



Central Bank of Ireland Administrative Sanctions Procedure (ASP)

Settlement Notice

To: Coinbase Ireland Limited (CBIE)

Date: 21 October 2026

PART 1. ACTION

1. For the reasons set out in this Settlement Notice, the Central Bank of Ireland is publishing a statement pursuant to Section 33BC(2) of the Central Bank Act 1942 as amended (the **1942 Act**), concerning Coinbase Ireland Limited (**CBIE**) an Electronic Money Institution (**EMI**), for contraventions of the European Communities (Electronic Money) Regulations 2011 as amended (the **EMR 2011**) between 1 November 2020 and 19 August 2025.
2. CBIE has agreed to the facts in Part 2 (the **Undisputed Facts**) and admitted the prescribed contraventions in Part 3 of this Settlement Notice, such that further investigation is unnecessary.¹ On this basis, the Central Bank has decided that it is appropriate to impose the following sanctions:
 - o A reprimand; and
 - o A monetary penalty in the amount of €**4,646,597** reduced to €**3,252,618** after application of the settlement scheme discount.
3. CBIE has agreed to these sanctions;² however the sanctions will not take effect unless they are confirmed by the High Court.³
4. Further details on the prescribed contraventions and sanctions are set out in Parts

¹ Section 33AR(1)(a)(ii) of the 1942 Act: “where there are undisputed facts that in the reasonable opinion of the Bank render an investigation unnecessary, suspects on reasonable grounds that a person is committing or has committed a prescribed contravention...”

² In this case, CBIE has also agreed to dispense with an Inquiry.

³ Pursuant to Section 33 AWA of the 1942 Act.



3 and 4 of this Settlement Notice.

SUMMARY OF REASONS FOR THE CENTRAL BANK'S ACTION

a. Governance, Risk Management and Outsourcing

5. The prescribed contraventions identified in this Settlement Notice reflect serious deficiencies in CBIE's governance, risk management, and operational substance as an Irish regulated entity.
6. CBIE is a wholly owned subsidiary of Coinbase Global Inc. (**Coinbase Group**), a United States corporation. Whilst CBIE can and does benefit from access to the global resources, infrastructure, and expertise of the Coinbase Group, these benefits do not diminish CBIE's responsibility to maintain an adequate presence in Ireland and effective control as an Irish regulated entity.
7. Firms operating as part of larger international groups must demonstrate:
 - The ability to make independent strategic decisions and maintain responsibility for core activities, with appropriate oversight of material risks including outsourced services.
 - Sufficient financial and operational capacity to deliver strategy sustainably and in a customer-centric manner, whilst complying with Irish regulatory and legislative obligations.
 - Effective internal governance arrangements, control mechanisms, and administrative policies designed to enable effective operation, manage risks, and protect customer interests.
 - Effective board oversight to identify, challenge, and constrain excessive risk-taking, with implementation of appropriate risk mitigation measures.
 - Sufficiently integrated governance arrangements and internal control functions with appropriate resources, stature, and expertise to respond to the range of risks facing the firm and safeguard customer interests.
8. CBIE failed to meet these expectations in full. For over four years, CBIE outsourced the critical function of safeguarding Users' Funds⁴ to a US Coinbase Group company without maintaining appropriate local oversight or expertise, thereby breaching Regulation 22(2) of the EMR 2011.

⁴ Users' Funds are funds that have been received from the EMI's customers in exchange for electronic money.



9. CBIE lacked the necessary local skill, expertise, and governance structures to:
- Understand and control the risks in its regulated business;
 - Identify and remediate safeguarding failures when they occurred;
 - Exercise meaningful oversight of critical outsourced functions and the outsourced service provider (**OSP**); and
 - Maintain the substance and appropriate decision-making oversight required of an Irish regulated entity.
10. The Central Bank previously – and clearly - communicated these expectations to all EMLs through in the “Dear CEO” letters of 9 December 2021 and 20 January 2023. Furthermore, these same expectations were directly communicated to CBIE in letters dated 14 July 2022 and 27 March 2023, with those direct communications including risk mitigation programmes (**RMPs**) that CBIE was obliged to implement in order to, *inter alia*, bring their governance structures into line with Central Bank expectations.
11. In particular, the RMPs highlighted that, considering the nature, scale and complexity of its business, CBIE’s governance arrangements were not sufficiently proportionate, appropriate, sound or adequate. The level of outsourcing to the Coinbase Group necessitated, at a minimum, greater oversight to ensure that policies, procedures, corporate governance, risk management and internal control arrangements in place were reflective of the Irish entity and relevant legislation.
12. CBIE did not adequately address these concerns. This inadequate oversight of outsourcing arrangements concerning the safeguarding of Users’ Funds remained substantially unchanged until December 2024, when CBIE appointed a safeguarding directly responsible individual (a **Safeguarding DRI**). This appointment came after the Central Bank carried out an on-site inspection concerning CBIE, beginning in May 2024 (the **Inspection**)⁵ which identified persisting weaknesses in CBIE’s outsourcing arrangements.
13. This failure on the part of CBIE concerning its outsourcing arrangements materially impacted its ability to adequately safeguard customers’ funds in accordance with its regulatory requirements.

⁵ The Central Bank carried out an onsite inspection of the three Coinbase entities in Ireland at that time (CBIE, CBEL and CCIL) which began in May 2024.



b. The Importance of Safeguarding

14. The safeguarding of Users' Funds is a key supervisory priority for the Central Bank and a fundamental requirement for all EMLs under the EMR 2011. Customers entrust their funds to EMLs with the expectation that those funds will be protected and readily available for redemption. If Users' Funds are not adequately safeguarded there is potential for loss or detriment.
15. Regulation 29 of the EMR 2011 establishes clear and mandatory requirements for the safeguarding of Users' Funds. These requirements, and the adequacy of a firm's testing and internal controls around them, exist to protect Users' Funds, particularly in the event of the insolvency of an EML.
16. The Central Bank has been explicit in communicating its expectations regarding safeguarding to EMLs. In a "Dear CEO" letter of 9 December 2021 and a "Dear CEO" letter of 20 January 2023, the Central Bank made clear that:
 - Firms must have robust, board-approved safeguarding risk management frameworks in place;
 - Safeguarding arrangements must be regularly reviewed to ensure ongoing compliance;
 - Firms must notify the Central Bank immediately of any safeguarding issues identified; and
 - The Central Bank has no tolerance for weaknesses in safeguarding arrangements.⁶
17. A key component of safeguarding is segregation i.e. where firms, on a daily basis, separate Users' Funds from all other funds including their own corporate funds, with Users' Funds held in a separate account with a third-party credit institution. Over a period of more than four years, CBIE failed to maintain proper segregation by allowing CBIE Users' Funds to be mixed with non-CBIE Users' Funds. This increased the risk of loss of these funds. These failures occurred despite CBIE's explicit representations to the Central Bank at the time of authorisation that it would implement robust and automated safeguarding arrangements.
18. EMLs utilising the credit institution segregation method to safeguard Users' Funds are obliged to maintain separate accounts for that purpose (**Designated**

⁶ This was repeated in the Central Bank's Payment and E-Money Newsletter (December 2025), the Regulatory and Supervisory Outlook Report 2025 and Regulatory and Supervisory Outlook Report 2026.



Safeguarding Account).⁷ This is a ring-fenced bank account that strictly separates Users' Funds from a firm's own operational money, ensuring e-money customers are protected from corporate insolvency and losses.

19. Maintaining accurate records regarding this account is vital for consumer protection. It mitigates the risk of loss or misallocation of Users' Funds. Firms must have strong internal controls in place to ensure the accuracy and integrity of data and that these controls are subject to regular testing, by both the first and second lines of defence of the EMI's risk management framework.
20. A key control for EMIs is a daily reconciliation of Users' Funds to ensure that EMIs maintain adequate funds in their safeguarding accounts so funds can be swiftly returned to the correct customer, particularly in the event of an EMI's insolvency.
21. CBIE failed to maintain accurate records in relation to its safeguarding obligations. Specifically:
 - The systems, processes and controls CBIE relied upon to calculate its daily safeguarding obligations and to conduct its Treasury Rebalancing Procedure,⁸ contained material errors from July 2022 onwards;
 - Consequently, CBIE did not accurately calculate or fully safeguard Users' Funds during this period; and
 - These errors resulted in the Designated Safeguarding Account being underfunded i.e. a shortfall existed in the account - on a daily basis - for at least 18 months. The maximum daily shortfall in Users' Funds safeguarded by CBIE was €3.4 million in 2023 and €5.2 million in 2024. The average daily shortfall was 0.54% of CBIE's safeguarding obligations in that period, which averaged €323 million in 2023 and €470 million in 2024.
22. These failures in data integrity and records are particularly serious because they directly affected CBIE's ability to comply with its legislative safeguarding obligations. CBIE could not demonstrate adequate internal control mechanisms to validate that Users' Funds were properly segregated and safeguarded because it was unable to accurately calculate how much it was obliged to safeguard on a daily basis.
23. The Central Bank has emphasised that EMIs must ensure that they are keeping

⁷ Any or all of the segregated bank accounts opened by CBIE in order to comply with regulation 29 of the EMR 2011.

⁸ The process of transferring funds in and out of CBIE's Designated Safeguarding Account is to ensure that the funds in the Designated Safeguarding Account match the total safeguarding obligation, undertaken by CBIE on a daily basis.



Users' Funds safe and ensure that all times they can be fully and timely redeemed and returned in a wind-down scenario.

24. CBIE's safeguarding failures could have created significant challenges in a wind-down scenario. Had CBIE become insolvent when the above referenced breaches of their safeguarding obligations were in being, then Users may not have been able to promptly and fully regain their funds. This represents a fundamental failure to meet the Central Bank's expectations regarding wind-down strategy.

c. **Communication and Transparency with the Central Bank**

25. The Central Bank has consistently emphasised the importance of proactive communication and transparency. In the "Dear CEO" letter of 9 December 2021, the Central Bank made clear that firms must:

- Take a proactive approach to communication with the Central Bank;
- Notify the Central Bank as soon as they become aware of any breach or potential breach of legal or prudential requirements; and
- Notify the Central Bank at the earliest possible opportunity of material changes to the business model or safeguarding arrangements.

26. CBIE failed to meet these basic expectations. In particular, the Central Bank has become aware of material changes post-authorisation to CBIE's safeguarding arrangements that were not notified to the Central Bank at the earliest opportunity, or at all. These material changes meant that CBIE's arrangements were no longer consistent with the arrangements assessed by the Central Bank for CBIE's authorisation. These changes were:

- Limited banking infrastructure: CBIE's safeguarding banking partner would not accept Users' deposits denominated in USD directly into the Designated Safeguarding Account located in the EEA. Consequently, Users deposited USD funds into CBIE bank accounts in the US which were then transferred to CBIE's Designated Safeguarding Account through the Treasury Rebalancing Process. This arrangement was contrary to the assurance provided by CBIE that Users' Funds would be deposited directly into and safeguarded in a specific segregated account(s) in a credit institution, separate from operational accounts.
- Users' Funds were routed through bank accounts owned and controlled by other group entities and not in the name of CBIE: Approximately 30 institutional customers were instructed to cease depositing into Silvergate



Bank, Signature Bank and Cross River Bank and were instead instructed to deposit funds into a US bank account of Coinbase Inc. Those funds were then transferred to CBIE's Designated Safeguarding Account, which was not consistent with the direct deposit process that was described and that formed part of the Central Bank's assessment of CBIE's EMI authorisation application.

- Manual processes instead of automation: Safeguarding arrangements relied on significant manual intervention in some cases. This contradicted the automated systems outlined in the authorisation application.
27. These failures to disclose material changes to the Central Bank are more than procedural breaches. As part of the authorisation process, the Central Bank has a gatekeeping mandate to ensure that those who are given access to the wider European market have done the necessary planning to ensure a well-governed and sustainable firm which can adequately safeguard Users' Funds and has robust and appropriate systems in place. The Central Bank cannot fulfil that mandate if firms do not fully adhere to the assurances made at authorisation.



PART 2. UNDISPUTED FACTS

Definitions

In this Settlement Notice:

“Brexit” refers to the withdrawal of the United Kingdom (UK) from the European Union on 31 January 2020.

“CBEL” refers to **Coinbase Europe Limited** an Irish entity previously registered by the Central Bank as a virtual asset service provider (**VASP**).

“CBIE” or the **“Firm”** refers to Coinbase Ireland Limited, an Irish entity authorised by the Central Bank as an electronic money institution.

“CCIL” refers to **Coinbase Custody International Limited** an Irish entity previously registered by the Central Bank as a VASP.

“CBG GmbH” refers to Coinbase Germany GmbH previously a BaFin licensed Crypto Custody and Principal trading business that did not passport into Ireland.

“Coinbase Group” refers to Coinbase Global, Inc. and its subsidiaries, which include CBIE and Coinbase Inc.

“Coinbase Inc.” is a Delaware corporation in the USA and is a wholly owned subsidiary of Coinbase Global Inc.

“Coinbase Ireland” as per the Integrated Assessment Report (the Inspection Report) means the Irish EMI (CBIE), and two previous Irish VASPs (CBEL and CCIL).

“Coinbase UK” or **“CBPL”** refers to CB Payments Limited, a UK EMI authorised by the Financial Conduct Authority.

“Crypto” is a broad term for any cryptography-based market, system, application, or decentralized network.

“Designated Safeguarding Account” refers to any or all of the segregated bank accounts opened by CBIE in order to comply with regulation 29 of the EMR 2011.

“EEA” is the European Economic Area.

“e-money” is electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which—

- (a) is issued on receipt of funds for the purpose of making payment transactions,
- (b) is accepted by a person other than the electronic money issuer, and
- (c) is not excluded by regulation 5.⁹

⁹ Regulation 5 of the European Communities (Electronic Money) Regulations 2011 [S.I. No. 183 of 2011].



“EMI” refers to electronic money institution.

“Fiat Currency” is government issued currency.

“GBP” refers to Great British Pounds or Pounds Sterling.

“Looker” is a business intelligence tool used by CBIE to generate dashboards and reports throughout the Coinbase Group business.

“OSP” refers to outsourced service provider.

“PI” refers to payment institution.

“PSR” refers to the European Union (Payment Services) Regulations 2018.

The **“Safeguarding DRI”** is the person who has responsibility for ensuring that an EMI’s safeguarding processes are performed daily and has responsibility for the approval of the daily reconciliation.

The **“EMR 2011”** refers to the European Communities (Electronic Money) Regulations 2011 [S.I. No. 183 of 2011] as amended by the PSR.

“Treasury Rebalancing Procedure” refers to a daily reconciliation process undertaken by CBIE of transferring funds into and out of CBIE’s Designated Safeguarding Account to ensure that the funds in the Designated Safeguarding Account match CBIE’s total safeguarding obligation.

“USD” refers to United States Dollars.

“Users” refers to EMI customers who use e-money services.

“Users’ Funds” means funds that have been received in exchange for electronic money that has been issued, and includes funds that have been credited to an EMI’s payment account or are otherwise made available to the EMI in accordance with the execution time requirements laid down in the **Payment Services Directive**¹⁰, where applicable, in exchange for electronic money that has been issued.

“VASP” refers to a virtual asset service provider registered with the Central Bank for the purposes of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 to 2021.

¹⁰ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015.



Background

1. CBIE is an EMI which was authorised by the Central Bank in October 2019 and began operating on 1 November 2020. It is a wholly owned subsidiary of Coinbase Global Inc., a United States corporation and is part of the global Coinbase Group. Coinbase Group operates one of the world's largest Crypto asset-trading platforms which allows for the buying, selling, transferring, and storing of Crypto assets. In addition to CBIE, until 31 December 2025, Coinbase Group operated two VASPs in Ireland, CBEL and CCIL.¹¹
2. CBIE facilitates the use of Coinbase Group's trading platform by issuing and redeeming e-money in exchange for Fiat Currency. As CBIE does not handle Crypto asset transactions itself, customers use the e-money CBIE has issued to buy Crypto assets on Coinbase Group's online trading platform via other Coinbase companies. Customers can also convert Crypto assets back into e-money (in Fiat Currency denomination) and store it with CBIE. CBIE passports its services across the EEA and previously also onboarded all customers of CBG GmbH.
3. As an EMI, CBIE is subject to the safeguarding requirements set out in Regulation 29 of the EMR 2011. These requirements are fundamental to the protection of Users' Funds and to maintaining public confidence in the financial system.
4. As part of the authorisation process, CBIE set out a business model and was thereafter obliged to seek approval from the Central Bank of any material changes to that business model and to inform the Central Bank – without undue delay – where any change affected the accuracy of information and evidence provided by CBIE in its application for authorisation, as per Regulation 18 of the EMR 2011.
5. The information provided by CBIE as part of the authorisation process included:
 - a. CBIE would have robust governance arrangements, including:
 - a clear organisational structure with well-defined, transparent and consistent lines of responsibility;
 - effective procedures to identify, manage, monitor and report the risks to which CBIE is or might be exposed to;
 - adequate internal control mechanisms, including sound administrative and

¹¹ On 30 December 2024, the Markets in Crypto-Assets Regulation (MiCAR) introduced a new EU framework for the regulation of crypto-assets. As a consequence, VASP registrations ceased to have effect by 31 December 2025. Coinbase transferred the business of CBEL (a VASP) to a Coinbase Group entity in Luxembourg which was granted authorisation under MiCAR to operate as a Crypto Asset Service Provider (CASP) in that jurisdiction. The Coinbase Group does not operate any CASPs from Ireland.



- accounting procedures; and
 - arrangements, procedures and mechanisms would be comprehensive and proportionate to the nature, scale and complexity of the services provided by the EMI.
- b. Users' Funds would be safeguarded in a specific segregated account(s) in a credit institution, separate from operational accounts;
 - c. A single segregated safeguarding account would be used for receipt, safeguarding and settlement of Users' Funds;
 - d. In the case of insolvency, CBIE's creditors would not be able to access funds in the Designated Safeguarding Account;
 - e. All transaction activity impacting CBIE's safeguarding obligations would be automated, with manual intervention only by exception;
 - f. Reconciliation of the Designated Safeguarding Account would be automated to minimise exposure to human error and fraud;
 - g. Daily reconciliations would be carried out by the OSP, Coinbase Inc., to ensure all transaction activity would reconcile against e-money balances held, which in turn would reconcile with funds held in bank accounts; and
 - h. The outstanding Users' Funds due to Users would be known at any given time.
6. On 9 December 2021, the Central Bank wrote to EMIs and PIs by way of a "Dear CEO" letter outlining its expectations of firms in those sectors. The Central Bank required recipients to complete a comprehensive assessment of their compliance with the following key legislative and regulatory requirements:
 - the firm's safeguarding obligations under Regulation 17 of the PSR and Regulation 29-31 of the EMR 2011; and
 - the conditions of their authorisation.¹²
 7. A board approved attestation confirming completion and conclusion of this assessment was to be provided to the Central Bank by firms in receipt of this letter. In its response dated 31 March 2022, the CBIE board stated it was *"satisfied that the Firm is in compliance with the rules and regulations that apply to an*

¹² For PIs and EMIs these include the PSR, the EMR, the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (as amended), and the Central Bank's Consumer Protection Code.



authorised Electronic Money Institution, specifically in respect of

- *Safeguarding obligations under Regulation 17 of the PSR and Regulation 29-31 of the European Union (Payment Services) Regulations 2018 (sic);¹³ and*
- *Specified conditions and requirements imposed on the Firm's authorisation.*

8. Thereafter, by letter dated 14 July 2022, the Central Bank wrote to CBIE concerning *"a number of significant deficiencies in the Firm's current governance arrangements, which are not appropriate in the context of the nature, scale and complexity of the Firm and are not in line with the commitments made in the Firm's application for authorisation."* That letter included an RMP that CBIE was required to complete. In particular, the letter and the RMP concerned measures related to maintenance of authorisation (pursuant to Regulation 18 of the EMR) and outsourcing. In this regard, the Central Bank required CBIE to ensure that the policies, procedures, corporate governance, risk management and internal control arrangements in place were reflective of the local entity and relevant legislation.
9. A follow up to that letter and RMP was sent to CBIE on 27 March 2023. That letter noted that the risks identified in the RMP sent in July 2022 had not been sufficiently mitigated, and the outcomes sought had not been achieved to the Central Bank's satisfaction. The Central Bank noted that *"the RMPs are being re-issued, with extended timelines together with a number of additional actions required to be undertaken to ensure that the risks identified by the Central Bank are appropriately mitigated."* Furthermore, that letter – as with the letter from July 2022 – noted the need for governance structures and risk management frameworks to be commensurate with CBIE's nature, scale and complexity. CBIE was also reminded that if any part of its control framework was outsourced, CBIE retained responsibility for such outsourced services.
10. On 20 January 2023, the Central Bank again wrote to EMIs and PIs generally by way of a "Dear CEO" letter outlining its expectations of the relevant firms. That letter reiterated that boards and senior management teams must ensure they have the skills and knowledge to meaningfully understand the risks their firm faces and the responsibilities they have. This responsibility also extended to outsourced activities conducted on the firm's behalf by any third party, including any group entity.

¹³ The Central Bank requested the attestation in respect of Regulation 29-31 of the EMR 2011 as opposed to the PSR.



11. That January 2023 letter also stated that firms were obliged to obtain an audit of their compliance with safeguarding obligations. An external third-party provider carried out the audit of CBIE's compliance with its safeguarding framework. It identified 20 findings in respect of oversight, controls, access and segregation.
12. Following those findings, and in light of deficiencies communicated through supervisory engagements and the notification of three safeguarding issues by CBIE to the Central Bank in January 2024 (detailed below), the Central Bank carried out the Inspection, which began in May 2024. The report that followed the Inspection (the "**Inspection Report**") detailed significant issues with, *inter alia*, CBIE's safeguarding and outsourcing arrangements. The Inspection concluded that the absence of local oversight and control of outsourced finance and safeguarding activities in CBIE resulted in an insufficient safeguarding risk management framework. As a result of the Inspection, CBIE was issued with another RMP in January 2025, which was subject to external third-party assurance.¹⁴ That third party assurance was successfully completed by CBIE in early 2026 leading to the closure of the RMP in June 2026.
13. The Investigation commenced in July 2025, concerning the issues set out below.

Issue 1: Outsourcing of Safeguarding Function

Background

14. Regulation 22(2) of the EMR 2011 provides that the outsourcing of important operational functions by EMIs cannot be done in a manner that materially impairs the quality of the EMI's internal control and the ability of the Central Bank to monitor and review its compliance with the EMR 2011.
15. Coinbase Group uses a shared services model for certain centralised functions, which means that companies within the Coinbase Group outsource those functions to other Coinbase Group companies. As part of this arrangement, CBIE outsourced a material proportion of its safeguarding services to Coinbase Inc. by way of an outsourcing agreement.
16. The Central Bank's guidance on outsourcing, including the EBA Guidelines on Outsourcing Arrangements 2019 and the Central Bank's Cross-Industry Guidance on Outsourcing (December 2021), makes clear that:

¹⁴ CBIE also engaged a separate external third party to conduct a review of its daily safeguarding process post the Inspection.



- A firm's board is, at all times, fully responsible and accountable for the setting of the firm's strategies and policies;
- Firms should maintain sufficient substance at all times and not become "empty shells" or "letter-box entities";
- Where operational tasks of internal control functions are outsourced, the firm must exercise appropriate oversight and be able to manage the risks generated by the outsourcing;
- Boards and senior management are ultimately accountable for the effective oversight and management of outsourcing risk; and
- While the performance of functions can be outsourced, boards and senior management cannot outsource their responsibilities.¹⁵

CBIE's Outsourcing Arrangement

17. CBIE outsourced the following safeguarding-related functions to Coinbase Inc.:

- Implementation and operation of safeguarding processes and controls;
- Daily reconciliation of the Designated Safeguarding Account;
- Maintenance of the Looker Report and related data systems;
- Calculation of CBIE's safeguarding obligations; and
- Execution of the Treasury Rebalancing Procedure.

18. The Inspection identified the following deficiencies:

- There was an absence of local skill and expertise available in CBIE to appropriately oversee the core function of managing and safeguarding Users' Funds;
- The people responsible for overseeing both safeguarding and the outsourced services provided by Coinbase Inc. were employees of other Coinbase Group entities (not CBIE) and were based outside of Ireland;
- The second and third line of defence testing of CBIE's outsourcing processes and controls was performed by functions which were also outsourced to Coinbase Inc.; and

¹⁵ The Central Bank Cross-Industry Guidance on Outsourcing (December 2021) Section 4.1 "while the performance of functions and activities can be outsourced, boards and senior management of regulated firms cannot outsource their responsibilities."



- CBIE had not maintained effective oversight, as required under the EBA Guidelines on Outsourcing Arrangements 2019.
19. This outsourcing arrangement resulted in CBIE not having a clear organisational structure with well-defined, transparent and consistent lines of responsibility. It lacked the local skill, expertise, and governance structures necessary to:
- Understand the risks in its regulated business including its OSP;
 - Identify and remediate safeguarding failures when they occurred;
 - Exercise meaningful oversight of critical outsourced functions; and
 - Maintain the substance and independent decision-making authority required of an Irish regulated entity.
20. The Central Bank previously – and clearly – communicated these expectations to all EMLs in the “Dear CEO” letters of 9 December 2021 and 20 January 2023. Furthermore, these same expectations were directly communicated to CBIE in RMP letters dated 14 July 2022 and 27 March 2023. CBIE engaged with the Central Bank in early 2024 – following the self-identification of safeguarding weaknesses – to advise of the implementation of a Control Uplift Programme, aimed at addressing weaknesses previously identified, including governance and conduct risks highlighted in the 2022 and 2023 RMP letters. Despite this, the governance and outsourcing issues identified were not adequately resolved.
21. This ongoing failure on the part of CBIE concerning its outsourcing arrangements had a material impact on its ability to adequately safeguard customers’ funds in accordance with its regulatory requirements.

Issue 2: Mixing of Users' Funds with non-Users' Funds

Collapse of US Banks (March 2023)

22. Regulation 29(2)(a)(i) of the EMR 2011 requires that “*users' funds shall not be mixed at any time with the funds of any person other than the electronic money holder's on whose behalf the funds are held.*” Co-mingling Users’ Funds with group funds, or the funds of other customers without explicit segregation is not permitted under the EMR 2011.
23. In March 2023, three US banks failed, including Silvergate Bank and Signature Bank. Until March 2023, CBIE USD institutional Users made USD deposits directly into a CBIE USD account at Silvergate Bank. These funds were then



transferred to CBIE's Designated Safeguarding Account held with AS LHV Pank (a bank in the EEA) by the end of the following business day, through CBIE's Treasury Rebalancing Procedure.

Issue 2(a): Coinbase Inc. Account Deposits

24. On 2 March 2023, in advance of the failure of Silvergate Bank, CBIE instructed 30 of its institutional Users to deposit funds into a Coinbase Inc. FBO (for benefit of) safeguarding account held at Signature Bank, instead of into Silvergate Bank. The account at Signature Bank was not a CBIE account; it was a Coinbase Inc. account.
25. On 12 March 2023, Signature Bank failed. This did not result in the loss of CBIE Users' Funds. CBIE's institutional Users were then instructed to make USD deposits into the Coinbase Inc. FBO safeguarding account at Cross River Bank. Once again, this was not a CBIE account; it was a Coinbase Inc. account.
26. This meant that CBIE Users' Funds were being mixed with the funds of a third party (Coinbase Inc.), as they were being received and held in a bank account in the name of Coinbase Inc., not CBIE.
27. This practice continued until October 2024 when CBIE opened its own settlement account at Customers Bank. This represents a period of approximately 19 months during which the funds of 30 CBIE institutional Users' were mixed with the funds of Coinbase Inc.
28. CBIE contended that these funds were protected by:
 - Ledgering: Deposits were credited to individual customer ledger accounts even when held in Coinbase Inc. bank accounts;
 - FBO and FDIC:¹⁶ Coinbase Inc. accounts had "For Benefit Of" protections and FDIC insurance; and
 - Statutory Protection: Funds were included in CBIE's custodial obligation calculations;
29. However, these protections do not alter the fact that CBIE Users' Funds were not held in CBIE's own account or in a segregated account in CBIE's name, with the result that Users' Funds were not segregated or safeguarded in accordance with CBIE's regulatory obligations. The requirement in Regulation 29(2)(a)(i) that "*users' funds shall not be mixed at any time with the funds of any person other than the electronic money holder's on whose behalf the funds are held*" is absolute and does not

¹⁶ Federal Deposit Insurance Corporation.



permit exceptions based on ledgering, insurance, or custodial calculations.

Issue 2(b): Coinbase UK Account Deposits

30. In 2020, as a result of Brexit, over 6.3 million customers migrated from Coinbase UK to CBIE. Despite email and in-app notifications from CBIE, some of these CBIE Users did not update their banking information and continued to make deposits into the Coinbase UK segregated safeguarding account.
31. This meant that some CBIE Users' Funds were being mixed with Users' Funds of a third party based outside the EU, as the funds were being deposited in a Coinbase UK account rather than a CBIE account. If Coinbase UK or its banking provider became insolvent, CBIE may not have been able to recover these funds.
32. CBIE notified the Central Bank of this issue on 17 January 2024. From 15 March 2024 CBIE rejected deposits into the Coinbase UK account and automatically returned them to Users. Thereafter, CBIE's internal audit reviewed the remediation process. In August 2025, it discovered that, owing to the manner in which some customers were originally onboarded, a small number (33) of CBIE Users continued to have access to the Coinbase UK account and made deposits into it. As a result, from 19 August 2025 all customers had their ability to deposit into the Coinbase UK account blocked and were requested to accept an updated CBIE user agreement before having the ability to transact again. This represents a breach of Regulation 29(2)(a)(i) for almost 5 years (November 2020 - August 2025).

Issue 3: Failure to Safeguard Users' Funds in the Designated Safeguarding Account

Background

33. Regulation 29(2)(a)(ii) of the EMR 2011 requires that if Users' Funds are still held by the EMI and not yet delivered to the payee or transferred to another EMI by the end of the business day after the day of receipt, they shall be deposited in a separate account in a credit institution.
34. CBIE established a Designated Safeguarding Account with an EEA credit institution to comply with this requirement. However, CBIE failed to ensure that all relevant Users' Funds were always held in this account.

Issue 3(a): Withdrawal of Non-CBIE Users' Funds from CBIE Safeguarding Account

35. In January 2024, CBIE notified the Central Bank that withdrawal requests in EUR from non-CBIE Users had been funded from the CBIE Designated Safeguarding Account. Consequently, CBIE Users' Funds were not properly safeguarded in



CBIE's Designated Safeguarding Account.

36. This happened because Coinbase UK and Coinbase Inc. arranged for CBIE (which usually holds most of the Coinbase Group's EUR) to pay EUR out to customers of Coinbase UK and Coinbase Inc. i.e. non-CBIE customers, who wanted to be paid EUR on the redemption of their e-money. This practice ceased on 19 January 2024.
37. This issue demonstrates that CBIE's safeguarding account was being used for purposes other than safeguarding CBIE's Users' Funds, contrary to the requirements of Regulation 29.

Issue 3(b): Timing Mismatch Issue – Underfunding of Designated Safeguarding Account

38. CBIE relies upon a daily reconciliation process i.e. the Treasury Rebalancing Process, to ensure that Users' Funds are safeguarded. This process involves:
 - Identifying which funds are Users' Funds (i.e., funds that must be safeguarded).
 - Identifying when funds cease to be Users' Funds and must therefore be removed from the CBIE Designated Safeguarding Account.
 - Transferring funds into or out of CBIE's Designated Safeguarding Account and CBIE's corporate bank accounts to ensure that the funds in the Designated Safeguarding Account match CBIE's total safeguarding obligation on a daily basis.
39. To determine the total safeguarding obligation, CBIE uses a software system called "Looker" to generate the CBIE safeguarding obligations report (the "**Looker Report**"). The Looker Report extracts data from various sources, including customer transaction data taken directly from the Coinbase Group ledgering system and separate records identifying the Coinbase Group legal entity to which a customer is contracted.
40. In July 2022, CBIE made changes to the maintenance of the data tables on which Looker Report relied. An unintended consequence of these changes was that the records on which the Looker Report relied presented incomplete information, thus undermining the completeness and accuracy of the Looker Report. For the purposes of the Investigation, this has been identified as the Timing Mismatch Issue. As a result of this issue, CBIE's Designated Safeguarding Account was underfunded.
41. CBIE identified this issue in January 2024. At that time, CBIE was of the view that the issue only impacted currencies not used by CBIE Users (i.e., currencies other than EUR, GBP and USD). However, the Inspection later identified that the issue



affected all currencies and related to both retail and institutional customers.

42. The Timing Mismatch Issue resulted in CBIE consistently underfunding the Designated Safeguarding Account from July 2022 until October 2024 – a period of over two years. CBIE identified underfunding of safeguarded balances every day throughout the period of 1 January 2023 to 27 June 2024. The maximum daily value of underfunding of CBIE Users' Funds in 2023 and 2024 was €3.4 million and €5.2 million, respectively. The average daily shortfall was 0.54% of CBIE's safeguarding obligations in that time period, which averaged €323 million in 2023 and €470 million in 2024.
43. This meant that CBIE failed to fully safeguard Users' Funds during this period. Had CBIE become insolvent during this time, the Designated Safeguarding Account would not have contained sufficient funds to meet CBIE's safeguarding obligations.
44. When the issue was identified in late June 2024, CBIE remediated the shortfall immediately to ensure its daily rebalancing process was accurate. A solution fixing the underlying timing mismatch issue was instituted in October 2024.

Issue 3(c): Unallocated Funds Issue

45. During the Inspection, CBIE identified that, between September 2023 and June 2024, certain unallocated Users' Funds¹⁷ were not appearing in the Looker Report and were therefore not included in the reconciliation calculations (the "**Unallocated Funds Issue**").
46. The failure to include unallocated funds in the reconciliation calculations created further underfunding of CBIE's Designated Safeguarding Account. This issue was due to CBIE's failure to complete appropriate control checks at the point of implementation for a new banking provider. CBIE also failed to implement periodic testing of the unallocated funds files to ensure that all transactions were included in the rebalancing calculation.
47. The Unallocated Funds Issue resulted in CBIE failing to safeguard a portion of Users' Funds for a period of approximately 9 months (September 2023 to June 2024).
48. This issue was remediated in October 2024.

¹⁷ Funds can be unallocated if an incoming deposit cannot be matched to a User (this is known as an "exception"). The following circumstances can lead to unallocated funds: Delay in identifying customers (For example, where an incoming deposit cannot be matched to a CBIE User as the system is unable to identify the beneficiary due to incomplete data being included in the payment to CBIE), refunds, rejected withdrawals, and deposits not requiring safeguarding.



Issue 4: Failure to Notify the Central Bank of Material Changes

49. Regulation 18 of the EMR 2011 requires that where any change affects the accuracy of information and evidence provided by an EMI in its application for authorisation, the EMI shall without undue delay inform the Central Bank in writing accordingly.
50. Regulation 31 of the EMR 2011 requires that where any material change will affect the accuracy of information and evidence provided by an EMI in measures taken for safeguarding of funds in exchange for e-money issued, the institution shall inform the Central Bank in advance and in writing accordingly.
51. CBIE failed to notify the Central Bank of the following changes affecting the accuracy of information provided in its application for authorisation:
 - Limited banking infrastructure: CBIE's safeguarding banking partner would not accept Users' deposits denominated in USD directly into the Designated Safeguarding Account located in the EEA. Consequently, Users deposited USD funds into CBIE bank accounts in the US which were then transferred to CBIE's Designated Safeguarding Account, through the Treasury Rebalancing Process. This arrangement was contrary to the assurance provided by CBIE that Users' Funds would be deposited directly into and safeguarded in a specific segregated account(s) in a credit institution, separate from operational accounts.
 - Users' Funds were routed through bank accounts owned and controlled by other group entities and not in the name of CBIE: Approximately 30 institutional customers were instructed to cease depositing into Silvergate Bank, Signature Bank and Cross River Bank and were instead instructed to deposit funds into a US bank account of Coinbase Inc. Those funds were then transferred to the CBIE's Designated Safeguarding Account, which was not consistent with the direct deposit process described and that formed part of the Central Bank's assessment of CBIE's EMI authorisation application.
 - Manual processes instead of automation: Safeguarding arrangements relied on significant manual intervention in some cases. This contradicted the automated systems outlined in the authorisation application.
52. These changes directly affected the accuracy of information provided by CBIE in its application for authorisation. CBIE's application stated that:
 - Users' Funds would be safeguarded in a specific segregated account(s) in a credit institution, separate from operational accounts, with a single segregated



safeguarding account used for receipt, safeguarding and settlement of these funds.

- All transaction activity impacting CBIE's safeguarding obligations would be automated.

53. This represents a breach of the notification requirements in Regulations 18 and 31 of the EMR 2011.

Part 3. Prescribed Contraventions

1. CBIE has admitted the prescribed contraventions set out below. The entirety of the EMR 2011 is a designated statutory instrument within the meaning of Section 33AN of the 1942 Act.¹⁸ Accordingly, contraventions of the EMR 2011 are “prescribed contraventions” for the purposes of Section 33AN and Part IIIC of the 1942 Act.

2. Regulation 22 (2) of the EMR 2011 provides:

Outsourcing of important operational functions, including information technology systems, shall not be undertaken in a manner that materially impairs the quality of the electronic money institution’s internal control and the ability of the Bank to monitor and review the electronic money institution’s compliance with these Regulations.

3. Regulation 29 (2)(a) (i) of the EMR 2011 provides:

a) users’ funds—

(i) shall not be mixed at any time with the funds of any person other than the electronic moneyholder’s on whose behalf the funds are held.

4. Regulation 29 (2)(a) (ii) of the EMR 2011 provides:

a) users’ funds—

(ii) if still held by the electronic money institution and not yet delivered to the payee or transferred to another electronic money institution by the end of the business day after the day of receipt, shall be deposited in a separate account in a credit institution or invested in assets accepted by the Bank as secure and low-risk;

5. Regulation 18 of the EMR 2011 provides:

¹⁸ See Schedule 2 Part 2 Item 51 of the 1942 Act.



Where any change affects the accuracy of information and evidence provided by an electronic money institution in its application for authorisation in accordance with Regulation 8, the electronic money institution shall without undue delay inform the Bank in writing accordingly.

6. Regulation 31 of the EMR 2011 provides:

Where any material change will affect the accuracy of information and evidence provided by an electronic money institution in measures taken for safeguarding of funds in exchange for electronic money issued, the institution shall inform the Bank in advance and in writing accordingly.

Prescribed Contravention 1

7. In the period from 1 November 2020 to 16 December 2024, CBIE contravened Regulation 22 (2) of the EMR 2011 in the following respects:

- a. There was an absence of local skill and expertise available in CBIE to appropriately oversee the core function of managing and safeguarding Users' Funds until CBIE appointed a Safeguarding DRI on 16 December 2024.
- b. CBIE was excessively reliant on Coinbase Inc. to implement and test safeguarding processes and controls and failed to exert sufficient oversight of this outsourced arrangement.
- c. The outsourcing of the safeguarding function and overreliance on Coinbase Inc. materially impaired the quality of CBIE's internal safeguarding controls in the following respects:
 - CBIE Users' Funds were not segregated and were mixed with non-Users' Funds as outlined at Contravention 2.
 - Users' Funds were not safeguarded at all times in CBIE's Designated Safeguarding Account as outlined at Contravention 3.
 - Safeguarding books and records, necessary to calculate safeguarding obligations, were not accurate as outlined at Contravention 3.

Prescribed Contravention 2

8. From 1 November 2020 to 19 August 2025, CBIE contravened Regulation 29 (2) (a) (i) because CBIE Users' Funds were mixed with non-Users' Funds as follows:

- The mixing of CBIE Users' Funds with Coinbase Inc. funds (March 2023 to October 2024) by allowing CBIE's institutional Users to make deposits directly into Coinbase Inc. USD bank accounts.



- The mixing of CBIE Users' Funds with Coinbase UK funds (1 November 2020 to 19 August 2025) by allowing CBIE Users who had migrated from Coinbase UK to continue to make deposits into the Coinbase UK segregated account.

Prescribed Contravention 3

9. From 1 November 2020 to October 2024,¹⁹ CBIE contravened Regulation 29 (2) (a) (ii) by failing to safeguard Users' Funds in the Designated Safeguarding Account through:
 - Allowing (until 19 January 2024) non-CBIE customers to withdraw funds from the CBIE Designated Safeguarding Account.
 - Consistent underfunding of its safeguarded balances on a daily basis for at least 18 months (1 January 2023 – 27 June 2024).

Prescribed Contravention 4

10. In the period from 1 November 2020 to 17 January 2024, CBIE contravened Regulation 18 and Regulation 31 of the EMR 2011 as a result of its undue delay in notifying the Central Bank of changes affecting the accuracy of information which CBIE had provided in its application for authorisation in the following respects:
 - Limited banking infrastructure: CBIE's safeguarding banking partner would not accept Users' deposits denominated in USD directly into the Designated Safeguarding Account located in the EEA. Consequently, Users deposited USD funds into CBIE bank accounts in the US which were then transferred to CBIE's Designated Safeguarding Account, through the Treasury Rebalancing Process. This arrangement was contrary to the assurance provided by CBIE that Users' Funds would be deposited directly into and safeguarded in a specific segregated account(s) in a credit institution, separate from operational accounts.
 - Users' Funds were routed through bank accounts owned and controlled by other group entities and not in the name of CBIE: Approximately 30 institutional customers were instructed to cease depositing into Silvergate Bank, Signature Bank and Cross River Bank and were instead instructed to deposit funds into a US bank account of Coinbase Inc. Those funds were then transferred to the CBIE's Designated Safeguarding Account, which was not consistent with the direct deposit process described and that formed part of the Central Bank's assessment of CBIE's EMI authorisation application.

¹⁹ This is the relevant operative date on the basis that CBIE did not fully resolve the Timing Mismatch Issue and the Unallocated Funds Issue until October 2024.



- Manual processes instead of automation: Safeguarding arrangements relied on significant manual intervention in some cases. This contradicted the automated systems outlined in the authorisation application.

Part 4. Sanction

1. The Central Bank's approach to the determination of sanctions under the ASP is delineated by the 1942 Act and Part 6 of the Administrative Sanctions Procedure Guidelines 2023 ("**ASP Guidelines**").
2. Having considered all of the available sanctions relevant to a firm as provided in section 33AQ (3) of the 1942 Act, the prescribed contraventions and the Undisputed Facts, the Central Bank has determined that a combination of a reprimand and a monetary penalty in the amount of **€4,646,597** (reduced to **€3,252,618** after application of the settlement scheme discount of 30%) represents a proportionate sanction in the totality of the circumstances. Further details on how the monetary penalty was assessed are set out below.

Determination of the Monetary Penalty

3. The Central Bank followed the steps outlined in Part 6 of the ASP Guidelines in determining an appropriate monetary penalty:

Step 1 – Consider starting point figure

4. The Central Bank can impose a monetary penalty up to a maximum of either 10% of CBIE's annual turnover for the last complete financial year or €10 million, whichever figure is greater. Based on the financial position of CBIE, the maximum penalty that could be imposed in this case is €10 million.
5. The Central Bank considers that the appropriate starting point for the calculation of the monetary penalty should be based on CBIE's average annual gross turnover for the period in which the breaches occurred (1 November 2020 to 19 August 2025). The Central Bank considers this to be a proportionate starting point as the prescribed contraventions were relevant to the entire firm, with one of the breaches persisting for the entirety of the Relevant Period, and the remaining breaches lasting for the vast majority thereof.
6. When rounded, the Starting Point Figure is **€63,219,000**.



Step 2 – Identify and apply the severity level

7. With reference to Table 2 (Nature Seriousness and Effect Factors) of the ASP Guidelines,²⁰ the Central Bank considers the following sanctioning factors as relevant in the assessment of the severity level to apply:
8. One prescribed contravention (Contravention 1 - Outsourcing Failures) is determined to be reckless. The Central Bank's position on outsourcing has been publicly stated through the publication of previous enforcement outcomes and in its publicly available guidance. Furthermore, the Central Bank explicitly told CBIE on 14 July 2022 that it must comply with EBA Guidelines on Outsourcing, which require:
 - (i) the management body to maintain full responsibility for strategies and policies;
 - (ii) firms to maintain adequate local substance and not become “empty shells”;
 - (iii) appropriate oversight of outsourced functions.
9. Despite this, CBIE: (i) continued to outsource critical safeguarding functions without adequate local oversight; (ii) failed to maintain a Safeguarding DRI until December 2024; and (iii) lacked local skill and expertise to manage core regulatory obligations.
10. The manner in which CBIE outsourced its safeguarding obligations (as set out above) was contrary to its regulatory obligations and was undertaken and persisted despite clear and unambiguous regulatory guidance to the contrary.
11. Three (of four) prescribed contraventions are determined to be negligent. They are:
 - Contravention 2 (Mixing of funds): The failures resulted from inadequate system design and insufficient controls to prevent mixing of funds. In particular, CBIE failed to implement adequate preventative measures.
 - Contravention 3 (Failure to safeguard): CBIE allowed certain withdrawal requests in EUR by non-CBIE Users to be funded from the CBIE Designated Safeguarding Account and its systems (the Looker Report) caused the Designated Safeguarding Account to be underfunded.
 - Contravention 4 (Failure to Notify): The failures resulted from inadequate escalation procedures and insufficient governance processes to identify and

²⁰ Paragraph 374 of the ASP Guidelines.



report material changes to the Central Bank.

12. Multiple Safeguarding Breaches: CBIE committed three separate breaches relating to safeguarding (Contraventions 2, 3 and 4), each involving different aspects of the safeguarding obligation:

- Contravention 2: Mixing of funds (failure to segregate).
- Contravention 3: Failure to safeguard (inadequate monitoring and remediation).
- Contravention 4: Failure to notify (inadequate governance and escalation).

The fact that CBIE failed to comply with safeguarding requirements in multiple distinct ways demonstrates systemic weaknesses in its approach to this core regulatory obligation. CBIE also committed serious outsourcing breaches – demonstrating a lack of appropriate skills and experience to oversee the activities of safeguarding undertaken by the OSP - which ultimately had a material impact on its ability to safeguard, further compounding the issues arising.

The Central Bank has consistently stated that the protection of Users' Funds remains one of the most important objectives for the Central Bank and that we have no tolerance for weaknesses in safeguarding arrangements. It is vital that firms have effective and appropriate safeguarding frameworks to ensure that Users' Funds are protected on an ongoing basis.

13. Duration of Breaches: 57.5 months. Specifically:

- Mixing of funds with Coinbase UK: entirety of Relevant Period (57.5 months), November 2020 to August 2025.
- Mixing of funds with Coinbase Inc.: 19 months (March 2023 – November 2024).
- Timing Mismatch Issue: 27 months (July 2022 – October 2024).
- Unallocated Funds Issue: 9 months (September 2023 – June 2024).
- Failure to notify: 38 months (November 2020 – January 2024).
- Outsourcing failures: 49 months (November 2020 – December 2024).

The prolonged nature of these breaches is particularly serious given that they affected the core safeguarding function.



14. Departure from published standards

The Central Bank has published clear guidance and issued communications to industry regarding safeguarding expectations:

- Dear CEO Letter (9 December 2021): Required firms to complete comprehensive assessment of compliance with safeguarding obligations; required board-approved attestation; required immediate notification of any safeguarding issues identified.
- Dear CEO Letter (20 January 2023): Required firms to obtain audit of compliance with safeguarding obligations.
- EBA Guidelines on Outsourcing Arrangements 2019: Required management body to maintain full responsibility for strategies and policies; required firms to maintain adequate substance and not become “empty shells”; required appropriate oversight of outsourced functions.
- The Central Bank’s Cross-Industry Guidance on Outsourcing (December 2021): This sets out the Central Bank’s expectations of the boards and senior management of regulated firms with respect to the governance and management of outsourcing risk.

CBIE significantly departed from these standards. In a letter dated 14 July 2022, the Central Bank specifically advised CBIE that: significant deficiencies existed in CBIE’s governance arrangements; CBIE was required to be in full compliance with the EBA Guidelines on Outsourcing Arrangements; and CBIE must ensure adequate internal control mechanisms and sound administrative procedures.

15. Impact on Financial Markets and Public Confidence

Safeguarding of Users’ Funds is key to maintaining public confidence in the financial system. The breaches as set out above impact public confidence as follows:

- Users entrusted funds to CBIE with the expectation those funds would be protected and readily available, but that was not done adequately by CBIE during the Relevant Period.
- The failure to adequately segregate and safeguard funds impacts public confidence in the operational resilience of firms in this sector.
- The breaches undermine confidence in the regulatory framework for EMIs and in the Central Bank’s oversight.



16. Serious Weakness Revealed

The prescribed contraventions reveal serious weaknesses in CBIE's:

- **Governance:** CBIE failed to maintain effective oversight, including testing, of outsourced safeguarding functions; the governance structures in place did not ensure adequate identification and/or escalation of safeguarding issues.
- **Risk Management:** CBIE failed to identify and remediate safeguarding failures; CBIE failed to maintain adequate data integrity and reconciliation controls; CBIE failed to implement promised automated processes.
- **Operational Substance:** CBIE outsourced key functions to its US entity without appropriate local personnel, expertise or oversight; CBIE lacked local skill and expertise to manage a core regulatory obligation (safeguarding) until December 2024.

17. Customer detriment or potential loss or detriment

While there was no evidence of actual consumer detriment being realised in this case, there was potential for customer detriment if CBIE had become insolvent during the Relevant Period, because Users' Funds were not safeguarded in accordance with CBIE's regulatory obligations. The maximum daily shortfall in Users' Funds safeguarded by CBIE was €3.4 million in 2023 to €5.2 million in 2024. The average daily shortfall was 0.54% of CBIE's safeguarding obligation over that time period which averaged €323 million in 2023 and €470 million in 2024.

18. Having considered these factors, the Central Bank deemed that the correct severity level to apply is **7 on a scale of 1 - 10**. This corresponds with 7% of the Starting Point Figure, i.e. 7% of **€63,219,000** is **€4,425,330**.

The Base Monetary Penalty is €4,425,330

Step 3 – Consider aggravating or mitigating factors

19. The Central Bank may increase or decrease the Base Monetary Penalty to reflect the extent to which the Subject aggravated or mitigated the prescribed contravention. Having considered the factors in Table 3 (Conduct Factors) and Table 4 (Previous Record Factors) of the ASP Guidelines, the Central Bank is satisfied there is one aggravating factor in the case.

Failure to address RMPs adequately

20. CBIE failed to adequately complete two RMPs which were issued by the Central



Bank (July 2022 and March 2023), requiring further Central Bank intervention. These RMPs both addressed, *inter alia*, governance issues, noting that the Firm's governance arrangements were not sufficiently proportionate, sound and adequate taking into account the nature, scale and complexity of its business. The fact that these RMPs and additional regulatory intervention (e.g. the Inspection) were required highlights a continued theme of governance and operational issues that failed to be properly addressed by CBIE. Had it addressed those failings when first required, the breaches would not have persisted or reoccurred over an extended period. This is an aggravating factor.²¹

21. Having considered this factor, the Central Bank has applied an aggravating factor of 5% of the Base Monetary Penalty i.e. 5% of **€4,425,330** which is **€221,267**.
22. The Base Monetary Penalty of **€4,425,330** has been increased by **€221,267** (5% of the Base Monetary Penalty) to **€4,646,597**.

Step 4 – Consider any further adjustment

23. The Central Bank then considers if the Base Monetary Penalty needs to be adjusted by reference to the factors in Table 5 (Other Relevant Considerations) of the ASP Guidelines.
24. The Central Bank does not consider any further factor as relevant. The Base Monetary Penalty remains at **€4,646,597**.

Step 5 – Consider whether any maximum penalty adjustment is required.

25. The Central Bank can impose a monetary penalty up to a maximum of either 10% of CBIE's annual turnover for the last complete financial year or €10 million, whichever figure is greater. As set out above, based on the financial position of CBIE, the maximum penalty that could be imposed in this case is €10 million.
26. As the figure proposed at Step 4 does not exceed that maximum, no maximum penalty adjustment is required.

Step 6 – Consider the sanctions to be proposed in their totality

27. In its approach to determining sanctions, the Central Bank considers the overarching general principles of proportionality, deterrence, and totality. The Central Bank does not consider that the imposition of a reprimand alone would

²¹ See Table 3 (para 3(b)) page 104 ASP Guidelines 2023.



be sufficient in the circumstances of this case to satisfy these principles, due to the serious nature of the prescribed contraventions.

28. In this regard, the Central Bank has considered the nature of the prescribed contraventions, the facts of the case and the circumstances of CBIE, including its size and financial position. The Central Bank considers that the sanctions in this case, being a reprimand and a monetary penalty in the amount of **€4,646,597** are proportionate to the prescribed contraventions and to the circumstances of CBIE. The Central Bank does not consider that any adjustment to the monetary penalty is required, having regard to the overall suite of sanctions to be imposed in the case. No totality adjustment is required / has been made.

Step 7 – Final Monetary Penalty

29. The Central Bank therefore considers that a monetary penalty of **€4,646,597** is appropriate. The final monetary penalty is **€4,646,597**.

Settlement Scheme Discount

30. As this settlement is agreed under the Undisputed Facts Settlement Process,²² the maximum percentage discount which can be applied is 30% in line with paragraph 304 of the ASP Guidelines. In this case, the Central Bank has determined that it is appropriate to apply the maximum percentage discount of 30%. Therefore, the final monetary penalty of **€4,646,597** has been reduced by 30% to take account of the settlement discount.
31. The monetary penalty being imposed is **€3,252,618**.

²² Section 38 of the ASP Guidelines.