FCA
Financial Services Consumer Panel

Telephone: 020 7066 9346
Email: enquiries@fs-cp.org.uk

12 November 2025

By email: cp25-25@fca.org.uk

Dear FCA,

The Financial Services Consumer Panel[1] welcomes the opportunity to respond to the FCA's Consultation Paper on proposed rules and guidance for cryptoasset firms across the Handbook.

We commend the FCA's efforts to enhance consumer protection, market integrity, competition, and international alignment in this rapidly evolving sector. These proposals could potentially impact 12% of the UK adult population (7 million people who currently own cryptoassets[2]), with over a quarter (27%) of cryptoasset users surveyed reporting that they have bought stablecoin, which is certainly noteworthy.

The Panel recognises the importance of establishing a clear and robust regulatory framework for cryptoassets, one that ensures consumers are appropriately protected. The Panel supports the overall direction of the FCA's proposals but emphasizes the need for tailored, enforceable rules that reflect the unique risks and dynamics of the cryptoasset market.

The Panel responses to the questions posed in the Discussion Paper are included at Annex A below. The Panel continues to appreciate the FCA's efforts and looks forward to further engagement on these topics.

Yours sincerely,

Chris Pond

Chair, Financial Services Consumer Panel

[1] https://www.fca.org.uk/panels/consumer-panel
[2] https://www.fca.org.uk/publications/research/research-note-cryptoassets-consumer-research-2024 and https://www.gov.uk/government/news/new-cryptoasset-rules-to-drive-growth-and-protect-consumers

Annex A – responses to questions.

Chapter 1

1. **Do you agree that new cryptoasset activities defined in the SI (and as described as 'qualifying cryptoasset activities' in draft FCA Handbook rules) should fall under the category of 'designated investment business' for the purposes of applying relevant sections of the Handbook?**

Yes, the Panel agrees that new cryptoasset activities defined in the Statutory Instrument (SI)[3] and described as 'qualifying cryptoasset activities' in the draft FCA Handbook rules should fall under the category of 'designated investment business' for the purposes of applying relevant sections of the Handbook.

Aligning qualifying cryptoasset activities with designated investment business ensures consistency across the FCA's regulatory framework. It also helps firms better understand their obligations, especially in areas such as client protection, disclosure, and conduct of business.

Treating qualifying cryptoasset activities as designated investment business allows the FCA to apply robust appropriateness assessments and consumer safeguards. It also reinforces the legitimacy of regulated cryptoasset firms signalling to consumers that these activities are subject to the same standards as traditional financial instruments, which is critical for consumer trust and market stability.

The Panel believes that embedding, where possible, cryptoasset activities within existing regulatory categories allows for scalable oversight. It avoids the need to create parallel frameworks and ensures that innovation is balanced with accountability.

Chapter 2

2. **Do you agree with our proposal for applying high level standards to cryptoasset firms in a similar way they apply to traditional finance?**

From a consumer perspective, the Panel broadly agrees with the proposal to apply High Level Standards (COND, PRIN, GEN and SUP) to cryptoasset firms as a necessary step towards building trust, safety and accountability in the crypto market. Consumers need consistent protection, transparency

---

3 https://assets.publishing.service.gov.uk/media/680f6387faff81833fcae94b/0302425_draft_RAO_SI.pdf , page 25.

and market integrity, to gain greater confidence that their interests are being protected.

While High-Level principles provide a strong foundation, firms may interpret these principles inconsistently. We therefore encourage the FCA to publish a practical guidance showing how these principles apply to crypto activities (custody, staking and stablecoin). The Panel also believes that incorporating illustrative use cases would enhance clarity and facilitate consistent application.

Consumer Awareness Campaign, Disclosures and Testing.

The Panel believes that High-Level Standards will work best when consumers understand what they mean and can hold a firm accountable. We therefore encourage the FCA to complement the rules with consumer awareness campaigns and testing, so that consumers can recognise warning signs of non-compliance.

The Panel also continues to urge the FCA to ensure that retail consumer disclosures and rules are clear and free of technical jargon. We consider that the FCA should use consumer testing to inform disclosure rules for cryptoasset activities in order to maximise their effectiveness.

Disapplication of PRIN 1, 2, 6 and 9 for transactions entered into a CATP by its members

The Panel does not agree with the proposal to disapply Principles 1 (Integrity), 2 (Skill, Care and Diligence), 6 (Customers' Interests), and 9 (Suitability) to transactions entered into on a Cryptoasset Trading Platform (CATP) by its members.

We believe this approach creates a significant protection gap for retail investors, who in the cryptoasset market often have direct access to CATPs and transact without intermediaries. Unlike traditional financial markets, where retail investors access multi-lateral trading venues (MTVs) through authorised brokers or firms that owe them conduct and suitability duties, most cryptoasset trading platforms (such as Binance, Coinbase, Crypto.com, or Kraken) allow retail users to open accounts, hold assets, and trade directly on the platform. This means there is no intermediary layer to uphold consumer protection obligations on behalf of retail clients.

While we recognise that certain transaction-level duties may not be practical to apply to peer-to-peer trades, we believe PRIN should continue to apply fully to the CATP itself in its dealings with retail investors. Disapplying these key Principles (Integrity, Skill and Care, Customers' Interests, and Suitability) from consumer transactions risks leaving retail

investors exposed, as there is no intermediary layer to carry those duties, as there would be in traditional markets.

Furthermore, the FCA's current proposals aim to protect consumers from misconduct by platforms, but not from the inherent risks of trading cryptoassets. Without a requirement for suitability assessments, platforms will not be required to consider whether trading cryptoassets is appropriate for individual consumers. This approach preserves the structural integrity of the trading venue but does not directly protect consumers from poor decisions or market losses.

The Panel therefore believes the FCA should adapt its approach to reflect the direct-access nature of crypto trading platforms. We recommend that the FCA retain PRIN 1, 2, 6, and 9 for CATPs in respect of their relationships with retail clients, to ensure that both the platform and the individuals facilitating trades behave responsibly.

The Panel understands that CATPs are there to facilitate trading, not to provide advice, and that applying suitability and customer-interest duties to every single transaction would be unworkable, especially in an open crypto marketplace where thousands of trades can occur per second. However, we propose that suitability assessments are carried out when the consumer is onboarded, for large and irregular transactions and on a regular basis, rather than per transaction, and that the Consumer Duty be applied as soon as possible to introduce outcome-based obligations ensuring that consumers receive fair value and genuinely understand the nature and risks of their activities.

Consumer Duty

As noted above and in the Panel's responses to DP23/4 on stablecoins and in the most recent response to DP25/5 for Chapters 6 and 7, the Panel is strongly supportive of firms being subject to the Consumer Duty (CD) for all cryptoasset activities, supported by specific rules and guidance to address sector-specific risks. CD alone is insufficient due to the complexity and rapid evolution of cryptoasset market.

The FCA's proposal not to apply the Consumer Duty (Principle 12) immediately creates a temporary gap in consumer protection, leaving retail investors potentially vulnerable to complex product designs, unfair terms, and inadequate post-sale support.

3. **Do you agree with our proposed application of the existing SUP rules (except SUP 16) to cryptoasset firms?**

From a consumer protection perspective, extending SUP rules to cryptoasset firms strengthens regulatory oversight and accountability,

which indirectly protects consumers. Applying SUP provisions can help the FCA monitor crypto firms' practices, reducing the likelihood of consumer harm from mismanagement or fraud.

Requirements such as notifying the FCA of significant changes and adhering to reporting obligations can alert FCA to emerging risks, which could otherwise harm consumers. Supervision mechanisms like audits (SUP 3), skilled person reports (SUP 5), and individual requirements (SUP 7) create formal accountability structures, which indirectly safeguard consumers. Also, notifications about breaches, insolvency, fraud, or civil proceedings enable FCA intervention before widespread consumer detriment occurs.

The Panel is aware that SUP rules primarily focus on regulatory compliance and firm governance rather than direct consumer-facing protections. Consumers may not see immediate benefits unless non-compliance triggers enforcement, but supervisory processes may not prevent real-time consumer losses from hacks and fraud.

SUP's limitations and Panel's concerns:

While the proposed application of SUP rules to cryptoasset firms aims to strengthen regulatory oversight, several limitations and concerns have been identified.

SUP2 – Information gathering requires FCA's supervisory expertise in crypto to interpret information effectively, otherwise consumer protection may be compromised. Furthermore, the decentralised nature of cryptoasset systems and technology can restrict FCA's ability to access them reducing the effectiveness of consumer safeguard.

SUP 3 - Existing audit frameworks are designed for traditional finance; they may miss risks unique to crypto, such as smart contract vulnerabilities, custody mismanagement of digital wallets, or algorithmic stablecoin failures.

SUP 5 - Skilled person reports are often commissioned after a concern arises, potentially after consumer harm has occurred.

SUP 15 – Notifications: Cryptoasset firms operate in highly volatile markets; what constitutes "significant" under 15.3.11R, 15.3.17R and 15.3.32R may be subject to firm interpretation, potentially leaving consumers exposed if firms underreport events. If no notification timings are communicated, bad actors may delay or omit notifications, undermining consumer protection.

To enhance consumer protection, the Panel recommends the FCA complement SUP provisions with crypto-specific consumer safeguards, such as mandatory transparency of product risks, digital asset custody standards, automatic notifications and rapid-response enforcement for incidents like hacks or insolvencies.

Chapter 3

4. **Do you agree with our proposal to require cryptoasset firms to follow the existing requirements in SYSC 1, 4 – 7, 9 – 10, and 18 in the same way as existing FCA-regulated firms (or existing DIBs)?**

The Panel broadly supports the proposal that cryptoasset firms should be required to follow the existing SYSC requirements (SYSC 1, 4–7, 9–10 and 18) on the grounds that robust systems and controls materially reduce consumer risk.

SYSC limitations and Panel's concerns:

While the proposed application of SYSC requirements to cryptoasset firms aims to strengthen systems and control oversight, several limitations and concerns have been identified.

SYSC requirements are largely technology-neutral. Crypto brings unique operational risks such as: Private key security issues, validator failures, smart contract vulnerabilities, and service disruptions. The Panel therefore believe it is important that FCA makes it explicit how SYSC maps to those cryptoasset risks.

Many crypto models rely on overseas custodians/validators. Exposed to that risk, firm's SYSC controls must demonstrably cover third-party failures and recovery plans for customers.

Lighter treatment for small firms might reduce consumer protection; any proportionality must not dilute core protections.

We acknowledge the FCA's intention to revisit conflicts of interest (SYSC 10) and training and competence requirements (Training and Competences Sourcebook) in future consultations. These areas are essential to maintaining consumer trust and ensuring that firms' personnel, not only key personnel, have the necessary expertise to act with integrity and competence. We therefore welcome further consultation on these topics and encourage the FCA to ensure that any forthcoming proposals set clear, enforceable expectations on how firms identify, disclose, and manage conflicts, as well as how they assess and maintain the competence of staff engaging in cryptoasset activities.

In response to FCA's Feedback Statement FS25/2[4] regarding minimum training requirements, the Panel is supportive of the FCA's proposal to remove rigid requirements such as minimum training hours, thereby allowing firms greater flexibility to tailor staff development to specific roles and levels of risk exposure. However, including consumer representatives, it will be important to ensure that this flexibility does not lead to a dilution of professional standards. The FCA should confirm that firms remain accountable for maintaining consistently high levels of competence and capability across all staff whose decisions or actions could impact consumers or market integrity. Similar to other jurisdictions, the FCA should consider professional licensing requirements for regulated activities that are particularly likely to expose consumers to harm.

5. **Do you agree with our proposal to apply the existing SM&CR regime to cryptoasset firms, taking into account various parallel consultations on the broader SM&CR regime to ensure consistency? If not, please explain why.**

Taking into account the various parallel consultations on the broader SM&CR regime, the Panel supports the FCA's proposal to apply the existing SM&CR regime to cryptoasset firms. Applying both SYSC and SM&CR to crypto firms in the UK will help ensure that FTX-style failures are far less likely to occur in future.

Crypto scandals such as FTX[5] have demonstrated how the absence of accountability, unmanaged conflicts of interest, poor segregation of client assets, and a lack of whistleblowing and oversight can enable reckless decision-making. Consumers benefit from well-governed organisations, as effective systems and controls significantly reduce the risk of failure or misconduct.

Bringing cryptoasset firms within the same regulatory framework as other FSMA-authorised firms will help ensure robust governance, personal accountability, and stronger consumer protection. Consumers have greater confidence when they know that senior management and to some extend the Board of Directors, is directly responsible for identifying, managing, and mitigating risks rather than concealing or ignoring them. Clear accountability also deters negligent or reckless behaviour — a critical safeguard given the volatility and complexity of crypto products.

The proposed regime protects consumers by ensuring that senior managers and certified staff are both fit and proper, and personally

[4] FS25/2: Immediate areas for action and further plans for reviewing FCA requirements following introduction of the Consumer Duty
[5] Sam Bankman-Fried convicted of fraud over FTX collapse, Financial Times, 2023 https://www.ft.com/content/24d153b0-0c28-4946-acbe-2e93329bca52

accountable for their conduct. Consumers rightly expect consistent standards of protection, whether they invest in traditional financial products or cryptoassets.

However, the Panel remains concerned that compliance costs could be passed on to consumers through higher fees. We therefore urge the FCA to monitor this risk closely to ensure that enhanced consumer protection does not come at the expense of affordability or market competition.

The Panel has consistently argued for the introduction of a Senior Management Function (SMF) with explicit responsibility for Customer and Consumer Outcomes. With the removal of the regulatory requirement for firms to have a Board member responsible for the Consumer Duty — and recognising that many firms have chosen to retain this Board-level role voluntarily — the Panel believes that now would be an appropriate time to formalise such a function within the SM&CR framework for companies offering services in the digital assets space.

Introduction of a Technology Champion Sponsor at Board Level

With the removal of the Consumer Duty Sponsor at Board level, and given the growing risks associated with technology failures, the Panel proposes the introduction of a Technology Champion Sponsor at Board level. This role would provide the necessary expertise to guide and challenge both the Board and the Executive team on technology-related decisions, particularly in the context of digital innovation and cryptoasset developments.

A diverse panel of technology experts, representing both technical knowledge and strategic perspectives, is essential to effectively challenge existing practices and strengthen decision-making. The ability to ask fundamental questions — such as "what could go wrong if we take this decision?" — should form part of the Board's culture and oversight processes. Continuous and structured discussions of technology risks at Board level will help prevent blind spots and ensure timely identification of potential vulnerabilities.

Recent cryptoasset failures and frauds have underlined the critical importance of informed oversight at the highest level. In several cases, Boards lacked the necessary expertise to recognise or address weaknesses in governance, controls, and data integrity. These incidents demonstrate that technological misunderstanding or complacency at senior levels can directly contribute to consumer harm and market instability.

Similarly, the Post Office scandal, though unrelated to cryptoassets, highlights the consequences of insufficient risk and technological

understanding among decision-makers. It reinforces the need for Boards to include members who possess a genuine grasp of how technology functions, where risks originate, and how they may evolve over time.

The Panel also believes it is time to break the culture of recycling the same individuals across Boards, particularly where such appointments perpetuate limited awareness of emerging technologies. Appointing new members with relevant expertise in digital systems, data, and technology strategy will strengthen governance and improve the quality of Board-level challenge.

Finally, a strong technology-aware culture must be driven from the top. The Panel recommends that firms embed technology awareness and continuous learning across all levels of the organisation, not solely within the Boardroom. This top-down reinforcement of technological competence will help build resilience, promote responsible innovation, and reduce the likelihood of repeating past failures — both in traditional systems and within the rapidly evolving cryptoasset sector.

In addition, the FCA should make it mandatory for firms to attest that every Senior Management Function (SMF) has the appropriate knowledge and understanding of any technology, including distributed ledger technology, that forms part of a consumer product or service offering in that SMF's remit. It is also worth noting that, out of 23 FCA defined functions, there is not a single function that is specifically responsible for the technology oversight of the firm. Whilst it is true that the SMF 24, Chief operations function covers this, the SMF 24 is far too broad to ensure that technology, which is at the core of most financial services in this day and age, is covered by an accountable person with the requisite specialist expertise. The FCA must address this gap.

6. **Do you agree with the proposed categorisation for enhanced cryptoasset firms, such as the threshold for allowing cryptoasset custodian firms to qualify as enhanced? Should we consider other ways to categorise cryptoassets firms as enhanced?**

The Panel agrees in principle with the FCA's proposed categorisation for Enhanced cryptoasset firms, including the introduction of thresholds to determine which cryptoasset custodians should qualify as Enhanced. This approach appears proportionate and consistent with the treatment of larger, systemically significant firms in traditional financial services.

From a consumer perspective, it is essential that firms holding substantial volumes of client cryptoassets, or undertaking high-risk activities such as custody or stablecoin issuance, are subject to the strongest governance and accountability requirements. Consumers need confidence that the largest and most systemically important crypto firms are managed to the

highest standards, with clear lines of responsibility and robust oversight of client asset protection.

However, the Panel encourages the FCA to ensure that the thresholds and criteria used to define Enhanced firms are both transparent and adaptable.

The crypto sector evolves rapidly, and firms can grow to systemic scale far more quickly than in traditional finance. The FCA may therefore wish to consider dynamic thresholds or additional qualitative criteria beyond pure asset value — for example:

- The number of consumers or customer accounts affected;
- The degree of vertical integration (e.g., where firms operate both an exchange and custody service);
- The complexity of technological infrastructure or reliance on proprietary algorithms;
- The potential contagion risk to other firms or markets.

These additional factors could help ensure that the Enhanced classification genuinely reflects the risks a firm poses to consumers and the wider market, rather than relying solely on asset-based metrics.

Overall, the Panel supports the FCA's direction of travel and recognises that applying the Enhanced category appropriately will strengthen consumer protection, promote market integrity, and reduce the likelihood of systemic failures similar to FTX.

7. **Do you agree with our proposal to extend the application of SYSC 15A to cover all cryptoasset firms, including FSMA-authorised firms carrying out qualifying cryptoasset activities? If not, please explain why.**

The Panel strongly agrees with the FCA's proposal to extend SYSC 15A to all cryptoasset firms. The Panel believes this proposal is both justified and proportionate from a consumer protection perspective. Consistent with the principle of "same risk, same regulatory outcome," consumers engaging with cryptoassets should receive the same level of protection as those using traditional financial products. Consumers interacting with cryptoasset firms often face even greater operational risks than in traditional finance, particularly in relation to cyber threats and technology failures and service disruptions. Extending SYSC 15A will help ensure consistent minimum resilience standards across the sector, strengthen consumer trust, enhance operational resilience and confidence, and promote stronger governance and market integrity.

SYSC 15A limitations and Panel's concerns:

While the proposed extension of SYSC 15A requirements to cryptoasset firms is intended to strengthen operational resilience, the Panel has identified several limitations and concerns.

First, SYSC 15A is designed to be technology-neutral. However, as the FCA notes in paragraphs 3.73–3.75 of the consultation, cryptoasset activities present distinct technological and operational risks, including the integration of distributed ledger technologies (DLT) into firms' core systems, that differ materially from those in traditional financial services. The Panel therefore believes it is essential that the FCA explicitly sets out in a guidance document how the SYSC 15A framework maps onto these crypto-specific risks to ensure firms apply the requirements effectively and consistently. Without such clarity, firms may interpret their obligations inconsistently, potentially leaving consumers exposed to gaps in protection. The Panel also believes that incorporating illustrative examples would enhance clarity and facilitate consistent application.

Second, many crypto business models depend heavily on overseas custodians, validators, or infrastructure providers. This cross-border reliance introduces additional vulnerabilities. The Panel considers it critical that firms' SYSC 15A controls clearly demonstrate how they manage these third-party dependencies, including robust recovery and contingency plans to protect customers in the event of failure. Again, the Panel believes that incorporating illustrative examples would enhance clarity and facilitate consistent application.

Finally, while the Panel recognises the need for proportionality in applying regulatory requirements, any lighter treatment for smaller firms must not dilute the core consumer protection outcomes that SYSC 15A is designed to achieve. Proportionality should adjust how obligations are met, not whether they are met.

The FCA's own comments within the consultation paper underline the importance of these points. The cryptoasset sector's dependence on technology means that weak operational resilience can greatly amplify operational and technological risks, leading to significant consumer harm. The FCA notes that approximately USD 2.2 billion worth of cryptoassets were stolen through hacks in 2024, including the USD 1.5 billion Bybit incident in February 2025. These examples highlight the urgent need for consistent, robust, and enforceable operational resilience standards across all cryptoasset firms, comparable to and perhaps even more enhanced to those applied in traditional financial services.

8. **Do you agree with our proposal that the use of permissionless DLTs by cryptoasset firms should not be treated as an outsourcing arrangement? If not, please explain why.**

The Panel agrees in principle with the FCA's proposal that the use of permissionless DLTs by cryptoasset firms should not be treated as an outsourcing arrangement. The Panel recognises that, as the FCA notes (paragraphs 3.78–3.79), permissionless DLTs operate without a central authority or direct contractual relationships, making it impractical to apply traditional outsourcing requirements which include detailed due diligence discussions with the provider. However, the Panel emphasises that this exemption should not create an accountability gap. Firms should remain fully responsible for the operational risks associated with the use of permissionless DLTs.

As highlighted in paragraphs 3.73–3.75, cryptoasset firms face unique technological considerations — including integrating DLT into core systems, testing resilience under severe but plausible scenarios, and maintaining robust cyber resilience measures. Firms should demonstrate they have:

- Identified and assessed the operational risks inherent in the DLT they use;
- Implemented appropriate mitigation strategies and contingency plans;
- Maintained sufficient understanding of the people, processes, technology, facilities, and information supporting the DLT infrastructure; and
- Applied relevant international frameworks for cyber resilience to protect consumers from potential cyberattacks or system failures.

The Panel recommends that the forthcoming non-Handbook guidance (paragraphs 3.80–3.81) provide clarity and practical examples on how firms should manage these risks while remaining operationally resilient. This will ensure that consumer protection is not compromised, even where permissionless DLTs are not formally treated as outsourcing arrangements.

9. **Do you agree with our proposal to require cryptoasset firms to follow the same financial crime framework as FSMA-authorised firms? If not, please explain why.**

The Panel broadly supports the proposal that cryptoasset firms should be required to follow the same financial crime framework as FSMA-authorised firms, recognising that robust financial crime controls materially reduce consumer risk.

From a consumer protection perspective, this approach strengthens market integrity, enhances accountability, and fosters consumer trust. For the framework to be fully effective, it should be complemented by broader

consumer redress mechanisms, ensuring protection extends beyond the prevention of financial crime to addressing consumer harm when it occurs.

Limitations and Panel Concerns:

While the proposed application of the existing financial crime framework aims to strengthen controls, it is largely technology-neutral. Given the unique operational and technical risks associated with cryptoassets, the Panel believes the FCA should explicitly clarify how the framework maps to these sector-specific risks (cyberattacks, hacks and fraud). Additionally, while lighter regulatory treatment for smaller firms may support innovation, any proportionality measures must not dilute the core protections afforded to consumers.

Chapter 4

10. **Do you agree with the guidance set out in this document, and can you outline any areas where you think our approach could be clearer or better tailored to the specific risks and business models in the cryptoasset sector?**

The Panel generally supports the guidance outlined in the document. The guidance appears to be comprehensive, well-structured, and rooted in established operational resilience frameworks (SYSC 15A), adapted for cryptoasset-specific risks.

The Panel is pleased to see the FCA's proposal and examples recognising cryptoasset-specific risks, particularly private key security issues, validator failures, smart contract vulnerabilities, and service disruptions that are unique to cryptoassets.

The Panel also welcomes the consumer-centric thinking reflected in some of the examples, which show how operational failures could directly affect consumers. It is also reassuring to see guidance on operational resilience principles that demonstrate how a trading platform might operate and resume during critical incidents, giving consumers confidence that services may remain available, or partially available, even during disruptions. We were also pleased to see the guidance on strengthening requirements for technologies dependent on third-party providers. The practical examples and guidance on how firms should communicate during disruptions are reassuring and reinforce consumer transparency and trust.

The Panel has identified the following areas for improvement:

While the guidance stresses impact tolerances, it does not explicitly require firms to define these in terms of concrete consumer outcomes

(e.g. lost transactions, delayed rewards, financial losses). We encourage the FCA to quantify impact tolerances in terms of tangible consumer outcomes, as this makes resilience more relatable and measurable from a consumer perspective.

Although the guidance emphasises timely communication, it could provide more prescriptive standards (e.g. maximum notification times, frequency of updates, and channels to use) to reduce uncertainty for consumers during disruptions. This is particularly important for high-risk events such as cyberattacks, blockchain forks, or system outages.

Adding a section on educating consumers about operational risks (e.g. the importance of private key security and how forks may affect access) could empower consumers, but the guidance does not specify who should be responsible for this. It could therefore include expectations for firms to educate their customers on operational risks, particularly in areas such as private key management and the potential implications of blockchain forks, as raised in section 4.45 of the consultation paper.

The Panel also continues to believe that mandatory signposting should be introduced to direct consumers to independent, FCA-approved sources of information and support (Citizen's Advice, Action Fraud, HM Treasury / Government / FCA Warning Lists and Guidance), helping them to better understand the risks and protections associated with their investment decisions.

While scenario testing is encouraged, there should be further guidance on how to manage compounded disruptions, such as simultaneous third-party outages and cyberattacks, which are likely to have severe consumer impacts.

Finally, firms should be encouraged to publish assurances or contingency plans, written in jargon-free language, regarding third-party services and dependencies. This would provide consumers with confidence that operational risks are mitigated, even when firms have limited control.

11. **Are there any emerging digital and cyber security industry practices or measures which we should consider when supporting cryptoasset firms complying with operational resilience and related requirements? Please elaborate.**

While the FCA's CP25/25 consultation shared some measures to comply with operational resilience, the FCA should consider including some more advanced and automated cybersecurity approaches.

Zero Trust Security Architecture: The paper requires firms to have proportionate technical and organisational measures but does not refer to

or suggests architecture types. The adoption of Zero Trust frameworks—where no user, device, or service is automatically trusted—has become an industry standard in reducing cyber risk. These frameworks prevent internal and external breaches, significantly reducing risks of unauthorised access to systems managing private keys, wallets, or customer data through continuous verification.

Advanced Key Management and Hardware Security: The guidance discusses private key security and secure architectures (e.g. using cold/hot wallets and multi-party computation (MPC) in examples), but it does not explain in detail how to adopt or validate such advanced techniques, which provide strong alternatives to traditional single-key storage. These technologies ensure that private keys cannot be compromised through a single point of failure, enhance consumer asset protection even if one component is compromised, and reduce the likelihood of total loss, aligning with the operational resilience principles outlined in SYSC 15A.

Privacy-Enhancing Technologies (PETs) and Data Minimisation Under Attack: There is no mention of advanced PETs or techniques to preserve the confidentiality and integrity of user data during attacks or disruptions. The inclusion of such measures could help firms better protect sensitive consumer information in the event of a cyber incident.

Automated AI-Driven Incident Detection and Communication: While the FCA requires firms to maintain clear communication with consumers during disruptions, the current proposals do not specify the use of automation or AI tools for real-time detection, updates, and response. These tools would ensure faster consumer notification, improve transparency, and reduce panic or misinformation during outages.

Continuous Third-Party Risk Scoring / Real-Time Supply Chain Monitoring: Firms could adopt real-time supply-chain monitoring and continuous risk scoring of third-party vendors using automated tools. This would improve early detection of risks within supply chains and provide consumers with assurance that critical dependencies are properly managed.

Scenario Testing and Mapping: The consultation paper mentions that firms must map important business services, dependencies, and conduct scenario tests on “severe but plausible” events. However, testing should also combine multiple simultaneous failures (e.g. a cyberattack combined with a third-party outage). Better preparation for complex, real-world events would minimise consumer impact and service disruption. The Panel also recommends that FCA provides a safe sandbox environment for those simulations to take place.

Red Teaming, Purple Teaming, Adversarial Tests, Supply Chain Attacks: The consultation paper could be strengthened by explicitly referencing adversarial testing methodologies, including simulations of sophisticated attacker behaviour, supply chain attacks, and insider threats. Advanced red teaming and continuous adversarial testing, including blockchain-specific attack simulations and stress testing of validator or wallet systems, can help identify weaknesses proactively before they affect consumers. From a consumer protection perspective, these controls safeguard funds and reduce disruption risk.

Sector-Wide Cyber Intelligence Sharing / Threat-Sharing Networks: The consultation does not explicitly mandate or encourage cryptoasset firms to participate in shared threat intelligence networks, as is common in the traditional financial sector. Establishing formal threat intelligence networks and cross-firm cyber information sharing could improve early warning of threats, reduce systemic risk, and enhance consumer protection across the sector.

Consumer Education and Transparency: While the guidance encourages communication, it does not clearly assign responsibility for consumer education. Standardised consumer education programmes on operational and cyber risks—such as those run by *Get Safe Online (UK)*, the *National Cyber Security Centre (NCSC)*, *CryptoUK*, or *Fintech Scotland*—would empower consumers to make informed decisions and reduce harm caused by misinformation or poor security practices.

To conclude FCA's consultation paper already establishes a solid guidance on operational resilience and cybersecurity approaches. Incorporating especially Zero Trust security, advanced key management, and continuous third-party risk monitoring could better safeguard consumers' assets and confidence in crypto markets.

Chapter 5

12. Do you agree with our proposal to apply the ESG Sourcebook to cryptoasset firms?

Applying the ESG Sourcebook to cryptoasset firms is a necessary first step towards aligning this sector with established consumer protection standards. It also ensures that sustainability-related information is fair, clear, and not misleading. Extending existing ESG rules to cryptoasset firms also promotes consistency across the financial sector preventing a "two-tier" system in which crypto firms could make sustainability claims with less scrutiny than traditional financial institutions.

The Panel understands that the FCA is not currently seeking to introduce cryptoasset-specific disclosure obligations or any additional sustainability

reporting. While this approach avoids over-burdening firms, it also means that consumers will not receive verified sustainability data about cryptoassets particularly in relation to energy use, carbon intensity, or governance practices.

Cryptoassets often rely on blockchain technology, which can be highly energy-intensive. The environmental impact of the energy consumption required for mining and transaction processing on these networks should not be overlooked. Without mandatory requirements, disclosures, or standardised reporting metrics and the rule, consumers will effectively rely on firms' self-assessment of their use of renewable energy sources and optimisation of energy efficiency. In particular, smaller or less-rigorous firms may lack the data, systems, and resources needed to gather relevant information. As a result, they might make vague or unverifiable eco-friendly claims regarding their energy use and efficiency measures.

We recognise that the cryptoasset market is at an early stage and that data reliability is currently limited. It is also possible that consumer awareness of energy consumption in this sector is insufficient to generate strong demand for sustainability information.

To fully realise consumer protection objectives, future stages of regulation could include verified sustainability data and clearer disclosure expectations. This would ensure that consumers are not only protected from harm, but also empowered to make informed and responsible investment decisions. While applying the ESG Sourcebook is a necessary first step, the FCA should consider adopting a phased approach — beginning with the anti-greenwashing rule and, as the market and data availability mature, introducing proportionate, data-based disclosure requirements.