CryptoUK

7 September 2026

CryptoUK
Formal House
60 St George's Place
Cheltenham
GL50 3PN

Submitted by email: civilinfoandinspectionpowerspolicy@hmrc.gov.uk

Dear HMRC

Response to the technical consultation on reforming civil tax information and inspection powers and modernising the definitions about computer records

CryptoUK welcomes the opportunity to comment on the draft legislation concerning HMRC's civil information and inspection powers under Schedule 36 to the Finance Act 2008 and the proposed amendments to section 114.

CryptoUK cannot support the measure as presently drafted. The perimeter of the proposed powers, the categories of recipient and the safeguards governing sensitive technical and personal data remain too uncertain. The Government should therefore remove the measure from the forthcoming legislation, or defer it pending further consultation and revised draft legislation which defines those boundaries and safeguards.

The linking of identity or location data to cryptoasset holdings can create particular physical-security risks that are distinct from traditional financial records. Cryptoasset holdings may be readily transferable and controlled through compromised credentials. The proposed powers should not be designed by analogy with traditional financial records without express consideration of those differences.

1. Financial Institution Notices and tax software providers

CryptoUK does not support the proposed extension of the Financial Institution Notice regime in its present form. The definition of "cryptoasset service provider" is broad, while the legislation and explanatory material do not define adequate boundaries for its use.

HMRC has confirmed in correspondence that the definition is intended solely to extend the Financial Institution Notice perimeter and is separate from the amendments to section 114. It has also confirmed that cryptoasset tax-software providers are intended to fall within that definition. That approach should not proceed without further consultation and clearer statutory limits.

HMRC has also explained that it would generally seek information from the taxpayer or, where appropriate, another third party such as an exchange, before approaching a tax-software provider. That expected sequence should be stated in the legislation or explanatory material. Information should be sought from the least intrusive and least burdened adequate source.

At a minimum, the final framework should distinguish providers that hold, administer, exchange or execute transactions in cryptoassets from standalone tax-calculation, software-development, advisory and infrastructure providers. A non-transactional provider should not receive a notice unless HMRC has recorded why the information is necessary, why it is unavailable from the taxpayer, exchange, custodian or another more direct source, and why the burden and security consequences are proportionate. This matters because a Financial Institution Notice does not require taxpayer agreement or prior tribunal approval, and its recipient has no appeal against the notice itself.

Every notice should be authorised by an HMRC officer who has considered and recorded its necessity, proportionality, provider connection and available less-intrusive alternatives. Notices seeking high-risk linked data, material from a non-transactional provider, or access to technical systems should require senior independent approval within HMRC before issue.

CryptoUK does not suggest that the domestic perimeter must reproduce the Crypto-Asset Reporting Framework exactly. Its business, covered-activity and UK-nexus tests nevertheless provide a useful baseline. Any material departure should be identified and explained so that software providers, protocol developers, wallet providers, custodians, exchanges, brokers, validators and other infrastructure providers can determine whether and why they are within scope.

2. Section 114 and technical records

The proposed section 114 amendments are intended to modernise the treatment of records created, stored or processed through software, cloud services and automated systems. HMRC has explained that there may be cases in which checking a taxpayer's position requires an understanding of how records were created, processed or calculated. CryptoUK recognises that legitimate need.

Section 114 does not itself create the underlying power to require or inspect material. The concern is how its broader references to 'anything' containing information and to persons involved in creating, developing or producing it will operate when another statutory power applies. Understanding a calculation will not ordinarily require unrestricted access to source code, a live system or an entire technical environment. Such access could reveal security controls, confidential information, legally privileged material and third-party intellectual property which extend beyond the tax evidence required.

The final framework should favour the least intrusive adequate method. Depending on the case, this may be a written explanation, a demonstration, controlled testing or an independent technical report. More intrusive access should be tightly scoped, supported by written reasons and subject to safeguards for privilege, confidentiality, system security, retention and onward disclosure.

3. Controlling credentials and high-risk linked data

The legislation should expressly exclude private keys, seed phrases, passwords, signing keys, authentication credentials and any equivalent secret capable of enabling an asset transfer or access to a system. The exclusion should turn on what the information enables a person to do, rather than its terminology or format. It would not prevent HMRC obtaining transaction histories, public addresses, account records, audit evidence or other non-controlling material needed to establish a tax fact.

HMRC should confirm whether the expanded powers could permit it to obtain or combine identifying information, including a person's name, residential address, passport details or family-location information, with wallet addresses, asset holdings, asset values or other information from which cryptoasset wealth may be inferred. Where that is possible, the legislation should impose specific necessity, data-minimisation, access-control, retention, incident-response and onward-disclosure safeguards. The risk arises from the sensitivity of the combined dataset, not from any assumption that HMRC will routinely create one.

4. Identification notices

The draft broadens identifying information to include information which identifies a person alone or together with other information. CryptoUK accepts that modern identifiers such as email addresses, National Insurance numbers and Unique Taxpayer References can assist HMRC in identifying a specific taxpayer. The power should nevertheless require the least identifying and least dangerous information adequate for the statutory purpose. Passport details, residential or family-location information and linked identity-and-holdings data should not be requested unless they are necessary; and where they are necessary, the enhanced safeguards for high-risk linked data should apply.

5. Information concerning deceased persons

The draft would permit information notices under paragraphs 1 or 2 of Schedule 36 more than four years after a person's death with tribunal approval. The policy paper also indicates that the existing authorised-officer approval process would apply to Financial Institution Notices. HMRC attributes the reform to changes associated with OECD information-exchange standards, but the published material does not identify the relevant recommendation or the cases which have demonstrated the need for this change.

We therefore ask HMRC to identify the OECD report, recommendation and wording relied upon, the expected use of the power and its practical outer limit. The final explanation should also address its interaction with assessment and record-retention periods and the burden on personal representatives and third-party record holders. Independent approval should remain an essential safeguard for notices issued more than four years after death.

6. Unavailable and historical records

The legislation should distinguish a refusal to comply from an inability to produce information which was never held, was lawfully deleted, was lost without fault or is not reasonably recoverable. A person should not be penalised in those circumstances where they can explain the position and have taken reasonable steps to identify adequate alternative evidence.

Before imposing a penalty, HMRC should consider possession or control, applicable retention periods, the reason for the record's unavailability, the cost and proportionality of recovery and whether the information is available from a less burdened source. This protection should not apply to deliberate destruction after a duty to preserve has arisen or to strategic non-retention intended to frustrate a lawful requirement.

7. Transparency and accountability

CryptoUK does not support the removal of the statutory annual reporting requirement for Financial Institution Notices and asks that it be reinstated. A non-statutory intention to publish

information, without a defined format or binding commitment, is not a proportionate substitute as the power is extended to a new and potentially broad recipient class.

Annual reporting should distinguish, using confidentiality-protecting aggregation, between recipient types and domestic and international purposes. It should also report approval and rejection outcomes and any reportable security incidents connected with requested or transferred data. This would allow Parliament and affected sectors to assess how the expanded power is being used without disclosing taxpayer information.

Conclusion

HMRC's correspondence and the roundtable discussion have clarified the intended separation between the FIN perimeter and section 114, the application of the FIN definition to tax-software providers and the expectation that HMRC would normally seek information from the taxpayer or an exchange first. Those explanations are useful, but they do not provide the statutory boundaries or safeguards needed for a power of this breadth.

CryptoUK supports targeted powers necessary for genuine compliance checks and international information-exchange obligations. It does not support this extension in its current form. The Government should withdraw or defer the measure unless revised legislation clearly narrows the provider perimeter, establishes a least-intrusive request sequence, excludes controlling credentials, protects high-risk linked data and retains meaningful approval and transparency safeguards.

CryptoUK would welcome further discussion on how these safeguards can be reflected without preventing HMRC from obtaining information which is genuinely required for a compliance check or information-exchange obligation.

Yours faithfully

CryptoUK