Introduction to anti-money laundering regulations – Responses to questions from firms

Regulatory perimeter, regimes and transition

Overarching Question:
How do the current Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) interact with the forthcoming Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026 (FSMA) regime, and what should firms be doing during the transition period?

For firms wanting to provide cryptoasset services in scope of the MLRs, MLR registration remains the route to operate before the new FSMA regime commences in October 2027.

However, firms that are registered with us under the MLRs should note that there will be no automatic conversion and that they will need to secure authorisation by us under FSMA.

Firms that are already authorised under FSMA to undertake other regulated activities will need to vary their existing permissions if they wish to offer one of new cryptoasset regulated activities when the regime commences.

Applications under the FSMA regime

We will start accepting applications for FSMA authorisation from 30 September 2026. We encourage new firms to focus on securing authorisation under FSMA, rather than applying for registration under the MLRs.

However, firms that still want to apply for registration after 30 September 2026 should contact our Pre-application support service (PASS) to explain their plans and why they need registration.

Where a firm can make a case for applying for registration after 30 September 2026, we will accept the information contained in a firm's application form for authorisation under FSMA as information relevant to its application for registration under the MLRs. This is subject to the firm confirming that it wants us to do this. There is further information here for firms considering applying for registration.

In preparing for the opening of the application period on 30 September 2026, firms should focus on confirming whether they are in scope of the new regime, identify which permissions they need, and starting early gap analysis against the threshold conditions and our proposed rules. Our proposed rules can be found across various Consultation Papers published in readiness for the new regime, including CP25/25 on the Application of the FCA Handbook for Cryptoasset Activities (which includes our proposed financial crime rules) and CP26/4 on the application of the FCA handbook for Cryptoasset

Activities (Part 2). As above, firms should also consider whether applying under the MLRs remains appropriate for their business plan, particularly where their intended model will predominantly fall within the future FSMA perimeter.

Firms should also consider the impact of **when** they submit their application. The application window will be open from 30 September 2026 until 28 February 2027, and whether a firm applies during this window or not will have regulatory implications. Further information on how the gateway will operate is available on our website. . .

Firms should note that this information is not relevant to cryptoasset firms that won't benefit from one of the exemptions from registration under Regulation 54(1A)(b) of the MLRs. These firms will still need to register with us once the FSMA regime has begun and the MLR gateway will continue to operate as normal for them.

Authorisation expectations and application quality

Overarching Question:
What are the FCA's expectations of firms' systems and controls, anti-money laundering (AML) and financial crime governance when applying for authorisation under the new cryptoasset regime?

Firms should plan for a financial crime assessment under the new cryptoasset regime, which is broader than MLR registration and includes an assessment of governance, systems and controls, resources and readiness, among other areas. We encourage firms to interact with our financial crime guidance, and consider using our pre-application support service (PASS) to introduce their business model, discuss key risks and mitigations and clarify our requirements/expectation early. This can all lead to a more efficient assessment.

Innovative or 'pure on-chain' models should focus on evidencing a risk-based AML/counter terrorist financing (CTF)/counter proliferation financing (CPF) approach that is calibrated to the firm's transaction flows and typology exposure (rather than assuming a different set of expectations). Where firms are pre-launch, evidence can include control design and implementation documentation (process maps, configuration evidence, scenario testing/UAT, MI packs, governance sign-off and a credible mobilisation plan) to demonstrate readiness by commencement.

We are aware that firms may use technology (including AI/ML tools) to support risk assessment and monitoring. However, the firm remains responsible for the outcomes and must ensure that it meets our expectations.

The most effective way to aid the assessment process remains submitting a complete, well-evidenced application aligned to the permissions sought. Therefore, we would further encourage firms to familiarise themselves with our proposed rules. CP25/25 includes our proposed financial crime requirements, to apply the financial crime elements of SYSC 6, as well as the Financial Crime Guide (FCG) and Financial Crime Thematic Reviews (FCTR).

We will continue to publish updates and engagement materials via our cryptoasset regime webpages. Firms should monitor these pages for further publications as the application period and regime commencement approach.

AML governance, MLRO and senior management arrangements

Overarching Question:

What governance, leadership and resourcing arrangements does the FCA expect firms to have in place for AML to prevent financial crime?

Firms seeking FSMA authorisation must comply with the FCA's expectations regarding systems and controls, governance and leadership. We expect firms to assess their own governance, reporting lines and individuals' fitness and propriety according to the standards set out in our rules, including SYSC and the SM&CR.

Firms must demonstrate clear governance and appropriate resourcing for financial crime risk management that is proportionate to the nature, scale and complexity of the cryptoasset business model. In practice, this means clear senior ownership and accountability, effective escalation routes, and management information that enables sufficient oversight, following SYSC 3.

Firms should ensure individuals in key AML roles (including the MLRO) are competent and appropriately experienced for the activities and risks in scope, and have sufficient time and resources to discharge their responsibilities effectively, as per the Competent employees rule in SYSC 3.1.6.

Where responsibilities are combined or reporting lines sit within an operational function (for example, reporting to a COO), firms should be able to demonstrate how potential conflicts are identified and managed, how independence and challenge are maintained, and how the MLRO has appropriate access to senior decision-makers. Resourcing should keep pace with growth and the firm's risk profile, and firms should be ready to explain to us why and when roles will need to separate as the business scales.

For integration-based or non-custodial models, obligations will depend on the activities being carried on and the firm's role in the transaction flow. Firms should be prepared to explain what the firm does (and does not) do, where it sits in the customer journey, and how risks are managed across any reliance on third parties (including through appropriate oversight and contractual arrangements).

AML framework design and documentation

Overarching Question

What are the FCA's expectations for the design and documentation of a firm's AML framework?

Firms should maintain a risk-based AML framework that is proportionate and tailored to the firm's cryptoasset activities. The FCA does not assess quality by document length or the use of standard templates; we look for a clear, internally consistent set of documents that reflects how the firm will operate.

The business-wide risk assessment (BWRA) is a foundational document and should be in place before a firm seeks registration/authorisation for in-scope activity. It should be kept up to date and reviewed whenever there are material changes. For example, new products, customer types, geographies, delivery channels, or changes to transaction flow.

Firms may use templates as a starting point but should ensure policies and procedures are appropriately tailored to the firm's business model and risk profile, embedded in day-to-day operations, and evidenced in practice (including training, MI, and governance sign-off).

Where firms are exposed to 'indirect risk' through counterparties, intermediaries or third parties, these risks should be identified and assessed in the BWRA and appropriately reflected in due diligence, ongoing monitoring and oversight arrangements.

Crypto-specific risk assessment and typologies

Overarching Question
How does the FCA expect firms to identify and assess money laundering risks specific to cryptoassets and cryptoasset services?

Following Regulation 18 of the MLRs, we expect firms to take a risk-based approach to identifying and assessing ML/TF/PF risks that are specific to their cryptoasset activities.

Firms are also expected to demonstrate how the business wide risk assessment (BWRA) drives their customer due diligence, monitoring and wider control framework. A strong BWRA will be one that is grounded in the firm's transaction flows and exposure points, rather than a generic list of crypto risks.

In practice, the BWRA should consider:

- the products and services offered (including features that affect traceability and typology exposure)
- customer types and expected use cases,
- geographic exposure
- delivery channels
- transaction risk, and
- the way the firm interacts with third parties or counterparties.

We would also expect firms to be able to explain which typologies are most relevant to their model and how controls mitigate them.

Firms should apply the MLR requirements on politically exposed persons (PEPs) and adopt a proportionate, risk-based approach to identifying and managing PEP relationships, including enhanced due diligence where required.

Transaction monitoring, Blockchain analytics and surveillance tools

Overarching Question
What does the FCA expect firms to demonstrate in relation to transaction monitoring, Blockchain analytics and surveillance capabilities?

Firms should be able to evidence that their transaction monitoring and surveillance arrangements are proportionate to the risks arising from their business model and risk profile, and can identify and investigate suspicious activity. This includes demonstrating how monitoring coverage operates across the customer journey, how alerts are generated, triaged and escalated, and how outcomes are recorded, reviewed and reported.

Where firms use Blockchain analytics or transaction monitoring (whether developed in-house or provided by a third-party), they should be able to explain why the solution is appropriate to the risks identified, what it does and does not cover, how it is configured and used in practice, the outcomes produced and how effectiveness is tested and overseen. We remind firms that Blockchain analytics forms only one aspect of financial crime controls, and should complement existing financial crime controls.

Where firms rely on third parties (for example, payment gateways or other partners), the firm remains responsible for meeting its regulatory obligations. Firms should be able to explain clearly which controls and checks are performed by who, what information is being shared, and how risks are managed on an end-to-end basis. This should be supported by appropriate oversight and assurance over any outsourced or delegated activities. SYSC 8 outlines our general outsourcing requirements, including third party dependencies, for FSMA authorised firms.

Travel Rule and information sharing

Overarching Question
How does the FCA expect firms to comply with the Travel Rule across different cryptoasset business models?

The Travel Rule obligations form part of the MLRs, which operates concurrently to the new activities under the new FSMA regime. Regulation 64A and 64B of the MLRs define cryptoasset transfers, and the scope to which the Travel Rule applies.

Firms should consider if the activity they are engaging in brings them into scope of the MLRs (Regulation 14A). The Travel Rule applies where a transfer is made within the meaning of Regulation 64A and Regulation 65B. This will need to be assessed on a firm-by-firm basis, taking account of a firm's individual business and operating model. Firms are generally advised to seek out their own independent legal advice unique to their business model and activities to understand their compliance obligations.

To provide some high-level examples, cryptoasset transfers where the originator and beneficiary are the same cryptoasset business, or where both hold accounts with the same cryptoasset business, may be exempt from Travel Rule obligations. Arranging firms could be subject to the Travel Rule, depending on if they are caught by the definitions in Regulation 14A, and if they are completing a transfer in line with Regulation 64A and Regulation 64B. If a firm is 'arranging' cryptoassets transactions and in scope of the MLRs as a cryptoasset exchange provider under the MLRs, the Travel Rule can apply even if the firm does not itself custody of transmit the cryptoassets.

Firms should consider if their business model for staking will constitute a transfer for the purposes of Regulation 64A, including whether the use of custodial or pooled staking models will engage the Travel Rule.

Sanctions, fraud and broader financial crime controls

Overarching Question
How do AML expectations for cryptoasset firms align with other financial crime obligations, including sanctions and fraud?

Firms should recognise that AML/CTF/CPF controls sit alongside other relevant financial crime obligations and risks, including sanctions and fraud. This should be reflected in governance arrangements, risk assessments, monitoring and escalation processes, and in how controls operate end-to-end across the customer journey.

For sanctions screening, the FCA expects firms to have appropriate governance over data sources (including the UK Sanctions List) and screening tools, together with periodic testing and/or quality assurance to assess whether screening arrangements remain effective. The frequency and depth of testing should be proportionate to the firm's risk profile and to relevant changes. For example, updates to the UK sanctions list, model changes, and new products. Following SYSC 3.1.2 and the Financial Crime Guide (FCG).

Operational resilience and systems considerations

Overarching Question
How do AML obligations interact with operational resilience and wider system-level risks for cryptoasset firms?

We expect firms to recognise the close links between operational resilience and financial crime controls. Disruption to systems and processes, ineffective change management, or weak oversight of third-party arrangements can create and amplify exposure to financial crime risk.

In testing operational resilience, firms should demonstrate how they have identified their important business services (IBS), focusing on customer or market-facing outcomes.

Where firms rely on common infrastructure or concentrated third-party providers, they should consider the operational resilience and financial crime implications of those dependencies. Relevant risks should be reflected in the risk assessment and supporting systems and controls, consulting our standards and expectations throughout.

Cross-border activity and international alignment

Overarching Question
How does the FCA approach AML supervision for cryptoasset firms operating across multiple jurisdictions?

Given the cross-border nature of cryptoasset services, firms operating across multiple jurisdictions should ensure their UK AML framework meets UK regulatory requirements

and is implemented effectively in respect of UK in-scope activity, regardless of the location of group policies, systems, or overseas operations.

Firms should be able to explain how group governance and decision-making arrangements work in practice and demonstrate how these comply with UK AML regulations.

Where group entities or third parties perform elements of AML controls (for example, screening or monitoring), firms should maintain an appropriate level of oversight, information sharing, record keeping and escalation arrangements, and should ensure responsibilities are clearly allocated. Firms should also consider how different jurisdictions' requirements (including Travel Rule implementation) interact with their operating model and reflect this in their BWRA and supporting policies and procedures.