
  - (3) Relevant data which Monzo did gather at onboarding (e.g. tax residency, ID type, IP address and adverse media) was not utilised when making decisions about customer risk.
  - (4) Concerns that the Business Banking CRA needed refinement given the need to distinguish customers operating in the same industry with different risk profiles, to collect greater detail around the nature and purpose of the business account and following "*higher than expected*" business customers rated low risk being identified with suspicious activity.
  - (5) Limitations in the onboarding controls were recognised but risks arising from the low number of customers assessed as high-risk were considered to have



been mitigated by transaction monitoring rules. However, Monzo also considered that reliance on behavioural information in the absence of a robust CRA gave rise to operational challenges and risked the Firm being less effective at detecting certain crime types.

- 4.76. Accordingly, during the Pre-VREQ Period, Monzo was aware that the information shortcomings of the CRA risked the Firm onboarding customers that it did not know enough about and could not effectively risk-assess.
- 4.77. Notably, in early 2022, Monzo completed an "*Initial Remediation*" exercise to identify customers exhibiting specific risk factors outside of its risk appetite. Monzo considered both pre-onboarding and post-onboarding risk factors and behaviours. Monzo reviewed 217,000 customers for the purpose of this exercise which led to the Firm exiting 44,163 customers, equating to just under 1% of Monzo's entire banking population. Previously, in 2021, Monzo carried out a "*High Risk Customer Remediation*" exercise following enhancements being made to Monzo's EDD procedure. Of the 449 high-risk business banking customers reviewed by Monzo, 326 were exited (equating to just over 0.5% of Monzo's entire business banking population) and nine downgraded to a lower risk rating.
- 4.78. In view of the results of Monzo's back-book customer remediation during the Relevant VREQ Period, the Authority considers that the risk of Monzo having insufficient knowledge about its customer base to conduct effective risk assessments became apparent.

### **Transaction Monitoring**

- 4.79. During the Pre-VREQ Period, Monzo placed significant reliance on transaction monitoring to manage financial crime risks including for the purpose of determining, and making subsequent adjustments to, customer risk ratings applied at onboarding.
- 4.80. As Monzo grew and expanded its product offering during the Pre-VREQ Period, the Firm relied upon transaction monitoring as one of the primary means of managing customer risk. Furthermore, Monzo relied upon transaction monitoring as a means of mitigating some of the recognised limits of its onboarding controls.
- 4.81. This meant that customer risk was predominantly considered in response to post-onboarding events, such as transaction monitoring alerts. Over the course of the relationship with the customer, Monzo's customer operations team was permitted

to manually adjust a customer's default risk score from "*No Identified Risk*" to a higher score based on any risk factors that were identified.

- 4.82. Monzo's transaction monitoring systems were based upon a number of data points, in particular, the size, amount, number and type of transactions carried out by a customer. However, the limitations in Monzo's approach to CDD and customer risk assessment at onboarding impeded the Firm's ability to accurately determine, from the outset of a relationship, customers expected transactional activity and therefore, the types of transactions to be treated as suspicious or unusual.
- 4.83. In particular, Monzo's failure to collect key customer information including occupation, the nature and purpose of the account, source of wealth and source of funds impacted any subsequent assessment as to whether customer transactions were suspicious. Furthermore, Monzo's ability to subject high risk customers' transactions to more enhanced monitoring was limited, given very few transaction monitoring rules actually utilised customer risk ratings.
- 4.84. In late 2019, Monzo engaged a third-party to review the design, adequacy and operational effectiveness of its AML transaction monitoring systems. The third-party review identified a wide range of issues, including:
- (1) a lack of clarity and documentary evidence of the responsibilities and reporting structure surrounding Monzo's transaction monitoring;
  - (2) limited industry-based experience within Monzo's AML management team;
  - (3) insufficiently experienced or trained staff performing key transaction monitoring tasks without sufficient guidance;
  - (4) unclear linkage between transaction monitoring rules and Monzo's money laundering risk appetite;
  - (5) there had been no independent compliance review of Monzo's transaction monitoring for 2019;
  - (6) a material number of "*false positive*" alerts had been identified but there was no recalibration of the alerts system or threshold to reduce their occurrence;
  - (7) no procedure or guidance document existed which explained how transaction monitoring alerts should be investigated; and

(8) limited quality assurance review of frontline staff's rationale for deciding whether a relevant transaction was suspicious or not.

- 4.85. In regard to determining whether a given transaction was suspicious and the appropriate customer risk rating, the third-party found that risk ratings were not properly defined, meaning Monzo's operations team would have to make a subjective assessment when allocating a risk rating. Relatedly, members of the operations teams had discretion when allocating a risk rating and such decisions were not tracked to any form of risk matrix or framework. Without sufficient guidance being available, the third-party considered that inappropriate risk ratings might be allocated by Monzo staff, potentially resulting in failures to identify money laundering risks.
- 4.86. Subsequently, in late 2020, the Skilled Person undertook a separate evaluation of Monzo's transaction monitoring policies and procedures. The Skilled Person found that Monzo's relevant documentation failed to provide sufficient guidance on several key areas including the appropriate weighting to give to the various data points referred to when assessing transaction monitoring alerts, the use of external sources to support alert assessments (although it noted that Monzo had a number of internal sources that could be used) and maintaining an audit trail of manual investigations of alerts (although noting Monzo maintained requirements for a clear audit trail for the review and investigation into automated alerts).
- 4.87. While the Skilled Person noted that Monzo's transaction monitoring rules operated as Monzo intended, the Skilled Person also identified, as a key deficiency, that Monzo's systems did not flag or record the specific transaction(s) which triggered transaction monitoring alerts. Consequently, reviewers were expected to identify the alerting transactions themselves and had no starting point or context to assist their reviews.
- 4.88. The Skilled Person also highlighted that Monzo permitted reviewers to close alerts as "Undecided" i.e. (where a staff member was unable to articulate clear suspicion of financial crime but can identify unusual activity or cause for concern in the account). This was despite the high number of undecided alerts being flagged in Monzo internal reports (for example, in the first half of 2019, Monzo recorded that 45% of transaction monitoring alerts were undecided).
- 4.89. Where alerts were closed by reviewers as "Undecided", rather than escalated for further review (albeit some were escalated), this increased the potential risk of

money laundering (or other financial crime) going undetected and/or unreported by the Firm.

4.90. The Skilled Person evaluated the effectiveness of the Firm's handling of transaction monitoring alerts by reviewing a sample of alerts which were not escalated further by Monzo. The 30 cases comprised 20 alerts automatically generated by Monzo's systems and a further ten cases which were raised through manual referral or another form of investigation. The Skilled Person disagreed with the outcome of 14 of the 30 cases. The Skilled Person's review included the following specific findings:

- (1) Of the 14 alert cases which the Skilled Person disagreed with, five cases were "Undecided" when they could have been closed as either "true" or "false" positive;
- (2) A further eight cases had not been adequately considered and could have been closed as "true" positive and further escalated; and
- (3) In seven out of the 20 automated alert cases, the reviewer had failed to address the alerting transactions as part of their decision.

#### **Enhanced Due Diligence and Treatment of PEP's**

4.91. EDD controls represent a necessary requirement for an effective risk-based approach to checking and monitoring higher-risk customers, transactions or situations, including:

- (1) customers linked to higher-risk countries or business sectors;
- (2) transactions that are either large, complex, unusual, or lack an economic or lawful purpose;
- (3) where the customer is not present; and
- (4) PEPs.

4.92. In accordance with the MLRs, the Authority expects firms to apply a risk sensitive approach to identifying PEPs and then to apply appropriate EDD measures. Importantly, firms must undertake risk assessments of PEPs on an individual basis rather than applying a generic approach. A firm's assessment and its decision to apply relevant EDD measures needs to be clearly documented. In July 2017 (i.e.

prior to the Relevant Period), the Authority issued finalised guidance to clarify these core requirements.

#### *EDD procedure*

- 4.93. Monzo's EDD controls should have allowed it to effectively understand who its higher-risk customers were, their financial behaviour, and what kind of money laundering or terrorist financing risk they presented.
- 4.94. During the Pre-VREQ Period, the procedure Monzo had in place for undertaking EDD on personal banking customers mainly entailed the selfie IDV procedure and duplicate user detection.
- 4.95. The coverage of Monzo's EDD procedure for personal banking customers was inadequate given, aside from PEP relationships, it did not describe the circumstances in which the Firm would be required to apply EDD. Such circumstances are set out in the MLRs and are not limited to where a customer or potential customer is a PEP. They include, for example, cases where a particular transaction is complex or unusually large.
- 4.96. Moreover, the procedure did not provide for how, when and where an EDD review needed to be documented. The Skilled Person's review of nine higher risk personal banking customer files found no evidence of EDD measures having ever been carried out either at the outset or during the course of each customer relationship.
- 4.97. In respect of business customers, the procedure was more comprehensive but still contained no direct reference on the need to apply EDD when the business customer was established in a high-risk country nor the measures to apply where high risk transactions were identified. This was a material omission from Monzo's EDD procedure in view of the Firm's risk appetite in respect of overseas personal and business customers. The Skilled Person's review of five higher risk business customer files found no evidence of EDD measures having ever been carried out either at the outset or during the course of each customer relationship.

#### *Treatment of PEPs*

- 4.98. During the Pre-VREQ Period, Monzo used a third-party provider to identify PEPs and potential PEPs at the onboarding stage and on an ongoing basis. The third party would categorise and risk-rate PEPs based upon information such as their country, position, seniority and corruption risk. Thereafter, Monzo would use the information provided by the third party and undertake its own searches to confirm

the status of the PEP and apply a risk assessment. In accordance with regulatory requirements, approval would then be sought from senior management for establishing or continuing the business relationship with the PEP. The resulting PEP status and risk-rating ascribed to the customer informed the level of ongoing monitoring to be applied (e.g. by necessitating more targeted transaction monitoring).

- 4.99. Monzo did not have its own internal definition of the categories of customer that amounted to PEPs for the purpose of identifying them but had understood that the third-party provider had utilised a definition articulated by the Authority. This meant that the Firm had no means to consistently and independently adjudicate the various types of PEP alerts. Further, at times, the lack of an internal definition risked PEPs or their associates not being properly identified before being onboarded as customers. Whilst the Skilled Person considered that the lack of an internal definition for PEPs did not constitute a regulatory breach, it was an area that Monzo needed to enhance to strengthen controls relating to the identification of PEPs.
- 4.100. At times, there was a backlog in Monzo's adjudication of PEP flag reviews and concerns were raised internally that staff were being tasked with performing such reviews without sufficient guidance. Although all PEPs were subject to tighter thresholds on behaviour triggers regardless of their review status, the true extent of Monzo's PEP relationships was also potentially misunderstood, given potential or "*low risk*" PEPs would not be reviewed to determine their true PEP status in the absence of a transaction monitoring alert.
- 4.101. Furthermore, Monzo's procedure for accepting PEPs was insufficient in that it provided for a PEP's source of wealth and source of fund details to be obtained after they had begun transacting. This element of the procedure presented a potential financial crime risk.
- 4.102. From June 2020 through to the end of the Pre-VREQ Period, due to the lack of adequate controls in how PEPs were being onboarded and managed, Monzo ceased to onboard PEPs, their relatives and/or close associates and by early 2021, Monzo had made progress in resolving these issues including undertaking a remediation exercise in respect of its existing PEP relationships. Of the 461 PEP relationships under review, 66 relationships were exited as a result of being outside of Monzo's risk appetite and 145 had their PEP labels removed on the basis that they never met the definition from the outset.

## **Breaches of the VREQ**

- 4.103. When the Authority imposes a requirement on an authorised firm's permission to carry on regulated activities, the firm must correctly implement all necessary changes to its systems and controls to ensure that the terms of the requirement are met immediately and on an ongoing basis, until the requirement is varied or cancelled by the Authority.
- 4.104. As detailed above (see paragraphs 4.18 to 4.22), from 5 August 2020, Monzo's permissions were made subject to the VREQ which included a requirement not to accept or process additional account applications from customers defined by the VREQ as high-risk. The VREQ contained 19 sub-requirements for the purpose of Monzo defining a high-risk customer.
- 4.105. During the VREQ Period, Monzo breached the VREQ by accepting or processing new or additional account applications for high-risk customers. In total, Monzo opened 26,325 accounts for high-risk customers in breach of the VREQ.
- 4.106. The VREQ breaches which led to Monzo accepting or processing new or additional account applications for high-risk customers resulted from a combination of technical flaws in the Firm's implementation of controls to comply with the VREQ ("VREQ controls") as well as instances of human error when applying those controls. The breaches arising from Monzo's control failings, and which led to the onboarding of high-risk customers, included but were not limited to:
- (1) Monzo failing to apply its VREQ controls to account applications already in progress prior to the VREQ Period;
  - (2) Monzo accepting account applications associated with certain addresses defined by the VREQ as making a customer high-risk;
  - (3) Monzo accepting account applications linked to devices already associated with at least two other customers; and
  - (4) Monzo accepting business account applications without properly assessing the industry risk posed by the underlying business customers.
- 4.107. Monzo also failed to comply with other VREQ requirements obliging the Firm to take additional steps and appropriately document its decision-making before onboarding certain prospective customers. Monzo's breaches in this regard impacted a further 6,714 customer accounts.

### **Non-application of the VREQ**

- 4.108. Separately, at times during the VREQ Period, Monzo failed to apply certain of its VREQ controls to new or additional account applications and at times applied its VREQ controls to incorrect information, including but not limited to when the Firm:
- (1) processed account applications already in progress prior to the VREQ Period;
  - (2) reopened accounts for customers; and
  - (3) onboarded customers aged under 18 years.
- 4.109. A number of these instances of non-application and/or misapplication of VREQ controls coincided with one or more of Monzo's VREQ breaches and were therefore causative of high-risk customers being inappropriately onboarded. Monzo estimates that these instances were connected to 167,444 accounts opened during the VREQ Period. Further, the Firm estimates that these instances may have led to the onboarding of 34,262 high-risk customers.

### **2021 Internal Review of VREQ Breaches**

- 4.110. In February 2021, after reporting its first breach of the VREQ, Monzo wrote to the Authority explaining that it had not identified any systemic issues and was confident that robust onboarding controls were in place. The Firm stated that additional ongoing oversight (including at the senior management level) had been implemented to ensure its continued compliance with the VREQ requirements.
- 4.111. In June 2021, following further breaches of the VREQ, Monzo committed to a "*top-to-bottom*" review of its implementation of the VREQ, undertaking a search for any additional VREQ breaches and putting in place comprehensive testing of its VREQ controls.
- 4.112. The main purpose of the internal review was to ensure that the Firm's VREQ controls had been appropriately implemented to satisfy each VREQ requirement. On 6 September 2021, Monzo provided the Authority with the outcome of the review, which had identified further issues, the majority of which had resulted in additional VREQ breaches.
- 4.113. On the 28 October 2021, the Authority wrote to Monzo highlighting significant concerns in relation to the scale and seriousness of the VREQ breaches which were identified by the Firm.



- 4.114. The Authority therefore requested Monzo to conduct a full review and assessment of the root causes of the implementation weaknesses in the VREQ controls, including the existence of cultural issues and lack of assurance.

#### **Legal Firm Review of VREQ breaches**

- 4.115. On the 8 November 2021, Monzo communicated to the Authority that it would be instructing a Legal Firm to undertake an independent review of the root causes and implementation issues which had led to the VREQ breaches ("the Legal Firm Review").
- 4.116. Thereafter, on 1 February 2022, Monzo provided the Authority with details of the outcome of the Legal Firm Review. Monzo explained that, in the Legal Firm's view, the overarching root cause of the VREQ breaches was that Monzo had applied an *"insufficiently robust governance framework to manage the implementation and operation of the VREQ."* The absence of a robust governance framework had a number of *"knock-on consequences"* identified by the Legal Firm.
- 4.117. In particular, it was unclear at times who within Monzo was accountable for different aspects of the VREQ's implementation. Certain key employees were not aware of the VREQ including its regulatory significance and limited specialist staff had been available to work on implementing the VREQ controls.
- 4.118. Furthermore, given the speed at which the VREQ was implemented, Monzo should have had more discussion with staff responsible for its implementation to understand what was achievable in the timeframe and better engage with the Authority. The Legal Firm considered Monzo should have sought more clarification from the Authority at an earlier stage about certain provisions of the VREQ rather than solely relying upon its own internal interpretations.
- 4.119. The effectiveness of any testing and assurance work which had been undertaken by Monzo was severely impacted by the speed at which the VREQ was implemented, a lack of clarity within Monzo regarding the VREQ's requirements and a lack of awareness by key employees, including those responsible for testing and assurance, that the VREQ controls needed to meet those requirements.
- 4.120. Significantly, the Authority had written to Monzo in January 2021 emphasising the importance of the VREQ and the expectation that Monzo should have sought advice from the Authority in circumstances where there was a lack of clarity around the wording of specific parts of the VREQ.

- 4.121. The Legal Firm also found that Monzo had taken some time to identify additional VREQ breaches and it was not until the VREQ breaches impacted a larger population of customers that Monzo undertook a more in-depth analysis and testing of the VREQ controls (which identified the additional breaches reported to the Authority on 6 September 2021).
- 4.122. The Legal Firm's review resulted in 7 proposed management actions. On the 31 January 2023, Monzo wrote to the Authority to confirm that 6 of the 7 management actions had been completed and embedded. Subsequently, on 13 April 2023, Monzo further updated the Authority that the final management action had been completed.

## **5. FAILINGS**

- 5.1. The regulatory provisions relevant to this Notice are referred to in Annex A.

### **Principle 3 breaches**

- 5.2. Principle 3 of the Principles requires that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
- 5.3. On the basis of the facts and matters described in paragraphs 4.1 to 4.102, the Authority considers that Monzo breached Principle 3 in the Pre-VREQ Period because it failed to take reasonable care to organise and control its systems and controls for managing the risk of financial crime (in particular in connection with customer onboarding) responsibly and effectively. In reaching this view, the Authority has taken account of the following:
- (1) During parts of the Pre-VREQ Period, Monzo's approach to undertaking CDD at onboarding was inadequate as the Firm did not always obtain and/or assess, sufficient information about prospective customers (particularly information which would enable it to establish the purpose and nature of its customer relationships);
  - (2) From late 2018 until the end of the Pre-VREQ Period, Monzo had no process in place for the purpose of verifying personal banking customer addresses (both initially and on an ongoing basis) in order to ensure that Monzo's customer base was aligned with its risk appetite;
  - (3) Monzo's IDV controls in respect of business customers were inadequate in that they failed to provide for the verification of all beneficial owners and PSCs;

- (4) Monzo's CRA was inadequate in terms of both scope and methodology which meant the Firm could not accurately articulate how many of its customers were high-risk and determine appropriate actions (e.g. undertake EDD on the customer, or decline/exit the customer);
- (5) Monzo's approach to managing financial crime risks relied upon transaction monitoring systems in circumstances where they were unable to readily identify suspicious/unusual activity and themselves included weaknesses (particularly in regard to the handling of transaction monitoring alerts);
- (6) Monzo lacked a clear process for applying and documenting EDD on high-risk customers other than PEPs (particularly customers established in a high-risk country); and
- (7) Monzo's process for applying EDD on PEPs was inadequate.

#### **Breach of the VREQ**

- 5.4. The requirements in the VREQ were imposed by the Authority under section 55L(5)(a) of the Act. By virtue of section 204A of the Act, they are therefore 'relevant requirements' in respect of a contravention of which the Authority is entitled to take action.
- 5.5. On the basis of the facts and matters set out in paragraphs 4.103 to 4.122, the Authority considers that Monzo contravened relevant requirements imposed upon it in the Relevant VREQ Period, in that:
  - (1) The VREQ required that Monzo *"must not accept or process any new or additional account applications (whether for personal use, business use or otherwise) from new or existing high-risk customers"*.
  - (2) The VREQ included 19 sub-requirements for the purpose of defining "high risk" persons and a further four associated requirements.
  - (3) Monzo opened 33,039 accounts in breach of the VREQ, 26,325 of these accounts were opened for high-risk customers during the Relevant VREQ Period (see paragraph 4.105 above) and a further 6,714 customer accounts were opened without Monzo first taking appropriate steps and documenting its decision-making as required by the VREQ (see paragraph 4.107 above).

- (4) Furthermore, Monzo estimates that 34,262 high-risk customers were onboarded as a result of Monzo failing to apply certain of its VREQ controls to new or additional account applications and at times applied its VREQ controls to incorrect information (see paragraph 4.109 above).

## **6. SANCTION**

- 6.1. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

### **Step 1: disgorgement**

- 6.2. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.
- 6.3. The Authority has not identified any financial benefit that Monzo derived directly from its breach.
- 6.4. Step 1 is therefore 0.

### **Step 2: the seriousness of the breach**

- 6.5. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area. The Authority considers that the revenue generated by Monzo is indicative of the harm or potential harm caused by its breach.
- 6.6. The Authority has therefore determined a figure based on a percentage of Monzo's relevant revenue as it relates to each of the breaches identified. Monzo's relevant revenue is the revenue derived by Monzo during the period of the breaches. This revenue comprises revenue earned from the relevant business areas in respect of the Pre-VREQ Period and all revenue earned during the Relevant VREQ Period from the population of accounts where Monzo either failed to comply with the requirements of the VREQ or failed to apply its VREQ controls correctly.

- 6.7. The Authority considers Monzo's relevant revenue for each of the breaches to be:
- (1) £107,362,365 in respect of the Pre-VREQ Period; and
  - (2) £4,473,612 in respect of the Relevant VREQ Period.
- 6.8. The total relevant revenue is therefore £111,835,977.
- 6.9. In deciding on the percentage of the relevant revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach; the more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels:
- Level 1 – 0%
  - Level 2 – 5%
  - Level 3 – 10%
  - Level 4 – 15%
  - Level 5 – 20%
- 6.10. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. DEPP 6.5A.2G(11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:
- (1) the breaches revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business; and
  - (2) the breaches created a significant risk that financial crime would be facilitated, occasioned or otherwise occur.
- 6.11. DEPP 6.5A.2G(12) lists factors likely to be considered 'level 1, 2 or 3 factors'. Of these, the Authority considers the following factor to be relevant:
- (1) the breaches were committed negligently or inadvertently.

6.12. Taking all of these factors into account, the Authority considers the seriousness of each of the breaches to be level 4 and so the Step 2 figure is 15% of £111,835,977.

6.13. Step 2 is therefore £16,775,396. This comprises:

(1) £16,104,354 in respect of the Pre-VREQ Period; and

(2) £671,042 in respect of the Relevant VREQ Period.

### **Step 3: aggravating and mitigating factors**

6.14. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

6.15. The Authority considers the following factors aggravate the breach:

(1) The Authority has published written guidance to remind firms of the importance of having robust systems and controls in place to ensure compliance with regulatory requirements.

(2) The Authority has also published a number of notices against firms for AML weaknesses both before and during the Relevant Period, including in respect of Standard Bank Plc on 22 January 2014, Barclays Bank Plc on 25 November 2015 and Deutsche Bank AG on 30 January 2017.

(3) In December 2017 (i.e. prior to the Relevant Period), the Authority sent Monzo a supervisory feedback letter raising high-level feedback and suggested areas for improvement concerning with the Firm's financial crime systems and controls (including not collating all required customer information at onboarding and having an unclear application of CDD and EDD to customers).

6.16. Monzo was accordingly aware, or ought to have been aware, of the importance of establishing, implementing and maintaining adequate AML systems and controls.

6.17. The Authority considers that the following factors mitigate the breach:

(1) Monzo has taken remedial steps in respect of its financial crime framework, implementing a financial crime remediation programme following the reviews

carried out by the Skilled Person. This has included investing significantly in additional resource and capability to manage financial crime risk.

6.18. Having taken into account these factors, the Authority considers that the Step 2 figure should be increased by 20%.

6.19. The Step 3 figure is therefore £20,130,475. This comprises:

(1) £19,325,225 in respect of the Pre-VREQ Period; and

(2) £805,250 in respect of the Relevant VREQ Period.

#### **Step 4: adjustment for deterrence**

6.20. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.21. The Authority considers that the Step 3 figure of £19,325,225, relating to the Pre-VREQ Period, represents a sufficient deterrent to Monzo and others and so has not increased this figure at Step 4.

6.22. However, the Authority considers that the Step 3 figure of £805,250, relating to the Relevant VREQ Period, is insufficient to meet its objective of credible deterrence: there is a risk that, in the absence of an increase to the penalty for the Relevant VREQ Period, similar breaches will be committed by the Firm or other firms in the future and the likelihood of detection of such a breach is low.

6.23. In making this assessment, the Authority has considered the following:

(1) the size and financial resources of the Firm;

(2) combatting financial crime is one of the Authority's key priorities;

(3) banking is a regulated activity which, by its nature, presents significant financial crime risks in the absence of robust controls - the VREQ was intended to reduce the financial crime risks associated with Monzo's business while work to remediate its financial crime controls was ongoing;

(4) the number and duration of the breaches, as well as the number of high-risk customers onboarded as a result of breaches of the VREQ significantly limited

the effectiveness of the VREQ as a tool to reduce the financial crime risks associated with Monzo's business;

- (5) since the terms of the VREQ were known to Monzo in advance of its imposition, the Authority was entitled to rely upon Monzo to ensure compliance with the terms of the VREQ;
  - (6) a failure to impose a significant penalty for breaches of this nature may cause firms to consider that compliance with requirements of the same type as the VREQ are of less significance than other requirements;
  - (7) a failure to impose a significant penalty for breaching requirements which impose restrictions on a firm's business may cause firms to consider that the financial advantages of growing their businesses outweigh the risks of breaching the requirements; and
  - (8) the Authority is generally reliant on firms to ensure their own compliance with requirements which, by agreement, impose business restrictions, meaning that, in the absence of firms putting in place robust measures to ensure compliance, breaches are likely to be undetected.
- 6.24. The Authority considers that it was imperative for Monzo to adhere to the terms of the VREQ to mitigate the financial crime risks posed by high-risk customers, while it remediated its financial crime systems and controls. VREQs of this type are an important supervisory tool used by the Authority and failures to comply with them are of significant importance.
- 6.25. The Authority therefore considers that, in order to achieve credible deterrence, the Step 3 figure in respect of the Relevant VREQ Period should be increased by £10,000,000.
- 6.26. The Step 4 figure is therefore £30,130,475. This comprises:
- (1) £19,325,225 in respect of the Pre-VREQ Period; and
  - (2) £10,805,250 in respect of the Relevant VREQ Period.

#### **Step 5: settlement discount**

- 6.27. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have



been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement.

- 6.28. The Authority and Monzo reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure. Step 5 is therefore £21,091,300.

### **Penalty**

- 6.29. The Authority therefore imposes a total financial penalty of £21,091,300 on Monzo for breaching Principle 3 and contravening the VREQ.

## **7. PROCEDURAL MATTERS**

- 7.1. This Notice is given to Monzo under, and in accordance with, section 390 of the Act.

### **Decision maker**

- 7.2. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

### **Manner and time for payment**

- 7.3. The financial penalty must be paid in full by Monzo to the Authority no later than 21 July 2025.

### **If the financial penalty is not paid**

- 7.4. If all or any of the financial penalty is outstanding on 22 July 2025, the Authority may recover the outstanding amount as a debt owed by Monzo and due to the Authority.

### **Publicity**

- 7.5. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this Notice relates. Under those provisions, the Authority must publish such information about the matter to which this Notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to Monzo, prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

- 7.6. The Authority intends to publish such information about the matter to which this Notice relates as it considers appropriate.

**Authority contacts**

- 7.7. For more information concerning this matter generally, contact Anthony Williams or Calum Duncan at the Authority (email: [anthony.williams@fca.org.uk](mailto:anthony.williams@fca.org.uk) / [calum.duncan@fca.org.uk](mailto:calum.duncan@fca.org.uk)).

Dharmesh Gadhavi

Head of Department

Enforcement and Market Oversight Division

## **ANNEX A**

### **RELEVANT STATUTORY AND REGULATORY PROVISIONS**

#### **1. Relevant Statutory Provisions**

*The Financial Services and Markets Act 2000*

- 1.1. In discharging its general functions, the Authority must, so far as reasonably possible, act in a way which is compatible with its strategic objective and advances one or more of its operational objectives (section 1B(1) of the Act). The Authority's strategic objective is ensuring that the relevant markets function well (section 1B of the Act). The Authority has three operational objectives (section 1B(3) of the Act).
- 1.2. The Authority's statutory objectives, set out in section 1B(3) of the Act, include the objective of the integrity objective which is protecting and enhancing the integrity of the UKs financial system. The integrity of the UK financial system includes it not being used for a purpose connected with financial crime.
- 1.3. Principally of the Authority's operational objectives, the integrity objective (section 1D of the Act), is relevant to this matter. Section 1D of the Act states:

*"The integrity objective is: protecting and enhancing the integrity of the UK financial system.*

*The integrity of the UK financial system includes –*

- a) Its soundness, stability and resilience,*
- b) its not being used for a purpose connected with financial crime,*
- c) its not being affected by contraventions by persons of Article 14 (prohibition of insider dealing and of unlawful disclosure of inside information) or Article 15 (prohibition of market manipulation) of the market abuse regulation,*
- d) the orderly operation of the financial markets, and*
- e) the transparency of the price formation process in those markets."*

- 1.4. Section 55L(5)(a) of the Act states:

*"The FCA may, on the application of an authorised person with a Part 4A permission-*

- a) impose a new requirement[....]"*

1.5. Section 204A of the Act states:

*"(1) The following definitions apply for the purposes of this Part.*

*(2) 'Relevant requirement' means a requirement imposed-*

*a) by or under this Act"*

1.6. Section 206(1) of the Act provides:

*"If the [Authority] considers that an authorised person has contravened [a relevant requirement imposed on the person,] it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate."*

## **RELEVANT REGULATORY PROVISIONS**

1.7. The relevant regulatory provisions as they were in force during the Relevant Period are set out below.

### *Principles for Businesses*

1.8. The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook. They derive their authority from the Authority's rule-making powers set out in the Act. The relevant Principles are as follows.

1.9. Principle 3 provides:

*"A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."*

### *DEPP*

1.10. Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act.