FINAL NOTICE

To: **CB Payments Ltd**

Reference Number: **900635**

Address: **The Scalpel**
18th Floor
52 Lime Street
London
EC3M 7AF

Date: **23 July 2024**

1. ACTION

1.1. For the reasons given in this Final Notice, the Authority hereby imposes on CB Payments Ltd ("CBPL") a financial penalty of £3,503,546 pursuant to regulation 51(1)(a) of the Electronic Money Regulations 2011 (the "EMRs").

1.2 CBPL 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 £5,003,646 on CBPL.

2. SUMMARY OF REASONS

2.1. CBPL is an Authorised Electronic Money Institution ("AEMI"), with permission to issue electronic money ("e-money") and to provide payment services. It is part of the Coinbase Group, which operates a prominent cryptoasset trading platform that is accessible globally. CBPL does not undertake cryptoasset transactions for customers but it enables customers to deposit fiat currency into e-money wallets which can then be used to purchase and exchange cryptoassets via other entities within the Coinbase Group.

2.2. Cryptoassets provide a near-instant and low-cost way to transfer value across borders. Whilst the vast majority of cryptoasset transfers are conducted for valid

purposes, they can be an attractive technological enabler for criminals seeking to launder funds. This is due to a number of factors including the pseudo-anonymous nature of cryptoassets and services, their accessibility online, and constant innovation offering new opportunities for criminals to exploit novel applications.

2.3. Combating the laundering of funds through the financial services sector is an issue of international importance, and forms part of the Authority's operational objective of protecting and enhancing the integrity of the UK financial system. Authorised firms are at risk of being abused by those seeking to launder money and firms that conduct payment services and/or those which facilitate trading in cryptoassets may be at particular risk. As a result, it is imperative that such firms maintain robust systems and controls to identify and mitigate the risk of their businesses being used in this way.

2.4. During a visit to CBPL in February 2020, the Authority identified significant weaknesses and gaps in the Firm's financial crime control framework. The Authority considered that the weaknesses meant that CBPL's business should be restricted to prevent high-risk customers accessing its e-money and payment services while the Firm remediated its financial crime controls.

2.5. In the following months, the Authority engaged with CBPL to agree a definition of "high-risk" which would enable CBPL's automated onboarding systems to prevent such customers being onboarded. On 30 October 2020, on CBPL's application, the Authority imposed on CBPL requirements which prevented such customers from being onboarded or provided with payment or e-money services ("the CBPL VREQ"). These were mandatory regulatory requirements, with which CBPL was required to comply.

2.6. Between 31 October 2020 and 1 October 2023 (the "Relevant Period") CBPL onboarded approximately 3.9 million customers. During this time CBPL repeatedly breached the requirements imposed on it by the CBPL VREQ by:

a) onboarding and/or providing payment or e-money services to 13,416 separate high-risk customers, as defined by the CBPL VREQ, with some of these customers being provided payment or e-money services on multiple occasions; and

b) permitting approximately 31% of these customers to make 12,912 prohibited deposits with a total value of approximately USD $24.9 million; these monies were then used to make withdrawals and, thereafter, execute multiple cryptoasset transactions via other Coinbase Group entities using the same funds, totalling approximately USD $226 million.

2.7. CBPL filed Suspicious Activity Reports ("SARs") in respect of 62 customers to alert law enforcement to potential money laundering. A number of the transactions subject to these SARs were of significant value, with several being in excess of USD $50,000, and the total value of the transactions involved being approximately USD $1.75 million.

2.8. The breaches of the CBPL VREQ were caused by a failure on the part of CBPL, between 30 October 2020 and 14 April 2023, in breach of Principle 2 of the Authority's Principles for Businesses (the "Principles"), to exercise due skill, care and diligence in relation to the design, testing, implementation and monitoring of the controls put in place to ensure compliance with it, including an automated 'flag' placed on relevant customers' accounts ("the VREQ Flag"). In particular:

a) CBPL failed to maintain adequate records regarding the steps it took to ensure compliance with the CBPL VREQ;

b) CBPL failed to ensure that the engineers tasked with updating the automated onboarding process were provided with complete instructions, including the most recent version of the CBPL VREQ, meaning that, when originally implemented, the controls failed to give full effect to the CBPL VREQ;

c) CBPL's pre-implementation testing of the VREQ Flag was inadequate;

d) CBPL failed to adequately consider all of the various products and systems through which customers could access e-money services when designing and implementing the VREQ Flag;

e) CBPL failed to ensure that when certain new systems enabling customers to execute transactions were introduced, effective controls were introduced to ensure that the new systems did not undermine CBPL's compliance with the terms of the CBPL VREQ;

f) CBPL failed to adequately consider all of the various ways in which customers might be onboarded when designing and implementing the VREQ Flag, in particular the position of customers migrating from other Coinbase Group entities and, crucially, whether an assessment was conducted at that time to ensure that any high-risk customers seeking to onboard were subject to the VREQ Flag;

g) The initial monitoring of compliance with the CBPL VREQ, conducted by the Product, Engineering and Design team ("PED") within the Coinbase Group, was inadequate; this meant that repeated and material breaches of the CBPL VREQ went undiscovered for almost 2 years; and

h) Notwithstanding CBPL identifying breaches of the VREQ shortly after it came into effect, CBPL failed to conduct a formal review of the overall effectiveness of the controls intended to ensure compliance with the CBPL VREQ until 2 years after it came into force, nor did the Firm issue a formal documented framework for ensuring compliance with the CBPL VREQ until April 2023.

2.9. The Authority considers that CBPL's failings in relation to the controls that it put in place to comply with the CBPL VREQ were serious and persistent. The failings significantly increased the risk that financial crime might be facilitated by the Firm at a time when the Authority had informed CBPL that its systems and controls were not fully effective and required remediation. The Authority hereby imposes on CBPL a financial penalty of £3,503,546 pursuant to Regulation 51(1)(a) of the EMRs.

2.10. Since 2020, CBPL has worked to enhance its financial crime framework. The Authority acknowledges the Firm's commitment to ensuring that it has an effective financial crime framework in place.

2.11. CBPL has cooperated with the Authority throughout the course of its investigation.

3. DEFINITIONS

3.1. The definitions below are used in this Notice:

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

"AEMI" means an Authorised Electronic Money Institution, as defined in Regulation 2(1) of the EMRs;

"AML" means anti-money laundering;

"the Authority" means the Financial Conduct Authority;

"CBPL" or "the Firm" means CB Payments Ltd (FRN: 900635);

"CBPL Board" means the Board of Directors of CBPL;

"CBPL VREQ" means the requirements imposed on CBPL under Regulation 8 of the EMRs, as applied for on 30 October 2020;

"Coinbase Card" means the debit cards provided to customers of certain Coinbase Group entities, including CBPL, and, in the case of CBPL, through which customers could make purchases of goods and services using the funds in their e-money wallets;

"the Coinbase Group" means the group of companies of which CBPL is part;

"Coinbase Pro" means a cryptoasset trading service offering customers via other entities in the Coinbase Group greater functionality than the core, retail service and which was provided to customers who required more sophisticated trading features;

"the Compliance Dashboard" means the dashboard, which became operational in December 2022, used by the CBPL compliance team for the daily monitoring of transactions conducted by customers who had a VREQ Flag applied to their accounts;

"Compliance Oversight Working Group" or "COWG" means the working group which was assigned day-to-day oversight of compliance matters impacting CBPL by the CBPL Board, formerly known as the Financial Crime Oversight Working Group before its remit was expanded beyond financial crime risk management in December 2020;

"DEPP" means the Authority's Decision Procedure and Penalties Manual;

"EG" means the Authority's Enforcement Guide;

"e-money" means electronic money, as defined in Regulation 2(1) of the EMRs;

"e-money wallet" means the digital wallet provided by CBPL to retail and institutional customers, enabling them to: (i) deposit and withdraw fiat currency; (ii) purchase cryptoassets via other entities within the Coinbase Group; and (iii) convert cryptoassets purchased via other entities within the Coinbase Group into withdrawable fiat currency ;

"EMRs" mean the Electronic Money Regulations 2011;

"fiat currency" means a national currency backed by the government or central bank that issued it;

"Financial Crime Oversight Working Group" or "FCOWG" means the working group which was established in May 2020 to assist with discharging CBPL's oversight responsibilities with respect to financial crime risk management and monitoring and assessing the effectiveness of CBPL's financial crime compliance programme;

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

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

"PED" means the Product, Engineering and Design team of the Coinbase Group, which provided services to CBPL, including the implementation and testing of the VREQ Flag;

"the PED Dashboard" means the dashboard used by PED until December 2022 to monitor the percentage of customers who had applied to open an account with CBPL and who had: (i) been permitted to open that account, (ii) had the ability to undertake fiat currency transactions via CBPL, and (iii) actually deposited fiat currency into their CBPL account;

"PEP" means politically exposed person, as defined in Regulation 35(12)(a) of the MLR 2017;

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

"Prohibited Transactions" means transactions prohibited under the CBPL VREQ, including deposits into, or withdrawals from, a high-risk customer's e-money wallet, cryptoasset purchases funded from a high-risk customer's e-money wallet undertaken via other entities in the Coinbase Group, cryptoasset sales undertaken via other entities in the Coinbase Group resulting in a deposit to a high-risk customer's e-money wallet and any other transaction or action which generates a balance in a high-risk customer's e-money wallet;

"the Relevant Period" means 31 October 2020 to 1 October 2023;

"SAR" means Suspicious Activity Report, a report which a firm is obliged to make to law enforcement authorities when it knows, suspects or has reasonable grounds for knowing or suspecting that a person has engaged in money laundering and/or terrorist financing;

"Second Breach Notification" means the notification of breaches of the CBPL VREQ which was provided to the Authority on 21 October 2022, with further updates on the extent of the breaches following thereafter;

"Simple Trade Service" means the new system on which certain retail transactions were executed from June 2022;

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

"VREQ" or "Voluntary Requirement" means, for the purposes of this Notice, a requirement on a firm's authorisation which may restrict or limits its business in some way, upon the application of that firm to the Authority: (i) pursuant to Regulation 8 of the EMRs with respect to firms authorised under the EMRs, such as AEMIs; and (ii) pursuant to section 55L(5) of the Act with respect to firms authorised under Part 4A of the Act;

"The VREQ Compliance Framework" means the written framework introduced by CBPL on 14 April 2023 that described the internal requirements and framework designed to give effect to the terms of the CBPL VREQ;

"VREQ Control Review" means the review performed at the end of 2022 regarding the effectiveness of the controls put in place to ensure compliance with the CBPL VREQ, following which a report was produced on 1 December 2022 setting out the results;

"VREQ Monitoring Procedure" means the framework introduced on 20 January 2023 setting out CBPL's use of the Compliance Dashboard; and

"VREQ Flag" means a control that applied a flag to the accounts of high-risk customers of CBPL who satisfied the criteria set out in the CBPL VREQ, in order to block their access to e-money services.

4. FACTS AND MATTERS

The Firm

4.1 CBPL is a company incorporated in the United Kingdom and is part of the Coinbase Group, which operates a prominent cryptoasset trading platform that is accessible globally. During the Relevant Period CBPL was authorised by the Authority as an AEMI, with permission to issue e-money and provide payment services.

4.2 CBPL provides hosted e-money wallets to retail and institutional customers. CBPL's customers can deposit funds into the e-money wallet from their own bank accounts. CBPL does not itself undertake cryptoasset transactions but the e-money wallet can be used by customers to purchase cryptoassets on the Coinbase platform via another company in the Coinbase Group or to store the funds converted back from cryptoassets traded on the platform. In effect, therefore, CBPL acts as a gateway for UK customers to exchange fiat currency for cryptoassets and vice versa.

4.3 CBPL also provides e-money services to affiliate entities within the Coinbase Group in exchange for a service fee from the affiliate. This forms part of the 'shared service' model operated by the Coinbase Group, whereby functions and employees serve a number of entities within the Coinbase Group. Accordingly, the organisation of the Coinbase Group is substantially by function, rather than entity, and CBPL receives services from various functions, including the Product, Engineering and Design team ("PED") and Compliance.

4.4 This meant that, in effect, CBPL outsourced certain of its important operational functions to other entities in the Coinbase Group. CBPL was entitled to outsource these functions but it remained responsible at all times for ensuring that it complied, and continued to comply, with regulatory requirements imposed on it.

4.5 At the start of the Relevant Period, CBPL's customer base was approximately 2.8 million, but by March 2023 it had increased to approximately 3.1 million. The majority of CBPL's customer base comprises individual retail customers, although it does service a much smaller proportion of institutional and corporate customers.

Financial Crime Risks in the E-money and Cryptoasset Sectors

4.6 In July 2020 the Authority published a letter sent to CEOs of payment and e-money firms which highlighted weaknesses identified in the sector, including ineffective systems and controls for preventing financial crime. Firms were required to put in place robust frameworks and governance and consider the financial crime risk posed by innovative products, unusual or agency-type business models and cross-border payments. A further letter was sent to payment and e-money firms in March 2023, reiterating the importance of robust systems and controls as there had been increasing evidence of financial crime in the sector over the previous two years. Weaknesses in some firms' systems and controls were specifically identified as making these types of firms a target for bad actors.

4.7 From at least 2018 the Authority has published materials highlighting the financial crime risks associated with cryptoassets. The UK's 2020 National Risk Assessment noted that it would likely be increasingly easy for criminal actors to enter the cryptoasset market by converting fiat currency. The National Strategic Assessment for Serious and Organised Crime 2023 warned that cryptoassets are an important facilitator for criminal transactions including paying for goods and services on the dark net, making ransom demands and a wide range of frauds. They are also increasingly being used by professional money launderers seeking to convert cash for global criminal networks. Although CBPL did not undertake any cryptoasset transactions for customers, customers could use fiat currency in their e-money wallets to purchase cryptoassets via other entities in the Coinbase Group.

Concerns raised in 2020 about CBPL's Financial Crime Framework

4.8 As a financial institution, CBPL is required to identify and assess the risks of money laundering and terrorist financing to which its business is subject and to maintain

controls to mitigate and manage effectively these risks. This includes compliance with the requirements of the MLR 2017. The Authority is responsible for supervising CBPL and taking necessary measures to secure its compliance with these requirements.

4.9 The Firm was the subject of a financial crime controls assessment visit on 27 and 28 February 2020. Following the visit, on 30 April 2020, the Authority issued a feedback letter, which concluded that significant weaknesses and gaps persisted in CBPL's financial crime control framework. The Authority noted that this was particularly concerning given the high-risk nature of CBPL's business and that limited progress appeared to have been made to address issues highlighted in audits performed by the Firm since 2018. In particular, a sample of reviewed files showed limited evidence of risk assessments having been performed in certain high risk situations.

4.10 The Firm provided the Authority with a detailed plan to address the Authority's feedback on 29 May 2020, with the objective of completing the remediation work by the end of the year. The Authority determined that it would be appropriate for the Firm to appoint a skilled person to conduct a review of CBPL's financial crime controls, following the remediation work, at the start of the following year.

Voluntary Application for Requirements (VREQ)

4.11 One of the tools used by the Authority to mitigate risks at an individual firm level is the imposition of requirements on a firm which may restrict or limit its business. While the Authority has the power to impose requirements on its own initiative, frequently, it will seek to agree the terms of any requirements which it proposes to impose and invite the firm to apply for their imposition. Agreement has potential efficiency benefits and enables the firm to provide input into the drafting of requirements which may anticipate and avoid any practical difficulties in complying with the proposed requirements. Whether imposed as a result of the Authority's own-initiative action, or as a result of an application by the firm, once requirements have been imposed, they become mandatory regulatory requirements with which the firm must comply. The imposition of voluntary requirements in this way is commonly referred to as a VREQ.

Discussion of Proposed Requirements

4.12 Following the 30 April 2020 feedback letter, the Authority raised the prospect of the Firm applying for voluntary requirements to restrict it from onboarding any new high-risk customers at a meeting on 31 July 2020. Given the Authority's concerns around CBPL's financial crime systems and controls at the time, the intention was to prevent an increase in CBPL's pool of high-risk customers (both retail and institutional), while CBPL undertook its remediation work.

4.13 Over the course of the next three months, CBPL and the Authority discussed the terms of the proposed requirements. CBPL voluntarily ceased to onboard new high-risk institutional customers from 6 August 2020. However, because CBPL's onboarding processes in respect of retail customers were automated, and it had no automated control to restrict onboarding based solely on the customer's risk, preventing high-risk retail customers from onboarding required bespoke systems changes to identify high-risk individuals according to specified criteria and then to block them from making transactions involving the provision of regulated services by CBPL.

4.14 In early August 2020, CBPL relayed to the Authority that it was working with its engineers to work out how to implement the terms of a VREQ as soon as possible. The Authority engaged with CBPL to ensure that the terms of the proposed voluntary requirements would both enable compliance by CBPL through its automated systems and adequately address the Authority's concerns. As a result of this engagement, CBPL knew, or should have known, the importance the Authority attached to compliance with the proposed requirements.

4.15 On 28 August 2020, CBPL first proposed to the Authority designing a bespoke automatic control to address the position of high-risk retail customers. Following further discussions, on 24 September 2020, CBPL relayed an updated systems solution to the Authority which, it asserted, could be implemented by 30 October 2020. On 6 October 2020, the Authority confirmed that the proposal was acceptable and, on 12 October 2020, sent CBPL the text of the proposed requirements.

4.16 On 15 October 2020, CBPL reverted to the Authority with some proposed amendments to the text of the proposed voluntary requirements. These amendments were discussed on a call between the Authority and CBPL on 19 October 2020 and in subsequent correspondence, which resulted in the Authority

making further amendments to the proposed terms of the CBPL VREQ. A revised version of the voluntary requirements, which incorporated these further amendments, was sent to CBPL on 23 October 2020.

4.17 On 29 October 2020, the Authority sent CBPL a finalised text of the draft voluntary requirements, which included an additional amendment at CBPL's request since the last version had been circulated. On 30 October 2020, CBPL applied for the imposition of the requirements based on this text. Later the same day, the Authority notified CBPL that its application for the imposition of voluntary requirements had been accepted. The CBPL VREQ was in force from 30 October 2020 in respect of institutional customers and from 31 October 2020 in respect of retail customers.

4.18 As a result of the Authority's engagement with CBPL, the Authority understood, and it was entitled to understand, that CBPL had fully considered the proposed requirements and had worked with its engineers and other relevant parties to ensure that its systems would enable and ensure compliance with the terms of the requirements.

The Terms of the CBPL VREQ

4.19 Under the CBPL VREQ, the Firm was required not to onboard, provide payment services or issue e-money to:

a) new institutional or corporate customers identified as 'high-risk' or 'ineligible' as per the Firm's institutional customer risk rating methodology; and

b) new retail or personal customers that met any one of a number of specific criteria.

The CBPL VREQ Controls

4.20 In May 2020, CBPL established the Financial Crime Oversight Working Group ("FCOWG"), part of whose remit was to monitor and assess the effectiveness of CBPL's financial crime compliance programme. In December 2020 FCOWG was renamed the Compliance Oversight Working Group ("COWG") and given an expanded remit covering all compliance matters relevant to CBPL. During the Relevant Period FCOWG/COWG was the relevant forum for internal governance

related to incidents concerning the CBPL VREQ, having assumed delegated responsibility for day-to-day oversight of compliance matters from the CBPL Board.

4.21 Also in May 2020, a 'cross-functional working group' was set up by CBPL to oversee the delivery of the action plan (the Firm's package of actions designed to address the concerns in the Authority's feedback letter of 30 April 2020). Following CBPL's meeting with the Authority on 31 July 2020, this group assumed responsibility for:

a) Devising proposals for CBPL to provide to the Authority in relation to the scope and terms of the CBPL VREQ;

b) Devising interim controls to prevent CBPL from onboarding new high-risk customers in August and September 2020, before the CBPL VREQ was signed; and

c) Designing and implementing controls to give effect to the terms of the CBPL VREQ.

4.22 The work of the cross-functional working group was in turn overseen by a 'steering group'.

4.23 The way in which the Firm sought to implement the CBPL VREQ differed as between retail and institutional customers. Onboarding of institutional customers was a manual process, undertaken by Compliance, in accordance with bespoke guidance.

4.24 However, the onboarding of retail customers was an automated process. In respect of these customers the Firm sought to implement the CBPL VREQ via a combination of pre-existing systems and controls, including sanctions and PEP screening, and a new control in the form of the 'FCA HR Flag' (the "VREQ Flag").

4.25 Prospective CBPL customers were required to complete customer due diligence and, where applicable, enhanced due diligence. Information provided during the onboarding process was then used to assess whether the customer was high-risk within the meaning of the CBPL VREQ. If a customer was deemed high-risk the VREQ Flag would be applied to their account. This was designed to be an entirely automated process that did not require human intervention by any CBPL employee.

4.26 The application of the VREQ Flag was intended to ensure that customer orders and transactions (including e-money deposits and cryptoasset transactions) were blocked at the point of creation, preventing all Prohibited Transaction types which could result in an e-money balance.

4.27 Because the design and application of the VREQ Flag involved changes to CBPL's automated systems, the necessary software changes needed to be made by the PED team, an outsourced function operated by another Coinbase Group company based in the USA. While CBPL was entitled to utilise the technical expertise of the PED team, it remained responsible for ensuring that the VREQ Flag had been applied in such a way as to ensure ongoing compliance with the CBPL VREQ and should have taken reasonable steps to satisfy itself that the VREQ Flag effectively implemented the requirements of the CBPL VREQ and that it operated in practice as it was anticipated. In the Authority's view, this could have included:

a) Ensuring that the PED team were provided with complete instructions, including the most recent terms of the CBPL VREQ;

b) Ensuring that the design of the VREQ Flag took into account all means by which high-risk customers may be provided with e-money services by CBPL;

c) Ensuring that adequate testing of the VREQ Flag was conducted before its implementation;

d) Monitoring the ongoing effectiveness of the VREQ Flag and CBPL's compliance with the CBPL VREQ;

e) Ensuring that those responsible for monitoring CBPL's compliance with the CBPL VREQ were provided with sufficient information to assess the effectiveness of the VREQ Flag, where appropriate through the assurance of independent review;

f) Putting in place processes to ensure that any systems upgrades or changes took account of the VREQ Flag and ensured ongoing compliance; and

g) Ensuring that appropriate records were kept, demonstrating the steps taken by CBPL to ensure compliance with the CBPL VREQ.

Design of the VREQ Flag

4.28 As outlined below, when initially designing the VREQ Flag, the PED team used a draft version of the text of the CBPL VREQ which was subsequently updated prior to its imposition. This meant that the VREQ Flag, as initially designed, did not take account of certain of the criteria which should have led to the assessment of a customer as high-risk.

4.29 Further, as subsequent events outlined below would demonstrate, the design of the VREQ Flag did not take account of some of the ways that high-risk customers of the Coinbase Group may access CBPL's e-money services, including use of the 'Coinbase Pro' product or migration from other Coinbase Group entities.

Pre-implementation Testing of the VREQ Flag

4.30 CBPL was required to keep records relating to its compliance with the VREQ. When required to provide details, including records of the pre-implementation testing of the VREQ Flag, CBPL produced five records of meetings having taken place between 28 September 2020 and 6 October 2020, involving Coinbase Group employees from PED and the Compliance, Legal and Customer Experience teams. Each meeting was scheduled to last between 20 minutes and half an hour. A single record, describing the testing undertaken, which took place on 6 October 2020, was produced. The testing involved three employees attempting to onboard and access e-money services as follows:

a) Two members of the PED team responded to the 'know your customer' questions in different ways designed to trigger the VREQ Flag. At the same time other members of the PED team observed whether the VREQ Flag was assigned to the accounts of the two employees seeking to onboard, following which those two employees would confirm whether they were able to access e-money services from CBPL;

b) Another member of the PED team responded to the 'know your customer' questions in such a way as to avoid triggering the VREQ Flag, before then confirming whether they were able to access e-money services from CBPL; and

c) The representatives of the PED team who participated in the testing described above confirmed that the VREQ Flag had operated as expected in blocking

access to e-money services where they had responded to certain of the 'know your customer' questions in a way designed to trigger the VREQ Flag.

4.31 CBPL asserted that similar testing was conducted by a single member of PED on 28 September, 30 September, 1 October and 5 October 2020 but was unable to produce any records of this testing beyond records of meetings having taken place. CBPL did not assert that any further testing of the VREQ flag took place until October 2022 when, as outlined below, significant issues with its operation had been identified.

4.32 The single record that was produced showing the output of the testing conducted on 6 October 2020 could not have provided CBPL with any adequate satisfaction that the VREQ Flag was fully effective in implementing the terms of the CBPL VREQ and preventing the provision of e-money services by CBPL to high-risk customers.

Implementation Issues (First Breach Notification)

4.33 On 13 November 2020 FCOWG was informed that the VREQ Flag had not been fully implemented by 31 October 2020 as required; the matter being discussed further on 9 December 2020 and reported to the CBPL Board on 15 December 2020. The following day the Firm informed the Authority that it was in breach of the CBPL VREQ.

4.34 CBPL subsequently confirmed that, between 31 October 2020 and 18 December 2020, it had onboarded and granted access to e-money services to 4,471 high-risk customers in contravention of the CBPL VREQ. Furthermore, 2,737 of these customers undertook Prohibited Transactions, comprising 6,344 deposits with a total value of USD $6.82 million.

4.35 All but one of the 4,471 customers onboarded in breach of the CBPL VREQ obtained access to CBPL's services as a result of one of two gaps in the controls:

a) assessment of whether a customer was high-risk, and should therefore be assigned the VREQ Flag, occurred dynamically based on information held on file at that time, rather than information provided at the point of onboarding. This meant that it was possible for customers to alter the information provided at onboarding in ways that could lead to their risk rating being downrated, resulting in the VREQ Flag no longer applying to their account; and

b) the VREQ Flag was designed using an earlier version of the CBPL VREQ criteria (which changed over time as a result of discussions between CBPL and the Authority). As a result, answers to four 'know your customer' questions asked at the time of onboarding that indicated a customer was high-risk did not trigger the application of the VREQ Flag as they should have.

4.36 The remaining customer was incorrectly onboarded and given access to e-money services as a result of PEP screening for customers living outside the UK not being implemented until just over two weeks after the CBPL VREQ had come into force, from 16 November 2020 onwards.

4.37 On 20 January 2021 the Authority wrote to the Firm emphasising the need for it to take all reasonable steps to ensure it had the relevant systems and controls in place in order to fully comply with the CBPL VREQ and expressing the expectation that senior management would oversee and ensure compliance with the terms of the CBPL VREQ. On 27 January 2021, having rolled out fixes to address the issues it had identified, CBPL confirmed to the Authority that the requirements of the CBPL VREQ had been fully implemented.

4.38 In the Authority's view these breaches arose from the Firm's failure to: (i) ensure that PED were provided with complete instructions, including the most recent version of the terms of the CBPL VREQ; and (ii) undertake sufficiently rigorous pre-implementation testing to enable it to understand how customer actions might inhibit the effectiveness of the VREQ Flag.

Monitoring of the VREQ Controls Pre-December 2022

4.39 The fact that the VREQ Flag had, within two months of its implementation, demonstrably failed to ensure compliance with the terms of the CBPL VREQ in numerous cases, should have impressed upon CBPL the ongoing importance of ensuring that the VREQ Flag was operating effectively and in all relevant cases. Indeed, in January 2021, CBPL had specifically confirmed to the Authority that the terms of the CBPL VREQ had been fully implemented and should have taken reasonable steps to gain the necessary assurance that it had been.

4.40 Yet, beyond addressing and remediating the specific breaches that were identified and looked into by CBPL in December 2020, CBPL conducted no broader and documented investigation into the CBPL VREQ controls and, in doing so, it failed to consider whether the breaches may have been indicative of other flaws in the

design of the VREQ Flag and whether, consequently, other flaws may have remained.

4.41 Moreover, until October 2022, CBPL conducted no ongoing monitoring or testing of the effectiveness of the controls put in place to ensure compliance with the CBPL VREQ. When required to provide details of any monitoring conducted prior to October 2022, the only measure which the Firm was able to describe was the use by PED of dashboards that showed, among other things, the percentage of customers who had applied to open an account and who had: (i) been permitted to open that account; (ii) had the ability to undertake fiat currency transactions via CBPL; and (iii) actually deposited fiat currency into their CBPL e-money wallet. Because these metrics showed a sharp drop in the proportion of customers able to access e-money services through CBPL at the point of implementing the VREQ Flag, and thereafter remained consistent, CBPL believed that this indicated that the VREQ Flag was working as designed.

4.42 However, to the extent that CBPL relied upon the consistency of these metrics to satisfy itself that the VREQ Flag (and other controls) were operating effectively, the Authority considers that this reliance was plainly misplaced. In particular:

a) The use of consistency of numbers of customers after implementation to be any indicator of effectiveness depended on the VREQ Flag having been implemented effectively in the first place (and CBPL knew that it had not been); and

b) The dashboards did not monitor the number of customers in respect of whom the VREQ Flag was applied and whether those customers were able to access e-money services from CBPL.

4.43 Other teams (including CBPL's Compliance function, the Quality Assurance function and Coinbase Group's Internal Audit function) did not consider or review the operation of the VREQ Flag and no external assessment of the VREQ Flag was conducted, despite there having been opportunities for CBPL to include a review of the VREQ Flag in other work that was being undertaken prior to December 2022.

4.44 As a result, prior to October 2022, CBPL had no adequate means to assess the effectiveness of the VREQ Flag. Because CBPL did not take reasonable steps to satisfy itself that the VREQ Flag was operating as intended, it failed to identify that there were significant flaws in its design. As a result, CBPL failed to identify or

prevent thousands of Prohibited Transactions that formed the subject of the Second Breach Notification.

The Second Breach Notification

4.45 On 23 September 2022, while dealing with a complaint against CBPL which had been made to the Financial Ombudsman Service, the Complaints team approached the Compliance team for information. During subsequent investigations, Compliance identified that the VREQ Flag had been applied to the customer's account and the customer should therefore have been prevented from receiving e-money services.

4.46 On 21 October 2022, CBPL notified the Authority that it had identified further breaches of the CBPL VREQ, all of which: (i) were the result of previously unidentified deficiencies with the operation of the VREQ Flag; and (ii) had not been identified by such ongoing monitoring as CBPL had in place.

4.47 CBPL's investigations identified that 8,183 customers had been able to access e-money services in breach of the CBPL VREQ as a result of the ineffective application of the VREQ Flag in two particular respects:

a) Coinbase Pro: CBPL enabled fiat services in relation to Coinbase Pro which was a cryptoasset trading product offered by other entities within the Coinbase Group to a subset of retail customers who required more sophisticated trading features; these users often conducted more frequent or high value trades than standard retail customers. The VREQ Flag was not applied to newly onboarded customers using the Coinbase Pro product, meaning that they were not prevented by CBPL from receiving e-money or payment services. Accordingly, high-risk customers using Coinbase Pro, who should have had the VREQ Flag applied to their accounts, were still able to undertake Prohibited Transactions, and had been able to do so since the VREQ Flag was implemented in October 2020; and

b) Simple Trade Service: In June 2022, a new system for certain transactions performed by retail customers had been introduced called the 'Simple Trade Service'. When it was introduced, CBPL failed to ensure that the VREQ Flag would be applied in the same way, resulting in customers subject to the VREQ Flag being able to perform Prohibited Transactions for a period of four months.

4.48 The investigations revealed further issues. A further 1,034 high-risk customers had been able to access e-money services from CBPL after having migrated from another Coinbase Group entity to the Firm. Although these customers were high-risk within the meaning of the CBPL VREQ, an assessment was not conducted to determine whether the VREQ Flag should have been applied to their account at the time of migration, resulting in it not having been applied as it should have been.

4.49 Finally, notwithstanding guidance provided to the relevant customer service teams, e-money had been manually credited to the e-money wallets of 199 high-risk customers by members of these teams, despite their accounts being subject to the VREQ Flag. This occurred, for example, when customers were compensated for a negative customer experience.

4.50 The Firm subsequently confirmed that between 31 October 2020 and 28 October 2022, as a result of the above issues, it had onboarded and granted access to e-money services to 9,416 high-risk customers in contravention of the CBPL VREQ.

4.51 Of these, 1,155 customers deposited a total of USD $17.86 million made up of 5,687 individual deposit transactions.

4.52 Customers forming part of the Second Breach Notification completed withdrawals and, thereafter, executed multiple cryptoasset transactions via other Coinbase Group entities using the same funds, totalling approximately USD $226 million.

4.53 The Authority considers it significant that the above breaches were only identified as a result of a customer lodging a complaint with the Financial Ombudsman Service, which led to an investigation by PED, and not through the Firm monitoring its compliance with the CBPL VREQ.

4.54 The Authority further considers that:

a) the considerable length of time taken to identify the breaches, coupled with them only coming to light following a customer complaint, demonstrates inadequate monitoring of the Firm's compliance with the CBPL VREQ. This is exacerbated by the Authority having already emphasised the importance of having appropriate systems and controls in place to restrict high-risk customers from being onboarded following the first breach, along with the Firm confirming

the CBPL VREQ had been fully implemented at that time, as set out at paragraph 4.37 above;

b) the failure of the Firm to adequately consider the position of the Coinbase Pro platform, one of the three primary product offerings of the Coinbase Group at the relevant time, or to test the operation of the VREQ Flag in relation to this product, is a serious oversight;

c) the breaches arising from the adoption of the Simple Trade Service demonstrate that inadequate procedures had been put in place to ensure that the VREQ Flag was appropriately carried over to or effective within this new system during the four month period following its introduction in June 2022; and

d) CBPL failed to adequately consider all the various ways in which customers might be onboarded when designing and implementing the VREQ Flag and, crucially, whether an assessment was always conducted at that time to ensure any high-risk customers seeking to onboard were subject to the VREQ Flag, namely those customers who migrated from other Coinbase Group entities.

The VREQ Control Review

4.55 Following the Second Breach Notification, CBPL undertook a review of the effectiveness of the controls put in place to ensure compliance with the CBPL VREQ, the results of which were set out in the VREQ Control Review report dated 1 December 2022. This was a point in time assessment based on confirmation by individual "control owners" that the relevant control was operational and working as intended. The review concluded that, with respect to new and existing customers who attempted to onboard directly to CBPL, the existing controls were effective, although the issue set out at paragraph 4.48 above regarding customers migrating from other Coinbase Group entities to CBPL was also acknowledged in the report. Notwithstanding the conclusion of the report, new forms of monitoring introduced by CBPL from December 2022 would go on to identify further instances of control failures.

4.56 The report also noted that, "*[r]oles and responsibilities relating specifically to the controls implementing the VREQ have not been formally documented… While the general roles of different functions are described in existing documentation, documentation of the VREQ Compliance framework has not been formalized and there is no formally issued document which lays out the roles of teams specifically*

with regard to the controls implementing the VREQ requirements". Given the importance the Authority attached to compliance with the CBPL VREQ, as explained in correspondence and demonstrated through significant engagement over its terms (see paragraphs 4.12 – 4.18), as well as the significant issues CBPL encountered at implementation and thereafter in complying with its terms (see paragraphs 4.33 – 4.38 and 4.45 – 4.54), the Authority considers that CBPL should have had a formal framework in place setting out how it would ensure compliance with the CBPL VREQ from the outset of the Relevant Period. It is notable that a document recording a formal framework was not issued until 14 April 2023, some two and a half years after the CBPL VREQ came into force, albeit certain of the arrangements outlined in the framework, including in relation to targeted dashboard monitoring (see paragraphs 4.57 – 4.60 below), had either already been implemented or were being discussed prior to that date.

The Compliance Dashboard

4.57 In December 2022 CBPL's Compliance team began monitoring accounts which were subject to the VREQ Flag. The monitoring worked by way of a dashboard (the "Compliance Dashboard") which showed Compliance: (i) the total number of customers who had had the VREQ Flag applied to, or removed from, their account on a monthly basis; (ii) a daily count of the fiat currency transactions conducted by customers subject to the VREQ Flag; and (iii) the total amount of fiat currency held by customers subject to the VREQ Flag at the end of each month.

4.58 To formalise this additional ongoing monitoring and set out how it would work in practice, CBPL introduced a VREQ Monitoring Procedure on 20 January 2023. The VREQ Monitoring Procedure provided that, on every working day, a member of the CBPL Compliance team would check the Compliance Dashboard to ensure that no e-money transactions, other than allowed withdrawals, had been conducted by CBPL customers who had the VREQ Flag applied to their accounts since the previous day's check. It also set out how the member of the Compliance team was required to escalate any instance of e-money transactions being performed by customers subject to the VREQ Flag, first to the team responsible for investigating the issue, and then to CBPL's money laundering reporting officer.

4.59 The implementation of the Compliance Dashboard represented an improvement in the Firm's monitoring of compliance with the CBPL VREQ and enabled it to identify and, in some instances, to prevent further breaches, as set out below.

4.60 While the improved monitoring, along with putting a formal framework in place regarding compliance with the CBPL VREQ, were positive steps taken by CBPL to assist with avoiding and detecting further breaches, the Authority considers these steps ought to have been taken much earlier, upon the CBPL VREQ first being implemented. The Authority further considers that the failure to develop and document such formalised processes and procedures for over two years after the CBPL VREQ came into force contributed to the significant breaches outlined above, including the considerable length of time that passed before CBPL identified the breaches subject to the Second Breach Notification (see paragraphs 4.45 and 4.53).

Further Breaches (Breach Notifications Three to Six)

Third breach notification

4.61 As part of the remediation work undertaken in relation to the Second Breach Notification, CBPL applied the VREQ Flag to customers not previously subject to it, including customers who had migrated from other Coinbase Group entities (see paragraph 4.48 above). In taking these steps, CBPL identified on 17 January 2023 that one high-risk customer with a pending e-money order (with a value of £11.35) at the time of the application of the VREQ Flag had still been able to execute this order once the VREQ Flag had been applied to their account.

4.62 The following day, 18 January 2023, CBPL identified a further five pending orders placed by high-risk customers, which it was able to cancel prior to execution and thereby avoid other transactions being executed in breach of the CBPL VREQ. The third breach notification in respect of the above customer was submitted to the Authority the same day.

Fourth breach notification

4.63 On 9 March 2023, CBPL submitted the fourth breach notification to the Authority. The Firm had identified that approximately 200 high-risk customers were able to undertake Prohibited Transactions after their accounts had been opened, but before the assessment as to whether VREQ Flag should be applied to their accounts had been completed. Whilst the assessment and assigning of the VREQ Flag had typically been completed in a matter of seconds, in some cases delays had resulted in it taking several minutes and, between 6 and 10 January 2023, the time taken

to complete the process increased to a number of days. Consequently, 182 high-risk customers were able to complete 272 prohibited deposits with a total value of USD $113,928.

4.64 Around the same time as the fourth breach notification, on 14 March 2023, CBPL notified the Authority that it had also identified that nine high risk customers had the ability to purchase cryptoassets via a third-party payments platform following the rollout of this feature in the previous month, with one of these customers going on to purchase cryptoassets.

4.65 Following the identification of these breaches, in March 2023, CBPL commenced a broader review of the electronic and code-based controls considered "*most critical*" to its compliance with applicable legal and regulatory AML requirements, including the controls that had been put in place to ensure compliance with the terms of the CBPL VREQ, such as the VREQ Flag. This review (and the testing of the controls which was carried out as part of the review) continued throughout 2023. It was through this review that CBPL identified the two further breaches detailed below.

Fifth breach notification

4.66 On 25 September 2023, CBPL submitted the fifth breach notification to the Authority. The Firm identified that 152 high-risk customers, to whose accounts the VREQ Flag had been applied, had received fiat currency (in the form of 'fiat credits') into their e-money wallets and who, in some cases, went on to spend these funds using their Coinbase Cards:

a) 145 customers received credits in the form of fiat currency through refunds of prior purchases made on their Coinbase Cards, totalling approximately £74,000. In a number of cases, the customers went on to spend these sums using their Coinbase Cards, totalling approximately £24,000; and

b) 7 customers received credits in the form of fiat currency through "*other means"*, such as a fee rebate or by way of compensation for a customer complaint, totalling approximately £4,000. These customers went on to spend approximately £387 of these funds using their Coinbase Cards.

4.67 The above customers used the prohibited deposits to conduct 600 transactions, with a total value of £98,000.

Sixth breach notification

4.68 On 1 October 2023, CBPL submitted the sixth breach notification to the Authority. CBPL identified that two high-risk customers had been able to purchase cryptoassets via the same third-party payments platform referred to at paragraph 4.64 above. According to CBPL, this breach arose as the control put in place to rectify the breaches subject to the fourth breach of the CBPL VREQ (see paragraphs 4.63 to 4.65) only applied to deposits and not purchases made via this third-party payments platform, resulting in these customers being able to engage in such purchase transactions in the period between their accounts being opened and the assessment as to whether they should be subject to VREQ Flag being completed. This issue persisted until the relevant high-risk restriction was applied to the relevant customer accounts and, therefore, transactions were permitted for a limited amount of time totalling £50.

Impact of the Breaches

4.69 Between 31 October 2020 and 1 October 2023, CBPL repeatedly breached the requirements imposed on it by the CBPL VREQ by:

a) onboarding and/or providing payment or e-money services to 13,416 separate high-risk customers; and

b) permitting approximately 31% of these customers to make 12,912 prohibited deposits with a total value of approximately USD $24.9 million.

4.70 These customers used the deposited monies to make withdrawals and, thereafter, execute multiple cryptoasset transactions via other Coinbase Group entities using the same funds, totalling approximately USD $226 million.

4.71 CBPL submitted SARs in respect of 62 of these customers to alert law enforcement to potential money laundering, scams and fraud, and the sale of illicit substances and stolen credit card information on the darknet. A number of the transactions subject to these SARs were of significant value, with several being in excess of USD $50,000, and the total value of the transactions being approximately USD $1.75 million.

4.72 The Authority considers that the breaches of the CBPL VREQ resulted in a significant increase in the risk of CBPL facilitating financial crime and were unacceptable given the matters already outlined above. These included:

a) CBPL's business model, as it acts as a gateway for UK customers to exchange fiat currency for cryptoassets and vice versa, and the known financial crime risks associated with cryptoassets;

b) the Authority's warnings to payment and e-money firms about weaknesses in the sector, including ineffective systems and controls which had been highlighted as being needed for preventing financial crime;

c) the weaknesses raised in April 2020 about CBPL's financial crime framework having led to the Authority proposing the CBPL VREQ, which was intended to help reduce CBPL's financial crime risk while it enhanced its financial crime controls, and CBPL was aware from both the Authority's feedback to it, as well as to the wider industry, of the importance of this work;

d) the importance that the Authority attached to compliance with the CBPL VREQ, which CBPL ought to have been aware of given the prospect of entering into requirements was first raised by the Authority, there was significant engagement between the Authority and CBPL over its terms and the serious risks it was intended to protect against while the Firm's financial crime control framework was remediated;

e) the extended period of time CBPL had to devise and implement controls to ensure compliance with the CBPL VREQ, having first become aware of the Authority's proposal for requirements to be put in place some three months before they were finalised, along with CBPL being provided the opportunity to input into the terms of the requirements in this period;

f) the failure by CBPL to issue any formal documented framework for ensuring compliance with the CBPL VREQ, nor develop an effective system for monitoring such compliance, until over two years after it first came into force; in addition to not adequately testing whether the controls were effective and operating as intended until October 2022; and

g) the 13,416 high-risk customers (as defined by the CBPL VREQ) who were onboarded and/or provided payment or e-money services from CBPL in breach of the CBPL VREQ, resulting in approximately USD $24.9 million in prohibited deposits being made, and withdrawals (including executing multiple cryptoasset transactions via other Coinbase Group entities using the same funds) totalling approximately USD $226 million being performed by those customers, ultimately leading to SARs being submitted to law enforcement authorities in respect of 62 customers.

CBPL's remediation efforts to date

4.73 Since 2020, CBPL has worked to enhance its financial crime framework, and CBPL continues to do so. The Authority acknowledges the Firm's commitment to ensuring that it has an effective financial crime framework in place.

5. FAILINGS

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

Principle 2

5.2. Principle 2 of the Authority's Principles for Businesses requires a firm to conduct its business with due skill, care and diligence.

5.3. Between 31 October 2020 and 14 April 2023 CBPL breached Principle 2 in relation to the design, testing, implementation and monitoring of the controls put in place to ensure compliance with the CBPL VREQ, as summarised below:

a) CBPL maintained inadequate records regarding the steps it took to ensure compliance with the CBPL VREQ, including in respect of the design and pre-implementation testing of the VREQ Flag;

b) CBPL chose to give effect to the CBPL VREQ by making changes to the automated process used to onboard customers. This required changes to the underlying computer code which were carried out by engineers from another entity within the Coinbase Group. CBPL failed to ensure that these engineers were provided with complete instructions, including the most recent version of the terms of the CBPL VREQ, meaning that, when originally implemented, the

controls gave effect to a previous draft of the terms of the CBPL VREQ and did not give effect to its terms as imposed;

c) the pre-implementation testing of the VREQ Flag was inadequate, as CBPL did not ensure that it operated with respect to all of the various criteria indicating a customer was high-risk, as set out in the CBPL VREQ, nor whether all relevant systems checked for its presence before enabling customers to receive e-money services, resulting in material gaps in its operation not being identified. Comprehensive testing of the effectiveness of the VREQ Flag (and other controls ensuring compliance with the CBPL VREQ) was not in fact conducted until October 2022 onwards;

d) CBPL failed adequately to consider all of the various products and systems through which customers could access e-money services when designing and implementing the VREQ Flag, such as via 'Coinbase Pro' and Coinbase Cards. This was a serious oversight given the prominence of these products and systems, with CBPL describing, for example, 'Coinbase Pro' as one of the Coinbase Group's three primary product offerings at the relevant time; and 8,183 high-risk customers being able to access e-money services as a result of the VREQ Flag not being implemented in relation to this product and the 'Simple Trade Service';

e) CBPL failed to ensure that when certain new systems which enabled customers to effect transactions were introduced, such as the Simple Trade Service, effective controls were introduced to ensure that these new systems did not undermine CBPL's compliance with the terms of the CBPL VREQ;

f) CBPL failed adequately to consider all the various ways in which customers might be onboarded when designing and implementing the VREQ Flag and, crucially, whether an assessment was always conducted at that time to ensure that any high-risk customers seeking to onboard were subject to the VREQ Flag, in particular those customers who migrated from other Coinbase Group entities;

g) the initial monitoring of compliance with the CBPL VREQ, conducted via the PED Dashboard, was inadequate until December 2022 as, prior to that point, it did not track whether customers subject to the VREQ Flag could nevertheless access e-money services, nor whether all customers of CBPL had undergone an assessment as to whether the VREQ Flag should have been applied to their

accounts before being onboarded. Consequently, the breaches underpinning the Second Breach Notification went undetected for a significant period of time, almost 2 years from when the CBPL VREQ came into force, and only came to light inadvertently after a customer lodged a complaint with the Financial Ombudsman Service; and

h) notwithstanding CBPL identifying breaches of the CBPL VREQ shortly after it came into effect, CBPL failed to conduct a formal review of the overall effectiveness of the VREQ Flag until two years after it came into force, nor did the Firm issue a formal documented framework for ensuring compliance with the CBPL VREQ until April 2023. It was around a similar time, from December 2022 onwards, that CBPL also improved its monitoring by developing the Compliance Dashboard. The Authority considers these are the types of steps that CBPL should have been taking much earlier upon the CBPL VREQ first being implemented and the failure to do so contributed to the significant breaches that occurred before these steps had been taken.

Electronic Money Regulations 2011

5.4. During the Relevant Period CBPL repeatedly breached the requirements imposed on it by the CBPL VREQ, pursuant to Regulation 8 of the EMRs:

a) CBPL onboarded and/or provided payment or e-money services to 13,416 separate high-risk customers; and

b) CBPL permitted (approximately 31%) of these customers to make 12,912 prohibited deposits with a total value of approximately USD $24.9 million and to complete withdrawals, including executing multiple cryptoasset transactions via other Coinbase Group entities using the same funds, totalling approximately USD $226 million.

Each high-risk customer onboarded, as well as each deposit and transaction performed by them, constituted a separate breach of the requirements imposed on CBPL by the CBPL VREQ.

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. As explained at paragraph 4.69 of the Notice, the Firm onboarded and/or provided services to 13,416 high-risk customers in contravention of the CBPL VREQ. The Authority considers that the Firm derived the following financial benefit from these customers:

a) revenue from fiat currency withdrawal and/or deposit fees in the sum of £1,505.95; and

b) revenue from bank account interest on fiat currency amounts in the sum of £1,637.54.

6.4. The financial benefit derived from these customers totalled £3,143.49.

6.5. In accordance with DEPP 6.5A.1G, the Authority has charged interest on the Firm's benefit at 8% from 2 October 2023 to 23 July 2024, amounting to £203.25.

6.6. Step 1 is therefore £3,346 (rounded down to the nearest £1).

Step 2: Seriousness of the Breach

6.7. 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 line 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.

6.8. The Authority has therefore determined a figure based on a percentage of the Firm's relevant revenue. The Firm's relevant revenue is the revenue derived from

the 13,416 customers who were onboarded and provided services in contravention of the CBPL VREQ during the period of the breach. The period of the Firm's breach was from 31 October 2020 to 1 October 2023. The Authority considers the Firm's relevant revenue for this period to be £3,143.49.

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:

a) The Firm's breach of the CBPL VREQ created a significant risk that financial crime would be facilitated, occasioned or otherwise occur (DEPP 6.5A.2G (11)(d)). The Firm onboarded and/or provided e-money services to 13,416 high-risk customers, whilst its financial crime control framework was being remediated and, in the Authority's view, remained inadequate to deal with the risks posed by them. Approximately 31% of these customers went on to place 12,912 deposits with a total value of approximately USD $24.9 million and to complete withdrawals, including executing multiple cryptoasset transactions via other Coinbase Group entities using the same funds, with a total value of approximately USD $226 million. SARs were filed with law enforcement authorities in respect of 62 of these customers. The reported value for some of these transactions was significant, with several being in excess of USD $50,000.

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 factors to be relevant:

a) Little, or no, profits were made or losses avoided as a result of the breaches, either directly or indirectly (DEPP 6.5A.2G (12)(a)); and

b) The breaches were committed negligently or inadvertently (DEPP 6.5A.2G (12)(e)).

6.12. The Authority also considers that the following factors are relevant:

a) The CBPL VREQ was put in place to mitigate the Firm's exposure to financial crime risks while it remediated its financial crime systems and controls following the Authority's feedback. Breaches of the CBPL VREQ are therefore considered particularly serious (DEPP 6.5A.2G (7)(a)); and

b) Within the Relevant Period, numerous breaches of the CBPL VREQ occurred, with six notifications of breaches being made to the Authority. The flaws leading to the Second Breach Notification went undetected for almost two years and were identified inadvertently (DEPP 6.5A.2G(7)(b)).

6.13. Taking all of these factors into account, the Authority considers the seriousness of the breach to be level 3 and so the Step 2 figure is 10% of £3,143.48.

6.14. Step 2 is therefore £314.35.

Step 3: Mitigating and Aggravating Factors

6.15. 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.

6.16. The Authority considers that the following factors aggravate the breach:

a) Following the first breach notification, the Authority wrote to the Firm on 20 January 2021 highlighting the importance of adhering to the CBPL VREQ and notifying it that any further breaches or failures to implement the terms of the

CBPL VREQ may result in the Authority taking additional regulatory or enforcement action against the Firm. Despite this warning, the Firm notified the Authority on five further occasions of breaches of the CBPL VREQ within the Relevant Period; and

b) In July 2020, the Authority published a letter sent to CEOs of payment and e-money firms which highlighted weaknesses identified in the sector, including ineffective systems and controls for preventing financial crime. The Authority has published various materials highlighting the enhanced financial crime risks associated with cryptoassets (and although CBPL did not undertake any cryptoasset transactions, customers could use fiat currency in their e-money wallets to purchase cryptoassets via other entities in the Coinbase Group, as many did). As a result, the Firm was, or should have been, aware of the importance of complying with requirements designed to reduce financial crime risk, including the CBPL VREQ.

6.17. The Authority considers that there are no factors which mitigate the breach.

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

6.19. Step 3 is therefore £377.22.

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 £377.22 is too small to meet its objective of credible deterrence; it is likely that similar breaches will be committed by the Firm or other firms in the future in the absence of an increase to the penalty; and the likelihood of detection of such a breach is low.

6.22. In making this assessment, the Authority has considered:

a) The significant size and financial resources of the Firm, including its position within the Coinbase Group;

b) The number, duration and persistence of the breaches, which indicate a significant and long-lasting failure to comply with requirements;

c) The ongoing nature of the breaches, which indicate that the gaps in controls and monitoring continue to persist, over 3 years after the CBPL VREQ was entered into. Indeed, two further notifications of breaches were made to the Authority in March 2024 and May 2024, respectively, with a significant number of additional high-risk customers being onboarded and provided services as a result of these breaches;

d) The fact that, since the Firm's business involves the facilitation of customers to trade with, or through, other Coinbase Group entities, the value of customers to the Firm and to the Coinbase Group may exceed the revenue they pay to the Firm;

e) The significant number of high-risk customers onboarded and/or provided services in breach of the CBPL VREQ (13,416); 31% of these impacted customers then went on to make 12,912 deposits with a total value of approximately USD $24.9 million and to complete withdrawals (including executing multiple cryptoasset transactions via other Coinbase Group entities using the same funds) with a total value of approximately USD $226 million, and CBPL filed SARs with law enforcement authorities in respect of 62 customers;

f) CBPL's lack of due skill, care and diligence was significant given that it involved a failure to comply with the terms of requirements that it had negotiated with the Authority on the basis that its systems would enable compliance and because, from January 2021, it was on notice of the Authority's expectations as to the importance of complying with the terms of the CBPL VREQ and the need for CBPL's senior management to oversee and ensure this compliance;

g) The Firm had been warned that any further breaches or failures to implement the terms of the CBPL VREQ may result in the Authority taking additional regulatory or enforcement action against it;

h) Combating financial crime is one of the Authority's key priorities, and the CBPL VREQ was intended to help reduce CBPL's financial crime risk while it enhanced its financial crime controls. The Authority has published various materials on this for a number of years now and, as a result, imposed substantial penalties on regulated firms for ineffective systems and controls for preventing financial crime;

i) A failure to impose a significant penalty for breaches of this nature, including their duration, persistence and magnitude, may cause firms to consider that compliance with requirements of this type imposed by the Authority is not of significant importance;

j) 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

k) 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 remain undetected.

6.23. Given CBPL acts as a gateway for UK customers to exchange fiat currency for cryptoassets and vice versa, together with the financial crime risks associated with cryptoassets and the increasing use by criminals of cryptoassets to launder funds, the Authority considers that it was important for CBPL to adhere to the terms of the CBPL VREQ to mitigate the financial crime risks posed by high-risk customers, while it remediated its financial crime systems and controls based on the Authority's feedback. The repeated nature of the failings relating to the controls that CBPL put in place to give effect to the CBPL VREQ indicate that the Firm did not take adequate steps to ensure compliance with the CBPL VREQ. VREQs are an important supervisory tool used by the Authority and failures to comply with them are of significant importance.

6.24. The Authority therefore considers that in order to achieve credible deterrence the Step 3 figure should be increased by £5,000,000.

6.25. The Step 4 figure is therefore £5,000,377.22.

Step 5: Settlement Discount

6.26. 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. The settlement discount does not apply to the disgorgement of any benefit calculated at Step 1.

6.27. The Authority and CBPL reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.28. Step 5 is therefore £3,500,200 (rounded down to the nearest £100).

Conclusion as to Penalty

6.29. The Authority hereby imposes a total financial penalty of £3,503,546 on the Firm for breaching Principle 2 and for breaching the CBPL VREQ.

7. PROCEDURAL MATTERS

7.1. This Notice is given to CBPL in accordance with section 390 of the Act, as applied by regulation 62 of, and paragraph 8 of schedule 3 to, the EMRs.

7.2. The following statutory rights are important.

Decision Maker

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

Manner and time of payment

7.4. The financial penalty must be paid in full by CBPL to the Authority no later than 6 August 2024.

If the financial penalty is not paid

7.5. If any or all of the financial penalty is outstanding on 6 August 2024, the Authority may recover the outstanding amount as a debt owed by CBPL and due to the Authority.

Publicity

7.6. Sections 391(4), 391(6) and 391(7) of the Act (as applied by regulation 62 of, and paragraph 8(c) of schedule 3 to, the EMRs) 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. However, the Authority may not publish such information if publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

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

Authority Contacts

7.8. For more information concerning this matter generally, contact Laurenz Maurer at the Authority (direct line: 020 7066 8096/email: laurenz.maurer@fca.org.uk).

Nicholas Hills

Head of Department

Financial Conduct Authority, Enforcement & Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS

RELEVANT STATUTORY PROVISIONS

1.1. Regulation 7(1) of the EMRs provides that the Authority may include in an authorisation under the EMRs such requirements as it considers appropriate.

1.2. Regulation 8 of the EMRs provides that the Authority may, on the application of an AEMI, vary the person's authorisation by imposing a requirement such as may, under regulation 7 of the EMRs, be included in an authorisation.

1.3. Regulation 51(1) of the EMRs provides that the Authority may impose a penalty of such amount as it considers appropriate on an electronic money issuer (which includes an AEMI) which has contravened a requirement imposed on it by or under the EMRs.

RELEVANT REGULATORY PROVISIONS

Principles for Businesses

1.4. 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 section 137A of the Act, as applied by regulation 62 of, and paragraph 2A of schedule 3 to, the EMRs. The relevant Principles are as follows.

1.5. Principle 2 provides:

A firm must conduct its business with due skill, care and diligence.

DEPP

1.6. 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.

The Enforcement Guide

1.7. The Enforcement Guide sets out the Authority's approach to exercising its main enforcement powers.

1.8. EG 19.23.12 states that, when determining whether to take action to impose a penalty under the EMRs, and when determining the level of a financial penalty, the Authority's policy includes having regard to the relevant factors in the applicable parts of chapter 6 of DEPP.