Bitcoin Policy
UNITED KINGDOM

Response to HM Treasury's Technical Consultation on Amendments to the Money Laundering Regulations 2017 (the Money Laundering and Terrorist Financing (Amendment and Miscellaneous Provision) Regulations 2025 (the Draft SI or the SI))

Submitted: 20 September 2025

---

1. Executive Summary

Bitcoin Policy UK (BPUK) is an independent, non-partisan organisation established to ensure that the UK develops coherent and forward-looking policies towards Bitcoin, based on objective fact and with a view to benefitting both the UK's citizens and our national economy. Our members include professionals from law, accountancy, engineering, financial services, education and the technology sector.

We welcome the opportunity to respond to HM Treasury's technical consultation on amendments to the Money Laundering Regulations 2017 (MLRs). Our comments are focused exclusively on the provisions that may affect Bitcoin and the businesses built around it.

BPUK recognises the need for robust anti-money laundering and counter-terrorist financing (AML/CTF) controls. However, any such regulation must be:

- **Proportionate and risk-based** – ensuring that compliance burdens are targeted where risks are real and evidenced, and not so excessive as to discourage UK growth and investment in a new industry;
- **Clear on scope** – avoiding regulatory overreach that inadvertently captures open-source developers, self-custody tools, or other actors who cannot perform AML functions;
- **Respectful of privacy and safety** – recognising the unique transparency of Bitcoin, and the real risks of physical harm if personally identifiable information is unnecessarily linked to on-chain addresses; and
- **Supportive of UK competitiveness** – ensuring that the UK's ambition to be a leading financial centre and "crypto hub" is not undermined by excessive or poorly tailored obligations.

Our detailed comments are set out below.

---

2. Definitions & Scope – "Cryptoasset Business" (Draft SI Regulation 4(a))

The draft instrument inserts a new definition of "cryptoasset business" (Regulation 4(a), via reference to the definition of 'cryptoasset business' in Regulation 64B of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017).

While we support efforts to ensure definitional clarity and consistency, any such provisions must carefully delineate scope. We note that the definition of "cryptoasset business" taken from the 'Information on the Payer' Regulations, means "a cryptoasset exchange provider or a custodian wallet provider". BPUK agrees that the scope of the definition should be limited in this way, and

limited either to exchanges or custodians, who will typically and in most cases already perform necessary checks on their customers. However, although the current definition appears to be of appropriate extent, BPUK recommends that its clarity could be improved, by expressly excluding businesses and persons that do not provide custodial or intermediary services in respect of cryptoassets. We cite the example of the European Union's flagship piece of legislation (the Markets in Cryptoasset Regulation or MiCA). MiCA explicitly provides at Article 83 that "*Hardware or software providers of non-custodial wallets should not fall within the scope of this Regulation*," having the immediate effect of giving persons and businesses operating in the EU and whose business relates solely to non-custodial solutions the comfort that they can freely operate and grow their businesses in the EU without the cost or risks of ensuring compliance with MiCA.

This clear approach is mirrored in other legislation besides. Much like MiCA, the European Union's AML Regulation (Recital 160, Article 79) rightly excludes non-custodial wallet providers from scope, making clear that relevant prohibitions do not apply " t*o providers of hardware and software or providers of self-hosted wallets insofar as they do not possess access to or control over those crypto-asset wallets*."

We would recommend that similar provisions are adopted here in the UK.

Explicit exclusions should be made for:

- **Open-source developers** (e.g. contributors to Bitcoin Core or wallet software).
- **Providers of self-hosted wallet tools** who never take custody of customer funds.
- **Node operators and miners**, whose role is to secure and validate the network and transactions made on the network, not to intermediate transactions or to act as payment processors or custodians with control of or legal title to funds.

These actors have no ability to perform AML/CTF functions. Including them, even implicitly, would create unworkable obligations and risk chilling innovation. Furthermore, failure to give persons and businesses equivalent comfort that their activities are definitively outside scope will only serve to increase the UK's poor international reputation in this growing industry and cement the impression that (unlike the EU and the United States) the UK is a hostile environment where regulators and lawmakers have a limited to poor understanding of the sector.

---

3. Counterparty Due Diligence for Cryptoasset Businesses – New Regulation 34A

The draft instrument introduces a new Regulation 34A requiring cryptoasset businesses to conduct due diligence on counterparties.

We recognise that such obligations are workable only where both sides of a transaction are hosted by regulated service providers. Extending this requirement to interactions with **self-hosted wallets** would be infeasible, disproportionate, and dangerous (if not purely impossible as a question of fact), and we support the extension of this requirement only to cryptoasset exchange providers and custodian wallet providers as contemplated by the SI. However, we reiterate our point above, that the legislation would benefit from the explicit exclusion of those to whom it does not apply (namely developers, or the creators and operators of self-hosted and self-sovereign hardware and software), in much the same way as MiCA has clarified this explicitly for the purposes of EU Legislation.

Further developing the position we set out above, any requirement upon hardware or software developers to comply with comparable requirements would be:

- **Infeasible:** By design, bitcoin users can transact peer-to-peer without intermediaries. A service provider cannot compel a self-hosted wallet user or developer to provide customer due diligence information, not least because this information is simply unavailable;
- **Disproportionate:** Everyday peer-to-peer use of bitcoin, including small-value payments, would be burdened with intrusive checks, despite presenting negligible AML risk; and
- **Dangerous:** Combining personally identifiable information with on-chain wallet addresses creates a "roadmap" for criminals. As BPUK has previously set out in evidence provided in response to consultations on the HMRC implementation of the proposed cryptoasset reporting framework , there has been a notable increase in the number of robberies, kidnappings and other violent attacks against bitcoin holders, each directly connected to personal information about such holders being or becoming available online.

Recommendation:

- Limit the applicability of Regulation 34A to hosted-to-hosted transactions.
- Explicitly exclude self-custody wallets from the definition of "counterparties."
- Introduce de minimis thresholds even for cryptoasset exchange providers and custodian wallet providers (e.g. aligned with the US $3,000 Travel Rule) to ensure proportionality.

---

4. Information Sharing & Coordination – Regulations 27–30 (Regulations 52A & 52B)

We note the proposal to extend information-sharing powers to cryptoasset businesses, including the addition of the Financial Reporting and Coordination Council (FRCC) to Regulation 52(5) - adding 'cryptoasset businesses' to the relevant bodies captured by the regulation, and changes to the statutory defence in Regulation 52B of the MLR (Information on the Payer).

BPUK supports improved regulatory coordination where it is targeted and necessary. However, owing largely to the particular nature of Bitcoin both as an asset and as a publicly viewable transaction ledger, safeguards are essential. Unlike traditional financial accounts, bitcoin wallet addresses publicly reveal both balances and the transaction history of that address. Linking these addresses to names, dates of birth and home addresses, and then sharing that data across multiple bodies, creates an unprecedented risk if data is breached or misused. As we noted above with reference to our previous consultation response relating to the Cryptoasset Reporting Framework, this can and does put the holders of Bitcoin at a disproportionate risk of harm if the entirely probable data breaches occur (as they inevitably will) and expose Bitcoin holders to severe risk of physical harm and danger.

The UK has already seen major breaches of sensitive personal data in other sectors, including healthcare and government records. The risk here is magnified by the nature of bitcoin: once stolen, it cannot be frozen or a transaction reversed so as to return funds to a victim.

Recommendation:

- Adopt a principle of **data minimisation**: share only what is strictly necessary, with strong encryption and retention limits. Reporting thresholds should be kept at a proportionate level and regularly reviewed so as to keep pace with inflation and currency debasement.

- Provide explicit guidance that wallet address data should not be shared alongside personally identifying information except where strictly necessary and proportionate.

---

5. Registration & Fitness / Change in Control for Cryptoasset Firms (Regulations 31, 37, 38)

In general terms, we support the alignment of the "fit and proper" test with the FSMA "controller" regime, and the intention to close loopholes in ownership structures. The application of such pre-existing structures from the current regime to the emerging Bitcoin system is a sensible application of the 'same risk, same regulation' principle that we have supported in the past.

However, clarity of scope remains critical. The regime must not inadvertently extend to actors who are not providing regulated services, such as:

- Developers of open-source software.
- Providers of non-custodial/self-hosted wallets.
- Miners and node operators.

These participants cannot perform AML functions, and including them risks creating an unworkable and hostile environment for legitimate bitcoin activity in the UK. As per our statements above, it would be prudent to emulate the approach taken in this context by European regulators and explicitly clarify in our own legislation that such persons are excluded from scope, for the simple reason that they cannot comply (given the fundamental lack of decision-making control over the distributed and decentralised elements of the Bitcoin protocol).

Recommendation:

- Amend guidance to clarify that the registration and change-in-control regime applies only to custodial and intermediary businesses.
- Ensure thresholds do not deter legitimate investment or restructuring in UK-based bitcoin firms.

---

6. Currency Conversions & Thresholds

We support the replacement of euro-denominated thresholds with sterling equivalents for simplicity and consistency.

However, we caution that the proposed **£800 threshold** for certain CDD triggers is too low if applied indiscriminately to bitcoin transactions. Given the volatility of exchange rates and the small-value nature of many legitimate bitcoin uses (e.g. remittances or day to day payments), such a low threshold risks capturing activity that presents no material AML/CTF risk.

Recommendation:

- Apply thresholds on a **risk-based basis**, with flexibility for firms to avoid imposing intrusive checks on low-value, low-risk transactions.
- Keep all thresholds under review and increase them proportionately so as to keep them in line with inflation and currency debasement over time.

---

7. Additional Observations

- **Pooled client accounts:** BPUK urges that enhanced measures for pooled accounts should not be used by banks as a justification for wholesale de-banking of lawful bitcoin businesses. The UK's ambition to be a crypto and Bitcoin hub is undermined when firms are debanked arbitrarily. We have previously submitted evidence (both oral and written) to Parliamentary committees and to the relevant APPG providing examples of businesses that are leaving the UK or choosing not to offer products and services here as a direct result of the hostile environment created largely by the Financial Conduct Authority.
- **Suspicious Activity Reporting:** Expanding reporting without a sound evidential basis risks imposing cost without benefit. As set out in BPUK's FOIA request to the National Crime Agency, official claims about the scale of "illicit crypto transactions" lack transparency and robust methodology. The latest data from the market leader in this space, Chainalysis , shows that a mere 0.14% of ALL cryptocurrency transactions made globally in 2024 were thought to be illicit (meaning that more than 99.5% of all global cryptocurrency transactions were lawful). **Regulation must be grounded in evidence, not assumption, and we encourage the Secretary of State also to adopt this approach**.

---

8. Conclusion

The UK has an opportunity to design a regulatory framework for Bitcoin that is both robust in its defence against illicit finance and which at the same time enables innovation and the growth of a new industry in which the UK, with its long history in financial services and information technology, should be leading. That we are not currently pre-eminent in this new industry is largely the fault of the FCA, which has hitherto acted as a blocker and a headwind to the sector, resistant to all attempts at outreach and education by willing industry participants.

The proposed amendments to the MLRs will only achieve the desired balance if they are proportionate, clear in scope, and mindful of the privacy and safety of UK citizens.

BPUK stands ready to assist HM Treasury, the FCA and other stakeholders in further refining these measures, and to provide expertise on the technical realities of Bitcoin and the ecosystem of businesses that are growing up around it - but which still face significant headwinds in the United Kingdom.

Freddie New

Co-Founder and Chief Policy Officer

Bitcoin Policy UK

freddie@bitcoinpolicy.uk