capital·com

Disclosures
For the year ended December 31st 2023

Capital Com (UK) Ltd

September 2024

Table of Contents

1. Overview

1.1 Introduction

The disclosures within this document are prepared in accordance with the Financial Conduct Authority (FCA) MIFIDPRU 8 standards.

Capital Com (UK) Limited is a non-SNI MIFIDPRU investment firm and is a wholly owned subsidiary of Capital Com SV Investment Ltd ("CCSV"), regulated by the Cyprus Securities and Exchange Commission (CySEC).

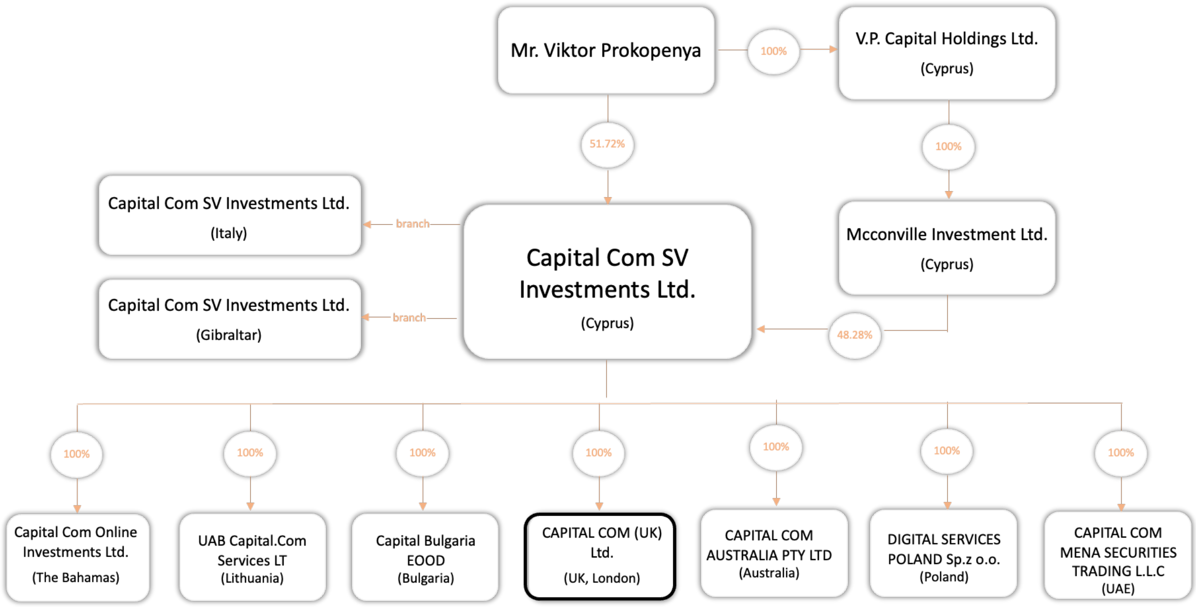
In accordance with MIFIDPRU 8.1.7, the disclosures are compiled on an individual basis for the year ended 31st December 2023. Any references to "the Group" are to Capital Com Group together with all its subsidiary undertakings.

1.2 About Capital Com (UK) Ltd

Capital Com (UK) Limited ("CCUK", "Firm" or "Company") offers financial Contracts for Difference (CFDs) in Forex pairs, Indices, Commodities, Stocks and Cryptocurrencies (available only to professional clients) as well as Spread Betting and Stock Investing services.

CCUK is an execution only firm that operates on a matched-principal basis. It is permitted to deal with retail and professional clients.

1.3 Group Structure and Its Regulated Entities



1.4 Frequency of Disclosures

The disclosures are published on an annual basis, together with the financial statements and are publicly available on CCUK's corporate website (Capital.com).

2. Risk Management Objectives and Policies

2.1 Risk Management Framework

The Company aims to embed explicit and robust risk management practices across its entire business operations, to ensure that the level of risk it faces is consistent with its corporate objectives and its level of risk tolerance. The Risk Management Framework ("RMF") sets out the principles and methods used to identify, assess, report, and mitigate the risk of harm to its clients, to the firm or to the financial markets. The framework also enables the Company to continually align its business objectives against a background of changing risks and uncertainty.

The risk management framework:

- Enables the Company to proactively manage its risks in a systematic manner.
- Ensures that appropriate measures are in place to mitigate risks.
- Helps drive a culture of risk awareness within the Company and
- Ensures that risk management is an integral part of the Company's decision-making process.

The areas covered within the RMF are Risk Culture, Risk Appetite, Risk Taxonomy, Risk Governance and Risk Management.

The Board of Directors ("BoD") sets CCUK's strategic business objectives, in line with delegated authority from the shareholder, whilst having overall oversight of and responsibility for ensuring risk controls and systems are robust and fit for purpose in pursuit of its strategic aims.

The BOD is ultimately responsible for the risk management framework of the Company and for reviewing the effectiveness of the firm's risk management arrangements and the operating effectiveness of the underlying internal controls. These are designed to mitigate the risks of not achieving business objectives, and, as such, offer reasonable assurance against harm, fraud, material misstatement and loss.

The BoD has responsibility for the business' governance and setting the risk appetite of the Group, understanding that risk is an inherent part of CCUK's business model and that the firm's objective is not to eliminate risk but to manage risk to an acceptable level within this defined risk appetite.

The Audit, Risk & Compliance Committee ("ARCC") acts as the Company's Risk Management Committee and has the responsibility to ensure that formal and transparent arrangements are in place for the consideration, monitoring and oversight of the Company's internal control and risk management systems (including credit, market, liquidity, and operational risks to which the Company is exposed), financial reporting, legal and compliance, and internal and external audit. Structurally, risk management is a separate unit independent of the business, with the ARCC reporting directly into the Board.

2.2 Risk Appetite

The Risk Appetite Statement ("RAS") describes and quantifies the level of risk which the firm is willing to accept in pursuit of its strategic objectives. It covers a set of high-level principles that look to balance both the qualitative and quantitative measures that provide an indication of increasing or decreasing risk levels across all relevant risk areas. The review and approval processes are undertaken at least annually.

These are designed to alert the senior management that risk levels are approaching or have exceeded tolerance levels, thus enabling the triggering of an appropriate management response.

2.3 Three Lines of Defence Overview

The three lines of defence model is used in risk management to help establish a system of checks and balances to protect against various risks and to ensure the firm has effective governance.

The first line of defence is assumed at the operating level and includes all principal risk owners who have the primary responsibility for the first line day-to-day risk management activities to ensure that the level of risk in their area remains within risk tolerance. The key responsibilities are:

- Reviewing and evaluating the business risks within each area
- Identifying and assessing the mitigating controls and procedures in place, and the action plans to address any weaknesses in controls.
- Contribute to the holistic view of the organisation's risk through their reporting responsibilities via the relevant governance with overarching Board-level oversight and responsibility.

The Risk and Compliance control functions act as the 'second line of defence' who monitor first line risk management activity, independently oversee, review, and challenge the effectiveness of the first line controls and act in a risk advisory capacity to the business. The role of the second line of defence is:

- To provide guidance and expertise to the first line on risk identification, assessment and control but to also challenge the first line's assumptions to any risks raised
- Review assessments and mitigation strategies defined by each first line of defence area.
- Reviews the breaches and incidents occurring from events, complaints management the appropriateness process for clients, market abuse alerts, financial promotion reviews and relevant CASS reports.
- Conduct independent risk assessments and validations

The 'third line of defence' is the Internal Audit function which are an independent function and has responsibility for safeguarding the firm's assets and reputation by providing independent objective assurance to the Board, Shareholder, and to Executive management team. The Internal Audit function has responsibility to:

- Ensure that all internal policy controls, procedures, and governance structures are suitable and functioning effectively to support the long-term sustainability of the business.
- Provide regular assurance reviews
- Provide recommendations on ways to enhance risk management and control effectiveness and updates to the Committees and Board as part of their annual audit plan.

2.4 Risk Statement of the Firm's Governing Body

The Board of Directors ("BoD") is ultimately responsible for the risk management framework of the Company and to embed a strong healthy risk management culture across the firm. The framework is designed to ensure it has adequate systems, structures, policies, processes, and people within the Company that identify, assess, mitigate, and monitor all internal and external sources of risk that could have a material impact on the Company's operations.

2.5 Principal Risks

Principal Risk	Risk Description	Controls	Appetite Rating
Employee Conduct Breach	**Client mistreatment/failure to fulfil consumer duty** The risk posed due to our employees mishandling sensitive company or client information or requests, potentially breaching internal code of conduct policies and contrary to the four outcomes of consumer duty. This involves the intentional violation of company policies including regarding data security and privacy and the risk of failure to comply with data protection and privacy laws and regulations but also staff behavioural breaches of conduct. Non-compliance with these policies and regulations can result in significant risk of harm alongside potentially severe legal, financial, and reputational consequences.	- HR and Compliance Policies and procedures: The firm ensures that each employee, particularly the first line of defence, has training regarding consumer duty and the potential risk to clients. This includes vulnerability training and best practice when dealing with clients - Transaction and call monitoring: Regular reviews on client transactions and client interactions - Monthly and quarterly consumer duty papers and MI presented to the Best Interests Committee, feeding up to other senior management committees with Board oversight - Regular reviews on whether our products and services offered to clients are suitable vs target market ensuring that clients have the correct knowledge and understanding of these via appropriate educational content - Quality Assurance, managers carry out regular ongoing reviews with customer outcome a main weighted factor in determining CS team performance. - Customer Satisfaction (CSAT) automated for chats interaction to give a better reflective measure of the service and the overall client engagement experience.	L
Regulatory Compliance	**Breach of Regulatory Rules and Implementation** The potential risk of failure to comply with local regulations, incorrect regulatory calculations or inaccurate regulatory reporting. This includes the failure to implement regulatory change (including tax changes and necessary changes to our products, services and technology to meet requirements). Failure to comply with regulation could result in restrictions on the products and services offered to clients and could result in severe business interruption, poor outcomes for clients and regulatory fines. **Lack of due diligence/KYC process or periodic update** The risk of harm resulting from the lack of appropriate due diligence performed and inadequate KYC processes, causing an adverse impact and financial loss to the business, harm to clients and potential wider market harm.	- Regular reviews on regulatory changes and the use of consultants for external expertise and any specific guidances - 4 eye review process on regulatory submissions - Regulator and external horizon scanning notifications set-up to inform the firm on any regulatory changes - Regular reviews on our client counterparties, considering any changes in business models and any potential new risks of harm - Regularly reviewed procedures and policies on KYC and other regulatory compliance to identify any control gaps - Compliance Assurance monitoring, e.g. call monitoring systems implemented to alert the firm on client vulnerability - Regular reviews of events and compliance breaches which could present any potential harm to the firm, client and or market with clear remedial actions and next steps defined	L
Financial Crime	**Financial Crime** The risk and failure to ensure that the clients' information remains up to date with accurate information that can lead to not identifying potential financial crime in a timely manner. This includes a failure to identify transactions which are received from verified sources and that transactions are in line with the client's economic profile, resulting in failure to report suspicious activity. The risk may be triggered from the potential of non-compliance with the Prevention and Suppression of Money Laundering Activities, Market Abuse and Terrorist Financing Law, regulations and directives. **Regulatory Enforcement** Risk of investigation, sanction or enforcement from regulatory authorities/ failure to adhere to Market Abuse Requirements which is there to increase market integrity and investor protection	- Policy and procedures: The firm ensures that each employee has completed financial crime training and the Operations team have established KYC procedures which are challenged and reviewed regularly - AML alerts to notify the firm if any transactions seem suspicious - PEP and Sanctions Screening including regular review procedures - Market Abuse monitoring by first and second lines of defence with committee level MI overseen and challenged - 1st line Call monitoring and 2nd line compliance assurance screening with senior management committee MI oversight - The firm provides execution only services to clients and not advice which could lead to market manipulation or insider trading	L
Process/Governance Failure	**Governance Failure** The lack of suitable management oversight (including senior management responsibility) and accountability across the business which can result in control failings, regulatory breaches and significant harm. This includes the escalation and reporting of management information via the firm's committee structure, ownership of and approval of policies and ensuring the timely embedding of agreed management actions with regards to approval of risk strategy and key operational processes and oversight and implementation of key control improvements.	- Implementation of Risk Management Framework and documented risk appetite with constant review - A robust committee structure with appropriate Terms of Reference for each, defining membership (senior management) responsibilities and regular meetings to discuss relevant management information and raise awareness of potential risks in each area and agree required management actions with key stakeholders - Suitable processes, KRIs and triggers and escalation mechanisms - Independent evaluation of risks within the organisation by a party that is not directly involved in the management of the assessed risks - Conducting Risk and Control Self-Assessment process to identify and review the potential risks within each department across the business, how effective the mitigating controls are and the actions to be taken to minimise the risks identified with clear accountability defined and timelines established	L

capital·com

Hardware Issues Cyber Risk Software Issues Network Issues Data Management/Data Theft	**Cybersecurity Threats**: The risk of harm from exposure, loss of critical assets or sensitive information, or reputational damage, due to a cyber attack or breach of an organisation's network. This includes ransomware, malware, insider threats, phishing attacks, data breaches, hacking, and system intrusions posing significant risk of harm to clients, the firm or the markets. **Technology Downtime**: The risk of harm caused by System outages or failures which can lead to significant trading losses and reputational damage, this includes 3rd party downtime over which Capital may have limited control. This can lead to notable client harm, severe reputational damage and result in significant financial loss for the organisation. **Data Leaks**: The risk posed by unintentional exposure or theft of confidential information, including client data (PII), trading strategies or proprietary algorithms, which could have grave implications regarding trust, compliance, and competitive advantage. Inadequate mitigation of this risk can result in major fines levied by both regulators and separate governing bodies. **Third Party Outsourcing** Failure to identify and take appropriate steps to ensure risks arising from services that are outsourced are known, managed and mitigated. This includes defining and frequently reviewing Critical third parties and critical outsourcing arrangements. **Operational Resilience and Business Continuity** The risk of loss arising from our ability to respond to and overcome adverse circumstances during a severe operational event that might cause financial loss or disrupt our business services. This includes the ability to deliver products or services, meet regulatory requirements, or maintain overall business continuity and to be able to respond and recover in a timely manner.	- Access controls to ensure the correct access authorisation is provided - Load testing to practice the modeling of expected and extreme usage by simulating multiple scenarios and elevated user volumes - Regular cybersecurity audits and penetration testing - Robust back-up data and recovery systems - Regular training on the importance of technology risk, how risks can be identified and mitigated - Sound firewalls implemented - Effective information security policies and procedures - Information security awareness program upon hiring and annually thereafter via Learning management system - Regular Backup Scheduled as per that outlined in the Backup policy, this also has an alerting feature for any failed and or interrupted back ups. - Access right termination	M
Trading and Client Management Issues	**Operational Process Failure** The risk of poor outcomes or client dissatisfaction as a result of direct issues relating to their user experience which could cause significant impact to the reputation of the business and cause a direct/indirect loss of business opportunities. It arises when elements of the products and services provided are unsatisfactory or internal processes fail resulting in poor customer experience. This includes failures in our onboarding processes, incorrect booking of client trading positions (including corporate action misbookings), incorrect pricing of our markets or operational failures in our payments processes. This dissatisfaction can manifest in various forms, including complaints, negative reviews, or, in extreme cases, legal action and can lead to reputational damage, reduction in client retention and client onboarding levels.	- Having secondary/ back-up processes and systems if the primary processes fail, including having secondary payment providers or back up internal methods - Regular front office training to ensure the firm has sufficient knowledge of the products and services offered and how to communicate clearly and effectively with clients and a thorough understanding of policies, manuals and internal systems and processes - Incident and Event Management response teams with escalation criteria and SLAs regarding raising operational risk events, agreeing mitigating actions and identifying and escalating breaches - Identifying operational risk events and producing management information to minimise re-occurrence of events and improving the processes and systems to reduce any negative reputational risk - Before implementation of IT infrastructure changes an approval of Service Owner is required. Based on approval received appropriate changes are implemented and go to the testing stage.	L

Liquidity Risk	**Liquidity Risk** The risk of the firm being unable to meet its short-term obligations when they fall due, or the risk of not having sufficient liquid assets to meet regulatory minimum requirements. The firm's liquidity position could be impacted by poor execution of its hedging strategy over a period of time, or if broker margin requirements increased or expenditure was to increase substantially in the short to medium term. The Group must also manage its liquidity obligations to support other entities within its structure and ensure locally incurred costs are covered and liquid assets requirements are met at all times.	- Daily monitoring and reporting to ensure the firm has sufficient liquid assets to meet its regulatory obligations - Having up-to-date policies and procedures which include how the financial needs of the company are managed and an authorisation process for purchasing and expenditure that minimises the risk of processing errors, internal fraud and duplicate payments. - Having up-to-date policies and procedures which include an internal diversification ratio for counterparties to minimise the potential of concentration risk - Segregating client money and corporate money to reduce the risk of counterparty default - Performing daily reconciliations which are reviewed and approved to minimise financial risk and ensure client and corporate funds are managed in line with regulations	**L**
Credit Risk	**Credit risk** The risk of loss as a result of the inability or failure of a counterparty to meet its contractual obligations in accordance with agreed terms. This could include one of CCSV's bank or broker counterparties or third parties having insufficient funds to meet payment obligations to the firm when they become due. Credit Risk also references the risk of clients failing to meet their margin call and debit balance obligations in the case where they are not covered by Negative Balance Protection.	- Daily monitoring and reporting of the exposures to ensure adequate levels and quality of capital and liquidity are held in light of potentially severe credit risk losses either from clients or financial banking and broker counterparties - Initial and Regular Due Diligence reviews on our client counterparties, considering ay changes in business models and credit profiles and any potential new risks of harm	**M**
Market Risk	**Market Risk** The risk of losses due to the change of the fair value or future cash flows of financial instruments due to price movements in markets. This could be a result of volatile markets to which the firm has large exposures to, and if insufficient hedging is in place, this could cause a loss for the firm	- Continuous monitoring of the client and residual market risk exposures - "Intraday", "end of day" and "end of week" market risk limits agreed and implemented per market to ensure the exposure of the business to the market is within the defined risk appetite. - Triggers with duration thresholds are recorded when exposures reach the limits and KRI's set to determine breaches of Market Risk Policy - Max open position limits per client and per market are set to ensure the risk of losses from potentially large concentrated trade sizes are mitigated - Having diversified broker hedging accounts with counterparties with good systems and financial standing to ensure that hedging trades can be executed efficiently at all times to reduce market exposures when needed	**L - M**
Capital Adequacy Risk	**Capital Adequacy Risk** The risk of having insufficient capital to meet the Company's capital requirements which may result in the firm no longer being able to continue its business activities. This could include falling below the required amount for both the own funds and the liquid assets requirement, or having insufficient funds for on-going operations.	- Production, constant review, senior management challenge, and board oversight and approval of the firm's ICARA and the own funds capital requirements within the assessment - Daily monitoring and reporting to ensure the firm has sufficient own funds capital to meet its regulatory obligations - Conducting on-going risk assessments and reflecting any change in risk profile of the firm resulting from ICARA, RCSAs or other risk reviews or business model changes to capture all potential risks of harm and the amount of own funds capital required to ensure business continuity - Effective capital transferability policies and procedures between entities and the parent company	**L**
Business Strategy Execution and Delivery/Reputational Risk	**Strategy Execution Risk** The risk from poor planning or execution of the business strategy. During business cycles, given market condition fluctuations over time and competitor risk factors this could be further constrained by capacity and capability needs as the business continues to grow and is required to spend time and resource on ensuring strategy is relevant and embedding newly and appropriately designed control and process improvements alongside these change initiatives.	- Regular commercial strategy meetings with senior management and the Board to drive awareness on the direction of the firm and challenge the existing initiatives and priorities in order to mandate clear objectives and goals - Clear project prioritisation and planning with agreed roadmaps for all technology builds relating to commercial initiatives, technology enhancements and control action improvements - Ongoing front office training to ensure clients receive good outcomes from our products and services, the target market is appropriately defined and that customer and market research feedback is taken into account in its strategy - Good internal and external communication strategies and information dissemination procedures to ensure understanding and alignment of client, stakeholder, Board and senior management expectations - Regular research and monitoring of competitor landscape and impact on our products and services by Product team	**M**

3. Governance Arrangements

3.1 Board of Directors

The firm ensures that the BoD and senior management defines, oversees and is accountable for the implementation of governance arrangements that ensure effective and prudent management of the firm, including the segregation of duties in the organisation and the prevention of conflicts of interest, and in a manner that promotes the integrity of the market and the interests of clients.

Regarding the potential risk of conflicts of interest, the firm operates a policy which aims to prevent this from occurring and to ensure awareness of the potential key risks of harm areas across the firm relating to this topic. The firm ensures individual accountability with roles and responsibilities clarified. A three lines of defence model is used within the firm to help establish a system of checks and balances to protect against various risks and to ensure the firm has effective governance.

CCUK ensures that the BoD:

- has overall responsibility for the firm;
- approves and oversees implementation of the firm's strategic objectives, risk strategy and internal governance;
- ensures the integrity of the firm's accounting and financial reporting systems, including financial and operational controls and compliance with the regulatory system.
- oversees the process of disclosure and communications;
- has responsibility for providing effective oversight of senior management;
- monitors and periodically assesses:
  - the adequacy and the implementation of the firm's strategic objectives in the provision of
  - investment services and/or activities and ancillary services;
  - the effectiveness of the firm's governance arrangements; and
  - the adequacy of the policies relating to the provision of services to clients, and takes appropriate steps to address any deficiencies; and
- has adequate access to information and documents which are needed to oversee and monitor management decision-making.

The persons proposed for appointment to the Board should commit the necessary time and effort to fulfil their obligations. Main factors influencing the decision to propose the appointment of potential Directors include:

- are of sufficiently good repute;
- possess sufficient knowledge, skills, and experience to perform their duties;
- possess adequate collective knowledge, skills, and experience to understand the firm's activities, including the main risks;
- reflect an adequately broad range of experiences;
- commit sufficient time to perform their functions in the firm; and
- act with honesty, integrity, and independence of mind to effectively assess and challenge the decisions of senior management where necessary and to effectively oversee and monitor management decision-making.

As at 31st December 2023, the Board is comprised of 3 executive directors and one non-executive directors:

Full name of Director	Number of executive directorships	Number of non-executive directorships
Rupert Simon Toby Osborne	1	
Sheena Kanabar	1	
Kypros Christopher Zoumidou*	3	
Philip John Anderson		0

**Please note that as at May 2024 Kypros Christopher Zoumidou is no longer a director of CCUK*
*** In accordance with MIFIDPRU 8.3.2, the above directorships are out of scope for this analysis:*

- *Executive and non-executive directorships held in organisations which do not pursue predominantly commercial objectives; and*
- *Executive and non-executive directorships held within the same group or within an undertaking (including a non-financial sector entity) in which the firm holds a qualifying holding*

3.2 Governance Committees

A range of governance committees have been formed to achieve a level of robust governance oversight to adequately monitor CCUK's operational effectiveness and its potential risks.

This includes the Audit, Risk and Compliance Committee, which is CCUK's Risk Management Committee (RMC), provides advice on the current and future risk appetite and strategy, and that formal and transparent arrangements are in place for the consideration, monitoring and oversight of the firm's internal control and risk management system, financial reporting, legal and compliance and internal and external audit. The committee also ensures that relevant policies and procedures are effectively implemented and executed to comply with legal and regulatory requirements and that risks are mitigated to the degree required by the Board.

Other committees which CCUK have are:

- Executive Committee – to assist the Managing Director in the performance of their duties within the bounds of its authority and are also responsible for the continual and thorough consideration of the firm's obligations under the FCA's new Principle 12 – The Consumer Duty – and shall ensure that the duty is considered and addressed as part of the decisions made by the Committee
- CASS Committee – assist the firm with the work of the Board in respect of all risks that may affect the business related to CASS
- Best Interests Committee – to assist the firm in respect of all risks to the business related to the fair treatment of clients, including its short medium and long term strategy impacting client related matters

A Group remuneration committee, Group Risk Committee, Group Technology Committee, Group Client Money Committee and Group Pricing Committee, also meets regularly to consider all global matters relating to each area. Where the Board delegates certain responsibilities, it reviews the decisions of these committees at each of its meetings to ensure these committees are not only challenging the information that it is presented, but that the decisions taken are in alignment with the Company strategy and risk appetite. Senior management of these committees are responsible for ensuring effective communication and alignment between different entities and the Group.

3.3 Diversity

The firm recognises the importance of skilled, diligent and accountable leadership in a diverse and inclusive workplace that represents the interests of all key stakeholders and the Board. The Group Diversity, Equity and Inclusion ("DEI") Policy applies to any employee, contractor, or Non-Executive Director ("NED") working for or engaged by any Group Company. The purpose of the policy is to encourage and promote DEI in all aspects of our work and business and promote an internal culture that values difference and recognises that people from different backgrounds and experiences can bring valuable insights to the workplace.

CCUK commits to encouraging and promoting DEI in the workplace; ensuring we do not discriminate in our recruitment processes and procedures; creating and maintaining a working environment free of bullying, harassment, victimisation and discrimination; taking seriously any complaints; providing opportunities for training, development and progression for all staff; making decisions concerning Team Members based on ability and merit; ensuring we work to avoid and eliminate unconscious bias, and reviewing employment practices.

Capital Com Group's workforce is a diverse one which is reflected in the Diversity & Inclusion reports produced internally. An Unconscious Bias ("UB") provider conducted training to the Senior Leadership Team ("SLT") and for all employee's company-wide in Q4 2023.

4. Own Funds

The own funds amount for CCUK derives from common equity tier 1 capital ("CET1"), comprising from share capital and retained earnings. Further detail of this can be seen in the below tables.

Table 1: Composition of regulatory own funds			
	Item	**Amount (GBP thousands)**	Source based on reference numbers/letters of the balance sheet in the audited financial statements
1	**OWN FUNDS**	**7,369**	
2	**TIER 1 CAPITAL**	**7,369**	
3	**COMMON EQUITY TIER 1 CAPITAL**	**7,369**	
4	Fully paid up capital instruments	4,699	i
5	Share premium		
6	Retained earnings	1,670	ii
7	Accumulated other comprehensive income		
8	Other reserves	1,000	iii
9	Adjustments to CET1 due to prudential filters		
10	Other funds		
11	(-) TOTAL DEDUCTIONS FROM COMMON EQUITY TIER 1		
12	CET1: Other capital elements, deductions and adjustments		
13	**ADDITIONAL TIER 1 CAPITAL**		
14	Fully paid up, directly issued capital instruments		
15	Share premium		
16	(-) TOTAL DEDUCTIONS FROM ADDITIONAL TIER 1		
17	Additional Tier 1: Other capital elements, deductions and adjustments		
18	**TIER 2 CAPITAL**		
19	Fully paid up, directly issued capital instruments		
20	Share premium		
21	(-) TOTAL DEDUCTIONS FROM TIER 2		
22	Tier 2: Other capital elements, deductions and adjustments		

Table 2: Own funds: reconciliation of regulatory own funds to balance sheet in the audited financial statements		
	Balance sheet as in published/audited financial statements	**Cross-reference to template OF1**
	As at 31.12.23 (£'000)	
ASSETS		
Non-current assets		
1 Property, plant and equipment	7,577	
2 Right-of-use assets	10,288	
Current assets		
1 Trade and other receivables	3,147	
2 Cash and cash equivalents	9,175	
TOTAL ASSETS	**30,187**	
LIABILITIES		
Non-current liabilities		
1 Lease liabilities	10,304	
2 Deferred tax liability	635	
Current liabilities		
1 Trade and other liabilities	10,367	
2 Corporation tax payable	-	
3 Lease liabilities	1,512	
TOTAL LIABILITIES	**22,818**	
SHAREHOLDERS' EQUITY		
1 Share capital	4,699	i
2 Other reserves	1,000	Iii
3 Retained earnings	**1,670**	ii
TOTAL EQUITY	**7,369**	
TOTAL EQUITY AND LIABILITIES	**30,187**	

Table 3: Own funds: main features of own instruments issued by the firm		
	Features of own instruments	**Cross-reference to template OF1**
Share capital	Instrument type: Ordinary share Amount recognised in Regulatory Capital (£000'): 4,699 Nominal amount of instrument: GBP 1 Accounting classification: Ordinary share capital	i

5. Own Funds Requirements

5.1 Own Funds Requirement

In accordance with MIFIDPRU 4.3.2, CCUK must at all times maintain own funds that are at least equal to its own fund's requirement.

The own funds requirement of a non-SNI MIFIDPRU investment firm is the highest of:

- Its permanent minimum capital requirement (PMR)
- Its fixed overhead requirement (FOR)
- Its K-Factor requirement (KFR)

The below table shows the own funds requirement in further detail:

Table 4: Overall financial adequacy rule (OFAR)	
Permanent minimum requirement	£190k (transitioning to £750k by Jan 2027)[1]
Fixed overhead requirement	£5.35m
K-Factor requirement	£926k

[1]MIFIDPRU TP 2 Own funds requirements: transitional provision 2.18

5.2 K-Factor Requirement

The K-Factor requirements considers the Risk of Harm to Clients (RtC), Markets (RtM) and the Firm (RtF) and these are broken down as follows:

Table 5: K-Factor requirement	Amount (£'000)
The sum of the K-AUM, K-CMH and K-ASA requirements	100
The sum of the K-COH and K-DTF requirements	119
The sum of the K-NPR, K-CMG, K-TCD and K-CON requirements	707
TOTAL	926

**Assets Under Management ("K-AUM"), Client Orders Handled ("K-COH"), Cleared Margin Given ("K-CMG") and Concentration Risk ("K-CON") is not applicable for CCUK*

The K-Factor requirements applicable for the Firm are:

- Client Money Held ("K-CMH")
- Assets Safeguarded and Administered ("K-ASA")
- Daily Trading Flow ("K-DTF")
- Net Position Risk ("K-NPR")
- Trading Counterparty Default ("K-TCD")

5.3 Assessment of Own Funds

In addition to the own funds requirements, CCUK must at all times hold own funds and liquid assets which are adequate, both as to their amount and their quality, to comply with the Overall Financial Adequacy Rule (OFAR) to ensure that:

- The firm can remain financially viable throughout the economic cycle, with the ability to address any material potential harm that may result from its ongoing activities; and
- The firm's business can be wound down in an orderly manner, minimising harm to consumers or to other market participants.

CCUK conducts an annual ICARA process to ensure that it has appropriate systems and controls in place to identify, assess and monitor potential material harms which may not be fully accounted for in the K-Factor requirements or from the ongoing operation or winding down of the business.

The higher of the own funds requirement and assessment of own funds is used as the Own Funds Threshold Requirement (OFTR) and Liquid Assets Threshold Requirement (LATR) which CCUK must hold at all times to comply with the OFAR.

CCUK has a framework for monitoring the adequacy of liquidity and financial resources and performs daily calculations and monthly monitoring reports. This information is provided to the Board who consider it when assessing risk strategy and risk appetite.

If there are any material changes in the Firm's business model or operating model, the ICARA is to be reviewed and updated when required.

6. Remuneration Policy and Practices

In line with MIFIDPRU 8.6, the disclosure requires the Firm to provide information about its approach and components for remuneration.

6.1 Remuneration Approach and Group Remuneration Policy

The Group Remuneration Policy is relevant to all Group entities, which includes the Company. Under a strict framework, the policy sets out remuneration practices for the Group. In accordance with SYSC19G.1.24G of the FCA Handbook, the Group Remuneration Policy applies to:

- All Group Employees (including Senior Management, Executive Directors, material risk takers, and staff engaged in control functions and sales based roles) (together, the "Employees");
- Non-executive members of the Board of Directors.

The Group undertakes practices under appropriate internal procedures, taking into account the interest of all of the Employees of the Group, with a view to ensure they are treated fairly, and a balanced approach is applied to -

- Financial and non-financial remuneration; and
- Fixed and variable remuneration.

The Framework is unbiased considering both individual employee and business performance, so that the remuneration does not favour the interest of the Group or any one individual employee. No external parties are used in the development of the remuneration policies and practices.

The Group Remuneration Policy aims to:

- Provide for sufficient incentives so as for all individuals, to achieve their agreed objectives in line with the Group's strategy; and
- Deliver an appropriate link between reward and performance whilst at the same time become a comprehensive, consistent, and effective risk management tool that prevents excessive risk taking and/or mis-selling practices considering financial incentives schemes, which could lead to compliance risks for the Group in the long-run.

The Group ensures fair remuneration in line with local standards for all geographies where it has a presence. The following aspects are taken into consideration:

- Place of employment and costs of living;
- Level and responsibilities of each individual;
- Local market (overall and with regard to specific roles);
- Qualifications and certifications; and
- Overall remuneration package.

6.2 Risk Management

The Company recognises the importance of promoting sound and effective risk management which promotes responsible staff behaviour linked to risk adjusted performance. In this respect, the Company aims to provide an appropriate remuneration environment where employees are not incentivised to take inappropriate and/or excessive risks which are not in line with the Company's risk approach.

6.3 Remuneration Elements

6.3.1 Financial Incentives

The Company's remuneration includes:
Financial Remuneration (i.e. salary, allowances, and variable incentives); and/or
Non-financial Rewards i.e. career progression or applicable benefits (such as health insurance, events, seminars, upskilling, etc.);

Fixed and variable Remuneration is different for each position/role depending on the position's actual requirements, and it is determined in a way that reflects the role performed by the person and the specific requirements for the role.

Factors taken into account in order to define Remuneration for all Employees are the following:
the financial viability of the Company,
the individual's performance is measured based on achievements, professional development, compliance with the Company's policies and procedures, compliance with regulatory requirements, commitment, etc.)

6.3.2 Variable Incentives

The Company applies a variable remuneration approach across all Sales based roles and operates a sales commission scheme which is both fair and transparent, and which has been designed to deliver good outcomes for the Company's customers.

For eligible Employees, work performance will be assessed on a yearly basis (depending on roles and responsibilities); assessment will start upon commencing employment, by their managers, according to the plan which the relevant Employees are eligible for.

Depending on the department, the following items may be measured:

- Response time to Client emails or chats;
- Scoring of Employees from call monitoring results;
- Time required for the execution of a withdrawal request;
- Number of conversions per month; and/or
- Other criteria as defined by individual plans.

The Company also evaluates qualitative criteria which can be adjusted as appropriate to reflect behaviours and performance in relation to risk and compliance behaviours. Those responsible to approve variable pay-outs are informed of relevant risk and compliance issues, breaches or failure which might affect those decisions. Examples of the criteria are:

- customer satisfaction rating for tickets and chats;
- Number of Client complaints received;
- Knowledge of the industry and how the Company operates;
- Compliance with the Company's processes and procedures;
- Understanding of how to work with other teams; and
- Teamwork, creativity, and engagement.

All other Employees (outside of the Sales team) are eligible to be considered for the Company Discretionary Annual Bonus Plan. The overall bonus pot is defined based on the Company meeting its strategic objectives in line with the business plan set by the Board at the beginning of each year and the Company's overall compliance with the regulatory frameworks. The discretionary element of this plan enables risk and compliance considerations to be taken into account.

For Employees eligible for the annual discretionary bonus, the following three (3) main criteria will be assessed:

- Company performance and compliance (access and overall bonus pot definition)
- Employee start date
- Individual performance (including compliance with overall policies and procedures)
- Achieving personal objectives/OKRs/KPIs.

6.3.3 Fixed Remuneration

All Company Employees receive a fixed base salary which is relevant to their role and function. In line with Global Performance Review, the base salary is reviewed on an annual basis.

6.3.4 Benefits

Benefits and perks provided to individuals are not Employee performance-related and are considered part of the fixed Remuneration. All Employee benefits are benchmarked according to the market conditions and competitors.

6.3.5 Pension

Employees receive a pension in line with statutory requirements. The Company promotes diversity, ethics, fairness, and inclusion best practices. In addition, it is gender-neutral in its application and is designed to create equal remuneration opportunities based on objective considerations.

6.4 Performance Review and Remuneration Cycle

The performance review process, in line with the Group Remuneration Policy, is based on long-term performance. Performance is formally reviewed annually thereafter with the Performance Cycle being January to December each year.

6.5 Decision Making Process

The principles for setting Remuneration are considered, reviewed, and approved by the Group Remuneration Committee which also oversees Company Employees. The Remuneration Committee meets regularly to consider all global matters relating to Remuneration.

The actual levels of Remuneration for new roles, and any changes to Remuneration for existing Employees must be authorised and agreed by the Group Chief Executive Officer.

Managers and Department Heads may make suggestions and recommendations on appropriate levels of Remuneration and indeed are likely to be asked to provide such information during the remuneration cycle and from time to time as appropriate.

The process for agreeing remuneration changes is as follows:

1. Recommendations are sought or provided from an Employee's Manager;
2. Recommendations are sought or provided from an Employee's Head of Department;
3. Heads of Department will agree proposed changes to Remuneration following discussion with HR;
4. HR and Heads of Department will recommend proposed changes to the Chief Executive Officer;
5. The CEO will approve or reject the proposed changes; and
6. HR will liaise with the Company's Legal Department to produce appropriate documentation on Remuneration to be sent to Employees to confirm changes.

6.6 Material Risk Takers

In accordance with SYSC 19G.5, the Company identifies individuals whose professional activities have a material impact on the Company's risk profile. Such individuals are known as Material Risk Takers (or

"MRTs"). The Company has applied the criteria set out at SYSC 19G.5.3R to identify the relevant individuals.

The Company's annual remuneration to Senior Management, Material Risk Takers, and staff members for 2023 was as follows:

	No. of Staff	Fixed Remuneration for 2023 (GBP)	Variable Remuneration for 2023 (GBP)	Total Remuneration for 2023(GBP)
Senior Management*	4	1,077,735	124,386	1,202,121
Material Risk Takers	5	964,372	34,959	999,331
Other staff members	156	10,360,426	2,623,170	12,983,596

**Please note that some Senior Management will also be Material Risk Takers*

Any severance pay would be paid in line with statutory requirements. No severance payments were to MRTs in 2023.

7. Investment Policy

In accordance with MIFIDPRU 8.7.6, a MIFIDPRU firm should disclose information regarding its investment policy:

- Only in respect of a company whose shares are admitted to trading on a regulated market;
- Only where the proportion of voting rights that the MIFIDPRU investment firm directly or indirectly holds in that company is greater than 5% of all voting rights attached to the shares issued by the company and;
- Only in respect of shares in that company to which voting rights are attached

As CCUK does not meet the requirements above, it is not required to make the disclosures in relation to its investment policy.

8. Further Information

Questions to this Report should be addressed to the Compliance Department: compliance.uk@capital.com