Stay Current

PAUL HASTINGS

March 2026

Follow us on LinkedIn

Regulatory Update

FCA Insights: Key Anti-Money Laundering and Counterterrorist Financing Framework Expectations for Cryptoasset Firms

By Nina Moffatt, Arun Srivastava, Bhavesh Panchal & Samantha Wood

The Financial Conduct Authority (FCA) held a webinar on 18 March regarding its expectations for cryptoasset firms' anti-money laundering (AML), counterterrorist financing (CTF) and proliferation financing frameworks (AML framework) under the new cryptoasset regime in accordance with the Financial Services and Markets Act 2000 (FSMA).

The webinar shared critical insights relevant to firms already registered under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), as well as new market entrants.

While firms under the new FSMA regime will remain subject to the MLRs (as crypto-asset registered firms are today), they will also be subject to broader financial crime obligations, such as in relation to sanctions. It is clear from the webinar that the FCA will continue to be focussed on cryptoasset firms' AML frameworks and on the role of the Money Laundering Reporting Office (MLRO).

Key Takeaways

1. **Money Laundering Reporting Officer:** The role of the MLRO is pivotal to application success:

    - **Resource and capacity:** MLROs must dedicate sufficient time for policy design and maintenance, ad hoc advisory service to the business and effective first-line challenge. MLROs must have suitable deputies for any period of leave.
    - **Knowledge and experience:** MLROs must demonstrate an understanding of how the risk factors in Regulation 18 of the MLRs (customer, geography, products and services, transaction and delivery channels) and crypto-specific typologies and risks (e.g., via sources like FCA Financial Crime Guide (FCG), Good and Poor Practices, and JMLSG guidance) apply to the firm's proposed business.
    - **AI:** Where AI tools in AML processes are used, there should be an understanding of how the algorithm operates based on the inputs and outputs of data. MLROs must also show that they know the governance/reporting lines in the firm.
    - **Competence and capability:** No formal qualifications are required, but prior regulated experience (especially in financial crime) and crypto-specific training are advantageous.
    - **Time commitment:** The MLRO must be able to demonstrate that they have sufficient bandwidth to perform the role.

- **Conflicts:** The MLRO can be combined with other functions, provided no conflicts arise (e.g., the MLRO cannot be involved in first-line, business development).

2. **Business-Wide Risk Assessment:** As with MLR applications, this is a cornerstone document:

   - The BWRA must be proportionate to firm's size.
   - The BWRA must be accompanied by a clear methodology detailing inherent risk identification/scoring (e.g., via 5x5 heatmap), control testing (using dummy/test data even for non-operational firms), residual risk calculation, sources (e.g., National Risk Assessment), senior management involvement, oversight and approval, and repeatability.
   - It must include transparent and considered inherent risks to the firm's business, effectiveness of controls assessments (demonstrated via testing) and residual risks (which may remain high even with strong controls).
   - The BWRA must align with the firm's risk appetite. If there are risks outside of the firm's stated risk appetite, then mitigation plans must be documented.
   - Common pitfalls include conflating control failures (e.g., late SARs) with inherent risks.

3. **Customer Risk Assessment:** CRAs must align closely with BWRA. The key elements include:

   - Assessment of Regulation 18 of the MLRs risk factors, relationship purpose, transaction size and nature, and duration and regularity.
   - Holistic weighting of factors (not isolated), driving due diligence levels, TM thresholds and review frequency.
   - Inclusion of red flags and automatic escalation triggers (e.g., PEPs, sanctioned wallet exposure) and overrides.
   - Methodology detailing scoring, thresholds (low, medium, high), judgment and overrides, and senior management approval and sign-off.

4. **Transaction Monitoring:** The FCA reiterated that TM is essential for detecting suspicious activity. Firms must justify tool selection (commercial or in-house) and cover:

   - How TM is embedded into operations, how monitoring of the TM tools' effectiveness is conducted, and calibration of the TM tools to the risk profile and business conducted by the firm.
   - TM must cover off-chain fiat and on-chain cryptoassets.
   - There must be high-risk wallet blocking and wallet screening/re-screening.
   - TM control must cover alert escalation, backlog management, adaptation to risk changes and clear links to SAR filing.
   - The FCA is keen to ensure that firms are candid about challenges (e.g., alert volumes, resources) and governance and escalation processes.

5. **Travel Rule:** The FCA is keen to ensure that firms are open about the challenges they may face, such as counterparty identification, potential fund delays and dealing with the sunrise issue. Applications should detail:

   - Chosen solution(s) and rationale for utilising that solution.
   - Tailoring to business model, accompanied by a flow-of-funds diagram linking to in-scope transactions and travel rule data requirements.
   - Integration into AML framework.
   - Handling of inter-business transfers, unhosted wallets and counterparty discovery, delays/risk assessments pending receipt of mandated travel rule information, escalation, and governance and reporting.

6. **Other Key Points:** The FCA also provided attendees with a chance to raise Q&As at the end of the session. Some interesting points discussed included:

    - **Global vs. UK AML frameworks:** Full localisation is not required, but any controls operated overseas must meet UK standards with oversight, quality assurance and audits from a UK perspective. In practice, this may result in many global firms simplifying their AML structures to incorporate localised requirements.
    - **AI in AML:** The FCA does not have any opposition to utilising AI in AML frameworks. However, where AI is used, firms must be able to provide an explanation of how the AI tool operates in the AML framework and the evidence of algorithms and outcomes.
    - **TM flexibility:** The FCA is open to both in-sourced or outsourced tools, provided that they are tested and cover all products offered by the firm. While testing may prove difficult for non-operational firms, the FCA expects firms to use dummy data for control testing.

Implications for Firms

With the new FSMA crypto regime on the horizon (the application window opens in September 2026), the FCA expects high standards for applicant's AML frameworks.

Firms should prioritise these core AML elements, ensuring crypto-specific risk understanding, robust documentation and demonstrable control effectiveness.

We recommend reviewing your AML framework against these points and considering pre-application enhancements. Our team is available to discuss how these insights apply to your specific business model or application strategy.

Please contact a member of the Paul Hastings team if you wish to discuss any of the themes and FCA concerns we are seeing in the market.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Nina Moffatt
+44-20-3023-5248
ninamoffatt@paulhastings.com

Arun Srivastava
+44-20-3023-5230
arunsrivastava@paulhastings.com

Samantha Wood
+44-20-3023-5234
samanthawood@paulhastings.com

Bhavesh Panchal
+44-20-3023-5148
bhaveshpanchal@paulhastings.com