

Electronic Money Association
Crescent House
5 The Crescent
Surbiton, Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

Financial Conduct Authority

09 March 2025

Dear Sir/Madam,

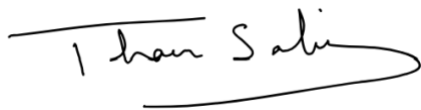
Re: EMA response to FCA Discussion Paper on Admissions & Disclosures and Market Abuse Regime for Cryptoassets

The EMA is the trade body representing virtual asset service providers. Our members include leading payment institutions, e-commerce businesses, and cryptoasset firms worldwide. Most members operate across the EU and UK, frequently on a cross-border basis.

We welcome the opportunity to contribute to the FCA Discussion Paper on Admissions & Disclosures and Market Abuse Regime for Cryptoassets.

We would be grateful for your consideration of our comments and proposals.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Thaer Sabri", with a long horizontal flourish extending to the right.

Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA RESPONSE

Chapter 1: Overview

Question 1: Do you agree with the outcomes we are seeking for the overall regime? Are there any important outcomes we may not have included, or any that you believe are not appropriate?

We broadly agree with the FCA's focus on market integrity, consumer protection, and responsible innovation. It would help to emphasize the global nature of crypto and the importance of international harmonization of rules, as well as fostering the UK's competitiveness as a leading market for cryptoasset activity.

Question 2: Do you agree with our assessment of the type of costs (both direct and indirect) which may materialise as a result of our proposed regulatory framework for A&D and MARC? Are there other types of costs we should consider?

We agree that firms will face direct and indirect compliance costs (legal fees, systems enhancements, staff training). The FCA should also consider the cost of legal uncertainty during any transitional phase and the disproportionate impact on smaller firms with fewer resources. A phased or proportional approach could mitigate potential market concentration or stifled innovation.

Question 3: How do you anticipate our proposed approach to regulating market abuse and admissions and disclosures (see Chapters 2 and 3 for details) will impact competition in the UK cryptoasset market? What competitive implications do you foresee as a result of our regulatory proposals?

Clear, well-structured rules could boost institutional confidence and increase competitiveness by attracting reputable market participants. However, if compliance obligations become too onerous, smaller firms may struggle to meet them, leading to consolidation among larger, established players. To avoid stifling innovation, the FCA should calibrate requirements to the size and risk profile of each business.

Question 4: Do you agree with our view that while the Consumer Duty sets a clear baseline for expectations on firms, it is necessary to introduce specific A&D requirements (see Chapter 2 for details) to help support consumers?

While we acknowledge that the Consumer Duty provides a valuable baseline for consumer protection, we question whether imposing a universal A&D regime on *all* cryptoassets is warranted. Such a broad requirement could create excessive compliance burdens and stifle innovation, particularly for assets—like Bitcoin or Ether—that do not have a formal issuer or centralized governance structure. For truly decentralized tokens without an identifiable party that can be held accountable for disclosures, mandating issuer-style obligations appears impractical and could hinder organic market growth. Instead, the regime might be better suited for cryptoassets where a clear issuer (or corporate entity) exists, so that meaningful disclosure obligations can be enforced. This targeted approach would preserve consumer protections for assets with identifiable sponsors while maintaining the openness and innovative potential that characterize decentralized networks.

Chapter 2: Admissions and Disclosures

Question 5: Do you agree with the risks, potential harms and target outcomes we have identified for the A&D regime? Are there any additional risks or outcomes you believe we should consider?

We agree with the identified risks (e.g., fraud, misleading disclosures) and outcomes (transparency, consumer protection). We also want to highlight that overly detailed or technical disclosures that may confuse retail participants and deter legitimate projects. Striking a balance between comprehensiveness and clarity is crucial.

In addition, another potential risk is creating compliance gaps for truly decentralized cryptoassets that lack a singular accountable entity. If an A&D regime relies on having an identifiable issuer or sponsor, decentralized projects may struggle to fulfil obligations, resulting in partial compliance or ambiguity about who is responsible. This, in turn, could both undermine the regime's effectiveness (by leaving certain high-profile or systemically important assets outside the rules) and stifle innovation if projects feel compelled to centralize to meet compliance requirements.

Question 6: Should an admission document always be required at the point of initial admission? If not, what would be the scenarios where it should not be required? Please provide your rationale.

Generally, an admission document is valuable for ensuring robust initial disclosures. However, certain exempt scenarios could include small-scale offerings limited to sophisticated or institutional investors, where the overall risk of consumer harm is minimal. This maintains flexibility while preserving investor protection for the broader market. Other exempt scenarios are outlined in our response to Question 4.

Question 7: Should an admission document be required at the point of further issuance of cryptoassets that are fungible with those already admitted to trading on the same CATP? If not, what would be the scenario where it should not be required? Please provide your rationale.

A full new document may be unnecessary for identical, already-admitted tokens if prior disclosures remain accurate. A shorter supplemental update could suffice unless there have been material changes (e.g., governance shifts, protocol upgrades). This reduces duplicative costs without compromising transparency for investors.

Question 8: Do you agree with our proposed approach to disclosures, particularly the balance between our rules and the flexibility given to CATPs in establishing more detailed requirements?

Yes. A core set of mandatory disclosures ensures minimum standards, while allowing CATPs flexibility to add further requirements tailored to their business models or risk tolerance. This approach encourages consistent investor protections while accommodating innovation and diversity in the crypto sector.

Question 9: Are there further disclosures that should be required under our rules, or barriers to providing the disclosures we have proposed to require? Please explain your reasons.

One significant barrier stems from the high technical complexity of many cryptoassets, where underlying protocols and tokenomics may be difficult to articulate in plain language. Compiling, verifying, and regularly updating this information can be both time-consuming and expensive, especially when frequent software upgrades or forks change project fundamentals in real time.

Another challenge arises from fragmented or decentralised structures, where responsibility for disclosures is unclear and coordination among multiple stakeholders (including open-source developers, DAO participants, or globally distributed teams) is cumbersome. In addition, decentralized projects may not have a single accountable entity to aggregate and authenticate data, which increases both the cost and the risk of omissions or inaccuracies.

These issues are further amplified if there is no standardized format or guidance on how to condense highly technical, often evolving information into concise, investor-friendly disclosures.

Question 10: Are there any disclosures in the proposed list that you believe should not be required? If so, please explain your reasons.

Overly granular technical details that are immaterial to investment decisions can clutter disclosures and overwhelm investors. We recommend focusing on material risks and governance features, ensuring clarity without diluting key information.

Question 11: Do you think that CATPs should be required to ensure admission documents used for their CATPs are consistent with those already filed on the National Storage Mechanism for the relevant cryptoasset? If not, please explain why and suggest any alternative approaches that could help maintain admission documents' accuracy and consistency across CATPs.

A viable approach would be to allow CATPs (VASPs) to rely on the existing admission documents filed on the NSM as a single source of truth, rather than producing separate or redundant disclosures. Under this model, the CATP could simply confirm that it has reviewed the NSM filing, verified that it remains accurate and up to date, and made it easily accessible to its users (for instance, via a direct link or reference). This would streamline the compliance process by avoiding duplicative documentation while still ensuring that investors and market participants receive consistent, high-quality information. If any material discrepancies arise, the CATP would be responsible for highlighting or supplementing the NSM filing, but in the absence of such discrepancies, reliance on the central document would suffice.

Question 12: What do you estimate will be the costs and types of costs involved in producing admission documents under the proposed A&D regime? Are any of these costs already incurred as part of compliance with existing regulatory regimes in other jurisdictions?

Costs will include legal, compliance, and operational expenses, potentially covering external counsel, internal documentation processes, and IT infrastructure. Firms subject to other regimes like MiCA may already have similar systems in place, partially offsetting new costs. Smaller issuers without compliance frameworks will face higher relative burdens.

Question 13: Do you agree with our suggestions for the types of information that should be protected forward-looking statements?

An alternative approach could be to adopt a tiered regime for forward-looking statements that accounts for the size, complexity, and stage of each project. Rather than applying the same level of scrutiny to all issuers, smaller or early-stage crypto firms could receive a more flexible framework that recognizes their limited resources and the inherent uncertainties of fast-evolving technology.

At the same time, larger or more established projects could be held to higher standards, requiring more rigorous substantiation of forecasts and clearer disclosure of underlying assumptions. This scalable method would ensure that forward-looking statements remain useful and informative for investors without overburdening start-ups or stifling genuine innovation.

Such an approach would still protect consumers by mandating appropriate disclaimers, while also acknowledging that not all projects can feasibly meet an extensive, one-size-fits-all requirement for forecasting and disclosures.

Question 14: Do you agree with the proposed approach to our rules on due diligence and disclosure of due diligence conducted? If not, please explain what changes you would suggest and why.

Yes. A summary of the due diligence performed can help investors gauge the integrity and rigor behind a listing decision. However, fully decentralized projects may require alternative structures (e.g., the CATP or a third-party assessor) to conduct or disclose due diligence on behalf of the network participants.

Question 15: Are there further areas where due diligence or disclosure of findings should be required, or where there would be barriers to implementing our proposed requirements?

Projects should clearly disclose tokenomics (e.g., supply schedules, vesting for team tokens) and any concentrated holdings that might influence price or governance. Barriers arise where no single entity has full visibility into these details, so flexible mechanisms for decentralized disclosures are needed.

Question 16: Where third-party assessments of the cryptoasset's code have not already been conducted, should CATPs be required to conduct or commission a code audit or similar assessment as part of their due diligence process?

Requiring CATPs to commission code audits for every asset with no existing third-party assessment could be both cost-prohibitive and logistically impractical, especially for smaller platforms. Many CATPs lack the internal expertise to conduct advanced technical reviews and would need to hire expensive external auditors for every new token—driving up listing fees and ultimately restricting

market diversity. Moreover, such a requirement could unintentionally favour larger, well-funded projects at the expense of innovative, smaller initiatives that may not have the resources to commission regular audits.

Question 17: Do you agree there is a need to impose requirements regarding rejection of admission to trading? If so, should the rules be more prescriptive rather than outcomes-based?

Yes, clear and transparent rejection criteria are important to protect investors from fraud or major undisclosed risks. An outcomes-based approach is acceptable if supported by a few prescriptive minimum standards (e.g., known security vulnerabilities, fraudulent disclosures) to ensure consistent baseline protections across CATPs.

Question 18: Do you agree that we should require CATPs to publicly disclose their standards for admitting and rejecting a cryptoasset to trading? If so, what details should be disclosed?

Publishing high-level admission/rejection standards—covering core due diligence checks, governance expectations, and common reasons for rejection—enhances transparency, helping issuers understand how to comply and giving investors’ confidence that the CATP enforces robust rules. However, this should not be overly prescriptive.

Question 19: Do you agree with the suggested approach to our rules on filing admission documents on the NSM?

Yes. Centralizing admission documents on the NSM provides a single authoritative record, easing access for both market participants and regulators. This improves consistency and reduces duplication of effort in verifying disclosures.

Chapter 3: Market Abuse

Question 21: Do you agree with the risks, potential harms, and target outcomes we have identified for the market abuse regime? Are there any additional risks or outcomes you believe we should consider?

We agree with the primary risks (insider trading, manipulation, information asymmetry) and outcomes (fair and transparent markets). Given the global and continuous nature of crypto trading, strong international coordination on enforcement and standards is crucial to avoiding regulatory arbitrage or gaps in market abuse coverage.

Question 22: Are there any market behaviours that you would regard as ‘abusive’ at present, or any new abusive behaviours that may emerge, that may not be covered by the above prohibitions? Please provide examples where possible.

Front-running in decentralized protocols can sometimes function similarly to insider dealing. Pump-and-dump schemes facilitated by social media are also a major concern. These activities, where being utilised for illicit activities, should be explicitly recognized as manipulative under any new regime.

Question 23: Do you agree with our proposals to make the issuer responsible for disclosure of inside information unless there is no issuer or the issuer is not involved in seeking admission to trading?

We agree in principle that an engaged issuer should bear primary responsibility for disclosure. However, for truly decentralized assets with no central sponsor—like Bitcoin or Ethereum—imposing issuer-style obligations on a CATP is impractical and could create excessive burdens. In these instances, most critical information is already public via open-source repositories and community governance channels. Instead of treating the CATP as a stand-in “issuer,” we propose a lighter-touch approach that recognizes the decentralized nature of the asset and focuses on verifying that material network changes and developments are publicly accessible rather than formally disclosed by a single entity.

Question 24: In the circumstances where there is no issuer, or the issuer is not involved with the application for the admission to trading, do you agree with our proposal that the person seeking admission to trading of the cryptoasset should be responsible for the disclosure of inside information?

We suggest a more flexible model. For assets that do have a clear sponsor but are not seeking admission themselves, it is reasonable to place disclosure duties on the applicant. However, for established, decentralized networks (such as Bitcoin) with no central sponsor and where material information is typically a matter of public record, requiring the applicant to function as a de facto “issuer” could be unduly burdensome. A balanced approach would let the applicant demonstrate that pertinent information is openly available in recognized channels (e.g., developer forums, network proposals) rather than forcing them to produce traditional “issuer” disclosures that simply may not exist.

Question 25: With regards to the second circumstance in question 24, do you agree that the person (say, ‘Person A’) seeking admission to trading of the cryptoasset should only be responsible for disclosure of inside information which relates to Person A and which Person A is aware of?

Yes. It would be disproportionate to hold Person A accountable for inside information that does not exist in a conventional sense or is distributed across a decentralized community. Person A should only be responsible for material facts that are under their direct control or awareness—such as any promotional activities they undertake, liquidity provisions they arrange, or arrangements made to support the asset’s trading infrastructure. This ensures accountability where appropriate, while acknowledging that no single individual can speak on behalf of an entire decentralized protocol or oversee every detail of public, community-driven development.

Question 27: What are some examples of information that should be considered inside information? Do you think we should provide a non-exhaustive list of examples in guidance?

Although providing a non-exhaustive list of examples can help clarify what constitutes inside information, it is crucial to acknowledge that CATPs, especially those listing decentralized assets, may not have a centralized source to consult or a clear party responsible for providing such

information. For instance, bug discoveries, major code upgrades, or large institutional purchases could all be deemed “inside information,” yet decentralized networks often discuss these matters publicly or semi-publicly in open forums, making it impractical for a CATP to track and assess every development in real time. Requiring CATPs to shoulder full responsibility for identifying, compiling, and disclosing these details could prove disproportionately burdensome. A more balanced approach might involve defining core categories of inside information and encouraging CATPs to perform reasonable checks, while also recognizing that, in some decentralized contexts, key details may surface organically through publicly accessible channels rather than a single “issuer.”

Question 28: Are there types of information, beyond those already proposed to be made available through the A&D regime and the MARC inside information disclosure regime, that would be useful for the cryptoasset market to have access to? Please specify the nature of the information, the frequency that such information should be disclosed (if applicable), and the importance to the consumer base.

Key data might include vesting schedules for team or investor tokens, governance votes or proposals, and treasury transactions. Event-driven disclosures (e.g., after any major governance decision) plus periodic snapshots (e.g., quarterly) could keep investors informed of material developments in real time.

Question 29: Do you favour any of the options set out above? If so, which one? What are the factors that led you to this decision?

We favour a coordinated, centralized channel (or small set of approved channels) for disseminating inside information, ensuring universal and real-time access to all market participants. This reduces the risk of selective or partial disclosures and fosters comparability across different platforms.

Question 30: Are there alternative options we should be considering? What might be the pros and cons of those alternative options?

One alternative is a decentralized on-chain bulletin where code commits and announcements are automatically logged. This could eliminate reliance on centralized entities, but it may be less user-friendly and lacks certain consumer-protection features.

Question 31: Should a centralised coordinating body coordinate the effort to help with identifying, developing and testing method(s) of disseminating inside information? If not, please provide alternative suggestions.

While a centralised coordinating body could offer consistency, it may conflict with the decentralised ethos of many crypto projects and could struggle to gain broad acceptance among stakeholders who value autonomy. An industry-led consortium or a flexible framework of collaborative working groups—one that allows projects of different sizes and governance models to participate voluntarily—could better accommodate the sector’s diversity while still promoting effective dissemination of inside information.

Question 33: Do you agree with these principles? Are there changes you would suggest? Are there others we should consider?

We agree that timely, fair, and accessible disclosures are essential. We propose adding a principle of proportionality to ensure that, while safeguards are robust, the regime remains adaptable for diverse business models and organizational structures.

Question 34: Should we apply the safe harbours from MAR concerning delays in disclosing inside information (MAR Article 17(4)), and possession of inside information and legitimate behaviours (MAR Article 9) to the cryptoasset market?

Yes. Extending established safe harbours provides consistency with traditional markets and gives firms clarity about acceptable delays or possession of inside information. Minor adaptations for crypto-specific scenarios (e.g., decentralized governance) may be needed, but the general framework is applicable.

Question 36: What, if any, amendments to the MAR formulation of these safe harbours should we make to them to ensure they align with the principles set out above and ensure they are tailored to the cryptoasset market? Is there any additional clarity you would need us to provide over how they would apply in order to be able to rely on them?

Clarifying how decentralized governance decisions or publicly verifiable on-chain actions factor into safe harbour conditions would be helpful. Further detail on “legitimate behaviours” tied to standard crypto activities (e.g., protocol upgrades or bug fixes) would reduce regulatory uncertainty.

Question 37: Are there other activities that we should be considering for safe harbours? Please explain your rationale including how these safe harbours would meet the principles set out.

Scheduled protocol upgrades, routine bug patches, and well-audited forks or merges could be protected where disclosures are made in open-source repositories. Such updates are often positive for network health rather than manipulative, so explicit safe harbours would deter undue liability.

Question 38: Do you agree with the approach to putting the onus on CATPs and intermediaries to both monitor and disrupt market abuse? If not, why not and what alternative do you think would better achieve the outcomes we are seeking?

We appreciate the need to address market abuse, but requiring CATPs to shoulder broad, real-time monitoring for every asset—especially those with no issuer—places a disproportionate burden on these platforms. Many CATPs, particularly smaller ones, may lack the technical and financial capacity to implement advanced surveillance systems or investigate global, decentralized networks in depth. Instead, we recommend a tiered model that differentiates between established, lower-risk assets and newer, higher-risk listings, allowing CATPs to allocate resources effectively while still meeting minimum standards. This ensures that legitimate market surveillance occurs without stifling smaller platforms or pushing them to list only the largest, most easily monitored assets.

Question 39: Do you agree with the areas of systems and controls where we will set outcomes-based requirements for CATPs and intermediaries? If not, which do you not

agree with and why? Are there any areas where we should be considering additional systems and controls either for these firms or other market participants in order to achieve the outcomes we are seeking for this regime?

An outcomes-based model is appropriate, allowing firms to tailor systems to their scale and complexity.

Question 40: Do you agree with the outcomes-based approach which allows firms to determine the best way to deliver the outcomes based on the nature, size and scale of their business?

Yes. This flexible approach encourages innovation in compliance solutions, particularly in a rapidly evolving sector like crypto. The FCA can monitor implementation and issue further guidance if certain outcomes are not being met effectively across different firm profiles.

Question 41: Do you agree that firms involved with cryptoasset trading and market sensitive information should be subject to requirements to have appropriate training regarding the handling and control of inside information and have appropriate information barriers in place within their firms?

We recognize the importance of training staff to handle market-sensitive information appropriately, but fully outsourcing this responsibility to CATPs can be resource-intensive—especially for smaller or newly formed platforms with limited budgets. To alleviate this burden, the regulator could provide standardized training modules, best-practice toolkits, or ongoing educational resources that firms can tailor to their specific needs. By offering a baseline curriculum and clear guidance, the FCA would ensure a consistent level of competence across the market while lowering the cost barrier for CATPs, thereby reducing reliance on ad hoc, firm-level solutions and promoting more uniform implementation of training standards.

Question 42: Do you agree on the proposals regarding insider lists for issuers and persons seeking cryptoasset admissions to trading?

Insider lists may be impractical for genuinely decentralized projects where no formal issuer or representative entity exists, as there is no central party capable of identifying all individuals who might possess material non-public information. In these cases, forcing a CATP or another party to assemble such lists would be disproportionately complex and likely incomplete. A more tailored approach would acknowledge that, for truly issuer less assets, critical information is often disseminated publicly via open-source channels, making the need for traditional insider lists less relevant or feasible.

Question 43: Do you feel that establishing a PDMR regime for issuers/persons seeking admission of cryptoassets would significantly advance the outcomes we are seeking at a proportionate cost?

We do not believe a formal PDMR regime would significantly advance market integrity or investor protection in a proportionate manner. Many crypto projects, particularly decentralized ones, lack a traditional management layer—making it unclear who would even qualify as a PDMR. Imposing such

obligations could become an administrative headache for smaller or issuer-less projects while offering little tangible benefit to consumers. Instead, regulators could focus on ensuring sufficient disclosure and accountability where a clear organizational structure exists, rather than applying a one-size-fits-all regime that fails to account for decentralized governance models.

Question 44: Do you agree with the approach set out with regards to requiring on-chain monitoring from CATPs and intermediaries?

Yes. On-chain analytics are vital for identifying suspicious wallet clustering, large token movements ahead of news, or other red flags unique to crypto. However, many smaller CATPs will need cost-effective third-party solutions or clear guidance on how to implement these tools practically.

Question 45: Are there any aspects of systems and controls that we haven't mentioned which would help us deliver on our desired outcomes?

Guidance on cross-border monitoring and reporting would be useful, given that crypto often involves multiple jurisdictions and varying levels of regulatory oversight. Firms could benefit from a framework to handle data conflicts and privacy constraints when investigating or sharing suspicious activity.

Question 46: Do you agree with our thinking, approach, and assessment of the potential cross-platform information sharing mechanisms discussed? Which of the options do you think is best? If none are suitable, why and what other alternatives would you suggest?

We generally support the principle of cross-platform information sharing to detect and mitigate market abuse, as it can significantly enhance transparency and protect consumers. However, we are concerned that many of the proposed mechanisms may be overly centralized and could impose substantial implementation costs—particularly for smaller CATPs that lack the resources of larger industry incumbents. For instance, establishing mandatory data-sharing consortia, centralized data repositories, or uniform technical standards requires not only significant financial investment but also considerable legal and operational coordination to address data privacy, liability, and governance issues.

We recommend exploring an approach that allows for a degree of flexibility based on a CATP's size, scope, and risk profile. One possibility is a collaborative framework in which more established or systemically important platforms implement robust data-sharing tools, while smaller CATPs adopt proportionate solutions (such as vetted third-party analytics providers) that fit within their operational constraints. In addition, industry-led or regulator-approved guidelines on common data formats and confidentiality protections would help ensure consistency and interoperability without prescribing a rigid, one-size-fits-all solution. This strikes a balance between improving market oversight and preventing barriers to entry that might reduce competition or hamper innovation in the UK crypto landscape.

Question 47: Should a centralised coordinating body coordinate the effort to help with developing and driving forward an industry-led solution to cross-platform information sharing? If not, please provide alternative suggestions to facilitate the creation of industry-led solutions.

Rather than establishing a single, centralized coordinating authority, a more organic and inclusive path would be to empower an industry-led body—such as a recognized trade association—to oversee the creation and evolution of cross-platform information sharing protocols. By drawing on the collective expertise and day-to-day experiences of varied market participants, this model would better capture the real-world nuances of cryptoasset trading and encourage broader buy-in from stakeholders who might otherwise be wary of a top-down solution. It also leaves room for flexible, incremental updates as the sector rapidly evolves, rather than locking everyone into a fixed structure that could soon become outdated.

Question 48: We would like to gauge what further support would be useful in helping introduce cross-platform information sharing. What kind of specific regulatory input or involvement would be beneficial for the industry?

One key area where further support is vital is establishing clear, consistent, and practical guidance on data governance, privacy, and liability when sharing information across different trading venues. Many CATPs hesitate to share potentially sensitive data—such as user identities, suspicious transaction patterns, or aggregated order book analytics—due to legal uncertainties and the risk of inadvertently breaching confidentiality or data protection laws. The regulator could publish a unified set of best practices and safe-harbour provisions, offering reassurance that platforms acting in good faith and following specified protocols will not be unduly penalized.

Additionally, industry participants could benefit from a structured sandbox or pilot program that allows them to test different data-sharing methods (e.g., centralized repositories, distributed ledgers, or encrypted data channels) under FCA oversight. This program would help uncover technical challenges in real time and refine how firms exchange information without compromising user privacy or trading competitiveness. Lastly, the regulator could facilitate workshops or working groups—ideally in partnership with an industry-led body—to define shared standards around data formats, encryption, and incident reporting. By clarifying rules and incentivizing collaboration, the FCA would reduce friction and encourage a coordinated solution to market abuse in the crypto sector.

Question 49: Is there any further information or feedback you would like to provide to us?

We commend the FCA for proactively shaping a cryptoasset regulatory framework. Ongoing engagement and dialogue with industry, particularly as decentralized finance and emerging token models evolve, will ensure the regime remains effective, proportionate, and globally competitive. We stand ready to collaborate and provide additional input as the proposals develop.

List of EMA members as of March 2025

Airbnb Inc
Aircash
Airwallex (UK) Limited
Amazon
Ambr
American Express
Banked
Benjamin Finance Ltd.
Bitstamp
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
Cardaq Ltd
CashFlows
Circle
Coinbase
Contis
Crypto.com
Currenxie Technologies Limited
Curve UK LTD
Decta Limited
Deel
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
EPG Financial Services Limited
eToro Money
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Finance Incorporated Limited
Financial House Limited
FinXP
First Rate Exchange Services
Fiserv
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
iFAST Global Bank Limited
Imagor SA
Ixis Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Kraken
Lightspark Group, Inc.
Modulr Finance B.V.
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand Ltd
MuchBetter
myPOS Payments Ltd
Navro Group Limited
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
OpenPayd
Owl Payments Europe Limited
Own.Solutions
Papaya Global / Azimo
Park Card Services Limited
Payhawk Financial Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal
Paysafe Group
Paysend EU DAC
Plaid B.V.
Pleo Financial Services A/S
PPS
Push Labs Limited
Remitly
Revolut
Ripple
Satispay Europe S.A.
Securiclick Limited
Segpay
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
TransactPay
TransferGo Ltd
TransferMate Global Payments
TrueLayer Limited
Uber BV
Unzer Luxembourg SA
VallettaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay

