12 November 2025

Financial Conduct Authority
12 Endeavour Square
London E20 1JN
Submitted by e-mail to: cp25-25@fca.org.uk

Dear Crypto Policy Team,

RE: Consultation Paper CP25/25 – Application of the FCA Handbook for Regulated Cryptoasset Activities (Chapter 1-5)

CFA Institute[1] and CFA Society of the United Kingdom (CFA UK)[2] welcome the opportunity to comment on the Financial Conduct Authority's (FCA) Consultation Paper CP25/25: *Application of FCA Handbook for Regulated Cryptoasset Activities*. We commend the FCA's proactive and pragmatic approach to establishing a coherent regulatory framework for cryptoasset activities.

In particular, we recognise the FCA's decisive approach in addressing two foundational issues in cryptoasset regulation – areas that many jurisdictions have yet to resolve. By including all qualifying crypto-related activities within the definition of *designated investment business*, the FCA has minimised legal ambiguity concerning the nature of the asset or activity. Furthermore, by clarifying the requirement for regulatory authorisation and consequent oversight for firms undertaking crypto-related activities, the FCA has reduced uncertainty and potential duplication across the regulatory framework. Together, these proposed measures represent important steps toward establishing clarity, consistency, and accountability within the cryptoasset ecosystem.

---

1 With offices in Charlottesville, VA; New York; Washington, DC; Brussels; Hong Kong SAR; Mumbai; Beijing; Abu Dhabi; and London, CFA Institute is a global, not-for-profit professional association of more than 190,000 members, as well as 160 member societies around the world. Members include investment analysts, advisers, portfolio managers, and other investment professionals. CFA Institute administers the Chartered Financial Analyst® (CFA®) Program. For more information, visit www.cfainstitute.org or follow us on LinkedIn and X.

2 Founded in 1955, CFA UK is one of the largest member societies of CFA Institute, which serves nearly 12,000 members of the UK investment profession. Many of our members analyse securities, manage investment portfolios, advise on investments, or are in roles responsible for investment operations or oversight. Most of our members have earned the Chartered Financial Analyst® (CFA®) designation. All our members are required to attest to adhere to CFA Institute's Code of Ethics and Standards of Professional Conduct. For more information, visit www.cfauk.org or follow us on Twitter @cfauk and on LinkedIn.com/company/cfa-uk/

This response addresses Chapters 1–5 of the consultation and builds on our previous submission on Chapters 6–7. It reflects our shared commitment to promoting market integrity and investor protection, while recognising the need to preserve market dynamism and enable responsible innovation.

Consistent with our broader regulatory engagement, we advocate for a holistic and proportionate approach to policy design – one that situates cryptoasset regulation within the wider financial conduct framework and evolving technological landscape. We support the FCA's intention to phase implementation in line with market maturity, and to ensure coherence with existing conduct, prudential, and disclosure regimes.

Relevant Publications and Comment Letters

CFA Institute and CFA UK have taken a keen interest in the development of digital finance and its policy implications. Our organization has released several pieces of research and comment letters related to this new field affecting capital markets, since 2021. We have consistently advocated for regulatory clarification and international convergence. Below is a list and links to those various pieces which will be mentioned throughout the rest of this response, as appropriate.

- *Cryptoassets: The Guide to Bitcoin, Blockchain, and Cryptocurrency for Investment Professionals*. January 2021.
- *Cryptoassets: Beyond the Hype – An Investment Management Perspective on the Development of Digital Finance*. January 2023.
- [Survey] *CFA Institute Global Survey on Central Bank Digital Currencies*. July 2023.
- *Valuation of Cryptoassets: A Guide for Investment Professionals*. November 2023.
- *An Investment Perspective on Tokenization — Part I: A Primer on the Use of Distributed Ledger Technology (DLT) to Tokenize Real-World and Financial Assets*. January 2025.
- *An Investment Perspective on Tokenization — Part II: Policy and Regulatory Implications*. May 2025.
- [Comment letter] *Response to FCA - DP25.1 — Regulating Cryptoasset Activities*. June 2025.

Summary of Key Positions

Question 1-2: Regulatory Alignment and Designated Investment Business

We agree that qualifying cryptoasset activities defined in the draft SI and FCA Handbook should be treated as designated investment business, providing legal clarity and consistency with the FSMA framework. This alignment allows cryptoasset activities – such as dealing in investment, custody (safeguarding and administrating investment), and arranging deals in investment – to be subject to established conduct standards under the Consumer Duty and COBS. We also support extending high-level FCA standards – including PRIN, SYSC, and SM&CR – to cryptoasset firms in line with the principle of "same risk, same regulatory outcome," while encouraging proportionality, targeted disapplications, and transitional measures to reflect the unique operational structures of crypto markets.

Question 3-5: Application of SUP, SYSC, and SM&CR

We agree with extending existing SUP rules (except SUP 16) to cryptoasset firms, as this ensures consistent regulatory outcomes across the financial sector while embedding SM&CR and related governance standards. We also support applying SYSC 1, 4–7, 9–10, and 18 to cryptoasset firms, though expectations should be adapted to recognise algorithmic systems, on-chain record-keeping, and vertically integrated business models. In addition, we endorse the application of the existing SM&CR regime to cryptoasset firms to maintain consistent accountability standards across FSMA-authorised entities, while urging the FCA to clarify role mapping, certification scope for technical functions, and cross-border responsibilities to ensure effective and proportionate implementation.

Question 6-7: Enhanced Firm Thresholds and Incident Reporting

We partially agree with the proposed categorisation for enhanced cryptoasset firms. We recommend setting the Assets under Custody (AuC) threshold closer to £5–10 billion to maintain a small, risk-focused enhanced population, while publishing expected capture rates for transparency. As AuC alone may not reliably indicate risk, we encourage a multi-factor approach, drawing on comparable frameworks in other jurisdictions. We also support extending SYSC 15A to cryptoasset firms to ensure prompt incident reporting and supervisory engagement, provided the FCA calibrates materiality thresholds for 24/7 markets, prevents duplicate notifications, safeguards confidential data, and promotes post-incident learning.

Question 8-10: DLT and Financial Crime

We agree that the use of permissionless DLTs should not be treated as outsourcing. Nonetheless, firms should still demonstrate how they monitor validator concentration, governance risks, and fork management within their operational resilience frameworks. We also support applying the same financial crime framework to cryptoasset firms as to other FSMA-authorised firms, reinforcing accountability and international consistency under SYSC 6 and the Financial Crime Guide. Finally, we broadly endorse the FCA's guidance in CP25/25, encouraging clearer expectations on cyber and operational resilience specific to crypto, and continued alignment with major jurisdictions such as the EU, Singapore, and Hong Kong to balance innovation, consumer protection, and global competitiveness.

Question 11: Cybersecurity and Operational Resilience

We recognise operational resilience and cyber security as critical to sustaining confidence in crypto markets, and highlight quantum computing as an emerging systemic risk to cryptographic systems. The ability of future quantum machines to break existing encryption—potentially by the early 2030s—poses a "harvest now, decrypt later" threat to distributed ledgers, given their permanent and transparent transaction histories. We encourage the FCA to monitor global initiatives such as NIST's post-quantum standards, the NSA's migration mandates, and the BIS's Project Leap, and to explore how post-quantum resilience can be incorporated into operational-resilience guidance under PS21/3.

Question 12: ESG Sourcebook and Anti-Greenwashing

We also support proportionate application of the ESG Sourcebook to cryptoasset firms, centred on anti-greenwashing requirements for sustainability-related claims. While most crypto businesses fall outside the scope of product-labelling regimes, consistent enforcement of ESG 4.3.1R will help curb misleading environmental claims and align the sector with broader FSMA standards.

Concluding Remarks

We appreciate the FCA's continued leadership in developing a robust and comprehensive regulatory framework for the evolving cryptoasset landscape. Consultation Paper CP25/25 marks a significant step towards achieving regulatory clarity and safeguarding market integrity.

We believe that a balanced and holistic approach – one that leverages international cooperation and convergence, embraces technological innovation, and establishes stringent yet proportionate safeguards – will be of crucial importance. For instance, we think it will be important to consider the recent development of 'The Transatlantic Taskforce for Markets of the Future', which has an important remit to smoothen capital markets access and crypto cooperation. This approach will ensure the UK remains at the forefront of financial innovation, while building a secure and trustworthy cryptoasset sector for all market participants.

Given the rising cryptoasset ownership among UK retail investors and the inherent risks associated with these assets, our comments across the relevant sections of this Paper are grounded in our commitment to advancing investor protection and market integrity. We emphasise that the two are inseparable: effective conduct regulation in crypto markets is not merely a consumer issue but a systemic one. Weak governance, poor disclosure, or inadequate redress mechanism can erode confidence across the wider financial system. We therefore encourage the FCA to continue coordinating closely with the Bank of England and HM Treasury to ensure coherence between prudential, conduct, and market-surveillance frameworks.

On the topic of decentralised finance and virtual assets, we have recently published two comprehensive reports focused on the development of tokenisation processes: "An Investment Perspective on Tokenization — Part I: A Primer on the Use of Distributed Ledger Technology (DLT) to Tokenize Real-World and Financial Assets" and "An Investment Perspective on Tokenization—Part II: Policy and Regulatory Implications." We invite you to refer to these for detailed analysis and recommendations.

We also encourage open communication and collaboration between regulators and market participants to ensure a seamless implementation of the proposed measures, together with any necessary adjustments arising from this Paper.

****

Thank you for your consideration of our views and perspectives. We would welcome the opportunity to meet with you to provide more details. If you have any questions or seek further elaboration of our views, please contact Mr. Olivier Fines, Head of Advocacy and Policy Research at CFA Institute, at olivier.fines@cfainstitute.org and Mr. Amit Bisaria, Professionalism and Ethics Adviser at CFA UK, at abisaria@cfauk.org.

Sincerely,

CFA Institute

Olivier Fines, CFA

Head of Advocacy and Policy Research

Phoebe Chan

Research Specialist, Capital Markets Policy,
EMEA Advocacy

CFA Society of the United Kingdom

Amit Bisaria

Amit Bisaria, CFA

Professionalism and Ethics Adviser

With thanks for their contributions to our volunteers: Suzanne Hsu, CFA, CIPM and Altaf Kassam, CFA, and Natalie Schoon, CFA.

Detailed Response

Set out below our comments for consideration.

Question 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?

We agree that the new qualifying cryptoasset activities defined in the forthcoming Statutory Instrument (SI) and draft FCA Handbook (the Handbook) rules, should fall under the category of "designated investment business" (DIB) – for the purposes of applying relevant sections of the Handbook.

The logic of creating a single legal perimeter under the Financial Services and Markets Act is sound. It promotes the legal clarity and regulatory coherence needed to achieve comparable conduct and prudential standards across financial markets.

This classification also makes practical sense. The activities described in the draft SI – such as dealing in investment, custody (safeguarding and administrating investment), and arranging deals in investment – perform functions that are already regulated when carried out in traditional finance. Aligning these activities with the DIB category allows the application of relevant principles of the FCA Handbook, especially through the Consumer Duty and COBS (Conduct of Business Source Book), which we have supported as the overarching conduct frameworks for cryptoasset activities in our earlier responses to Chapters 6 and 7.

Having said that, we encourage the FCA to apply this designation proportionately, to reflect the technological and operational nuances of cryptoasset markets, with consideration for:

- Over-capture of purely technological or decentralised activities.
- Conceptual mismatch between traditional DIB concepts and decentralised markets.
- Transitional and operational burden.
- International convergence and competitive advantages.

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

We agree with the FCA's principle of ensuring "same risk, same regulatory outcome" by extending high-level FCA standards – including the Principles for Businesses (PRIN), the Senior Managers and Certification Regime (SM&CR), and the Systems and Controls (SYSC) requirements – which should apply to cryptoasset firms in a way consistent with their application to traditional finance.

Cryptoasset firms, including facilitators, custodians, and distributors, perform functions that directly affect investor outcomes and therefore their trust in the market. Extending the high-level standards to them will promote a level playing field across sectors, and embed the Consumer Duty within a coherent governance framework.

Alongside the expansion, the framework should remain agile and proportionate, with the ability to carve out or disapply provisions. We broadly support the FCA's proposed disapplication of certain Principles for transactions entered into on a cryptoasset trading platform (CATP) by its members, and for firms operating CATPs for professional clients. Aligning this with the approach taken for multilateral trading facilities in traditional finance is reasonable, given the institutional nature of member-to-member trading and the absence of retail advice relationships.

The move directly from MLR registration to full FSMA authorisation can, in practice, represent a substantial uplift in governance expectations. Crypto firms often have smaller, flatter organisational structures and different operational realities, and hence may not immediately have the infrastructure to meet all SYSC or SM&CR obligations in full. We therefore encourage the FCA to consider transitional arrangements, including:

- Early publication of templates for governance mapping in cross-border and decentralised structures.
- Temporary-permissions or phased SM&CR rollout for smaller firms; and
- Clarifications of how the FCA will assess "readiness" for each stage.

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

We agree. Extending these requirements will ensure that authorised crypto firms are subject to the same standards of regulatory cooperation and notification that apply across the wider financial sector. This approach also helps embed the SM&CR and other high-level standards.

Many of the principles raised in our previous responses – notably the need for proportionate implementation, clarity for decentralised and cross-border models, and international coherence – apply equally here.

Question 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)?

We agree, as these provisions form the operational backbone of governance and control for authorised firms. Set out below our recommendations, in view of the potential frictions to SYSC execution:

- **Risk control for automated systems (SYSC 7):** Crypto firms often depend on code-based systems – including smart contracts, matching engines, and price oracles. Existing expectations built for manual processes might not translate. We suggest the FCA cross-reference the Bank of England AI discussion (DP5/22) and, for banks, PRA SS1/23 on model-risk management, clarifying expectations for model inventory, validation, explainability, change control, and challenge apply to algorithmic risk controls in crypto.

- **Record-keeping with on-chain data (SYSC 9):** Transaction data on public ledgers is immutable, but not necessarily retrievable or comprehensible in the format supervisors require. We recommend the FCA clarify, via Handbook guidance, that "readily accessible" records may include on-chain data if firms maintain off-chain mapping from addresses or keys to clients and products.

- **Conflicts of interest in vertically integrated models (SYSC 10):** Given many crypto firms combine exchange, brokerage, and custody functions within a single group, we support structural separation for custody and clearer guardrails for principal trading. We also welcome the direction of travel on a strengthened custody framework to underpin this, and recommend that FCA guidance for crypto custody mirror CASS fundamentals (CASS 6 Custody rules; CASS 7 Client money rules) and align with the FCA's CP25/14 proposals for stablecoin issuance and cryptoasset custody. For instance, create a crypto-equivalent to CASS acknowledgment letters in which third-party wallet providers confirm no right of set-off or lien over client cryptoassets.

Question 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.

We support applying the existing SM&CR regime to cryptoasset firms, given the approach remains consistent with broader SM&CR reforms. Applying a common accountability framework across FSMA-authorised firms will promote regulatory comparability and reinforce the expectation that senior leaders in crypto must meet the same standards of competence and integrity as those in traditional finance.

In implementing SM&CR for cryptoasset firms, we highlight the areas requiring clarification:

- **Role mapping and scale:** Crypto firms often have flat structures with overlapping responsibilities. The FCA should provide illustrative Senior Management Functions role maps for common business types (exchange, custodian, staking provider), and clarify where dual-hatting remains acceptable in smaller firms, to maintain clear accountability without forcing artificial hierarchies.

- **Certification scope:** The Certification Regime, as currently defined, focuses on traditional client-dealing and risk-taking functions. In crypto businesses, however, technical personnel – such as wallet-security engineers, smart-contract deployers, or key-management specialists – can have an equivalent or greater impact on customer outcomes. The FCA should clarify how the Certification Regime will capture such roles, or whether supplementary crypto-specific certification functions may be required to close this gap.

- **Alignment with the MLR regime and cross-border oversight:** Many firms have already designated a Money Laundering Reporting Officer (MLRO) under the MLRs.

The FCA should confirm when this individual can also hold SMF17 (Money Laundering Function) and how one set of reporting can satisfy both regimes. In addition, given that funds invested in cryptoassets can move across jurisdictions more easily than in other FCA-regulated activities, the FCA should clarify expectations on cross-border governance. For example, how senior managers remain accountable for AML controls applied to overseas affiliates or technological infrastructure. Clear guidance would help ensure that SM&CR accountability is not weakened where assets or counterparties operate beyond UK jurisdiction.

Question 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?

We partially agree with the proposed categorization. The FCA's intent to mirror the existing SM&CR tiering – targeting a small population of larger or systemically significant cryptoasset firms – is sound. This approach is consistent with the FCA's consumer-protection objectives and CFA Institute's long-standing support on proportionality.

Given the goal of capturing a comparable proportion of Enhanced firms to that in the broader market, we recommend setting the Asset under Custody (AuC) threshold toward the lower end of the proposed £1bn–£100bn range – specifically £5bn–£10bn AuC. We also encourage the FCA to publish the projected and actual number of firms captured at this level using the new custody reporting return. This would keep the Enhanced population small and risk-focused, consistent with the FCA's ~1% intent.

However, AuC alone may not be a reliable proxy for risk. The main drivers of harm are operational (eg, key management, wallet security, reconciliation, and third-party dependencies) rather than market-value-driven. Moreover, AuC figures can fluctuate sharply due to price volatility, causing firms to cross thresholds without material changes in their risk profile. To improve stability, the FCA could apply a rolling average AuC and a buffer before designation.

We support using AuC as a practical starting point, and recommend that the FCA:

1. Monitor impact across business models. Conduct a thematic review to assess whether AuC remains a suitable proxy as more data become available; and
2. Draw, where relevant, on lessons from comparable regimes. For example, EU, Singapore, and Hong Kong do not rely on a single notional asset value test to decide who is "significant". They use multi-factor triggers that better map to potential harm:
    - EU (MiCA; Chapter 5 Article 43) – "Significant" tokens are designated using multiple criteria including number of holders, daily transactions and value, international significance, and interconnectedness with the financial system.
    - Singapore (Major Payment Institution Licence under Payment Services Act) – The Standard vs Major Payment Institution split is based on scale and activity metrics, i.e., monthly transaction values and average daily e-money float.

Question 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.

We support the FCA's proposal to extend SYSC 15A (incident-reporting requirements) to cryptoasset firms. Crypto markets are fast-moving and technology-dependent; when key infrastructure fails, rapid communication with supervisors is essential.

That said, we believe the current rulebook language needs calibration to crypto-specific contexts:

- **Clarify materiality thresholds:** Because token markets operate 24/7, even brief interruptions can appear "significant." We urge clarity in defining 'materiality' in outcome terms.

- **Avoid duplicate notifications:** Many firms will also be subject to Operational Resilience (SYSC 15B), cyber-incident reporting under NIS2, and potentially FOS/FCA consumer-redress notifications. The FCA should confirm that a single integrated notification satisfies new, overlapping obligations.

- **Provide confidentiality safeguards:** Crypto incidents often involve public addresses and forensic data that could be exploited if disclosed. FCA guidance should outline secure-submission methods and clarify when summaries can replace granular information.

- **Encourage post-incident learning:** In line with the Consumer Duty's consumer-support outcome, firms should be expected to perform and retain post-incident reviews, rather than simply filing a report. This will embed a preventive-over-reactive culture and ensure consistent treatment of disruptions across sectors. The FCA could also use these reviews to build sector-wide lessons learned.

Question 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.

We agree, since permissionless DLTs are open, decentralised systems maintained by unaffiliated participants, which have not presumed a bilateral contractual relationship and defined service provider. A firm hence cannot perform due diligence or negotiate audit rights with a wide network of anonymous validators, which makes the application of the outsourcing rulebook conceptually and operationally inapplicable. Global regulators, including the BIS, FSB, and IOSCO, have also recognised that while permissionless networks pose systemic operational dependencies, these do not fit within traditional outsourcing frameworks or bilateral service relationships.

At the same time, we caution that treating permissionless DLTs wholly outside the outsourcing perimeter could lead to regulatory blind spots and weaken accountability, if firms interpret it as a blanket exemption. For such operational dependencies, we recommend that the FCA to

require firms to evidence, in their operational-resilience mapping, how they monitor validator concentration and fork-handling runbooks for the networks they rely on.

We also support that permissioned or consortium-based blockchains should continue to be assessed under SYSC 8. Contractual accountability and oversight are feasible in those arrangements.

Question 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.

We agree. Applying the same financial-crime framework to cryptoasset firms as to other FSMA-authorised firms is consistent with the FCA's proposal to bring crypto within SYSC 6 and the Financial Crime Guide (FCG), alongside existing legal duties. This includes senior-management responsibility to strengthen accountability at the top.

Our earlier comments on risk-based, proportionate implementation and additional sector guidance are pertinent here.

Last but not least, given the cryptoasset's cross-border flow of funds, international convergence and supervisory cooperation become critical. We encourage the FCA to coordinate with HM Treasury and international counterparts for data-sharing and reciprocal recognition arrangements to prevent regulatory fragmentation and competitive disadvantages for UK-authorised firms. Meanwhile, convergence should not mean lowest common denominator; rather, the UK should help raise global expectations by demonstrating how a proportionate, principles-based framework can work in practice.

Question 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?

We broadly support the guidance set out in CP25/25. Meanwhile, cryptoasset activities are inherently more exposed to operational disruption, cyberattack, and irretrievable loss than other FCA-regulated sectors. These risks arise from the sector's reliance on decentralised, cryptographic systems that can be compromised through malicious code, software errors, or technological advances such as quantum computing. We encourage the FCA to consider requiring companies to be more specific about their defenses / recovery plans) for cryptoassets.

At the same time, given the global nature of crypto markets, the UK's regulatory framework should promote coherence with other major jurisdictions and minimise frictions for cross-border activity. Within Europe, the EU's MiCA provides the principal benchmark, while in Asia-Pacific, Singapore's Payment Services Act and Hong Kong's regulation of Virtual Asset Trading Platforms represent comparable models for decentralised systems – each embedding -based, risk-based accountability standards.

Ensuring alignment with leading international frameworks will be essential to achieving competitive neutrality, while maintaining high standards of consumer protection.

Question 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.

We recognise the importance of operational resilience and cyber security as foundational to maintaining integrity and confidence in cryptoasset markets.

One emerging issue is the potential impact of quantum computing on cryptographic systems. While the precise timeline remains uncertain, the eventual arrival of so-called "Q-Day" – when quantum computers can break existing encryption – could pose systemic risks to digital assets and distributed ledgers. Several studies suggested that as few as 2,330 logical qubits would be enough to crack Bitcoin's encryption, with most major quantum firms expect to reach two to three thousand logical qubits by 2029-2030.

The U.S. National Institute of Standards and Technology (NIST) has already selected quantum-resistant algorithms for adoption across government systems[3]. The U.S. National Security Agency also mandates their adoption across national security systems by 2033. Firms should monitor global developments in post-quantum cryptography and consider long-term resilience planning as part of their operational-resilience frameworks.

The Federal Reserve's 2025 study "Harvest Now, Decrypt Later (HNDL)" warns that adversaries can capture encrypted data today and decrypt it once quantum computing matures – meaning the risk precedes "Q-Day." Distributed ledgers like Bitcoin are particularly vulnerable because their entire transaction histories are public and permanent. Because past transactions cannot be re-encrypted, no current method can retroactively protect data already stored on public ledgers.

The Bank for International Settlements' Project Leap (Phase 2, started in July 2025) also offers lessons on implementation of post-quantum cryptography in a European payment system by sending liquidity transfers between Project Leap's central bank partners using post-quantum digital signatures.

We encourage the FCA to monitor these global initiatives and consider how post-quantum resilience can be embedded into its operational-resilience expectations under PS21/3 – an area for future guidance and supervisory dialogue as market structures and standards evolve.

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

We support a proportionate application of the ESG Sourcebook, focusing on anti-greenwashing compliance for all sustainability-related communications. Cryptoasset firms are unlikely to issue investment products that would fall within the sustainability-labelling regimes. However, the anti-greenwashing rule (ESG 4.3.1R) applies to all authorised firms and is pertinent in this market, where environmental claims such as "carbon-neutral," "green," or "energy-efficient" are common.

[3] The quantum-resistant algorithms include ML-KEM (Kyber) for key exchanges, ML-DSA (Dilithium), and SPHINCS+ for digital signatures.

This targeted approach ensures consistency with the wider FSMA framework while recognising that the ESG Sourcebook's labelling and disclosure provisions have limited direct applicability to most cryptoasset activities.

*PS: Erratum. Note regarding Question 25

We would like to clarify our response to Question 25. In our previous letter, we agreed that cancellation rights should not apply to cryptoasset products or services where the price or value is exposed to market fluctuations. For the avoidance of doubt, we also wish to confirm our support for *not* introducing cancellation rights for distance contracts relating to services whose price is *not* driven by market fluctuation, such as staking and safeguarding.

Our position remains consistent with the proposal not to apply COBS 15 to cryptoasset activities, and with the FCA's rationale that introducing cancellation rights in these contexts would impose disproportionate operational complexity without improving outcomes. Instead, we support reliance on the Consumer Duty's consumer-understanding and consumer-support outcomes, together with clear, prominent disclosures in a durable medium explaining that statutory cancellation rights do not apply and outlining practical exit or unstaking terms.