



Modernising Payment Services Regulation | GBBC Response

About Global Blockchain Business Council (GBBC)

GBBC is the largest leading non-profit association for the blockchain, digital assets, and emerging technologies community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 251 Ambassadors across 119 jurisdictions and disciplines.

GBBC furthers adoption of digital technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chains, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), GBBC Digital Media, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Executive Summary

- The core perimeter, key definitions, statutory payment rights and safeguarding outcomes should remain in legislation. The FCA should set detailed operational requirements and update them as technology develops.
- The scope of existing definitions must be reconsidered for applicability to tokenised payments to mitigate any unintended consequences.
- A blockchain address, self-hosted wallet or software interface should not become a payment account merely because it can transmit a token.
- A single set of payment activities for tokenised and non-tokenised payments is preferable, but technology neutrality should not erase differences in the underlying form of value or control model.
- Stablecoin issuers should not need a second full authorisation for payment services integral to issuance, redemption and transfer. Other payment activities should be added through a streamlined variation using evidence already assessed by the FCA.
- Payment safeguarding, issuer backing-asset safeguarding and cryptoasset custody protect different interests. CASS 15, CASS 16 and CASS 17 should be allocated by function, with common evidence and no duplicate segregation or reconciliation for the same asset or entitlement.
- Recognition of overseas stablecoin regimes should be transparent, outcomes-based and capable of operating at regime or issuer level. Transitional recognition is needed to avoid disrupting established cross-border use cases.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Questions Addressed

This response addresses Questions 1–20 and 42. GBBC does not offer positions on the remaining questions.

Question 1

Which requirements should remain in legislation, and which should be delegated to the FCA? Please explain your reasoning.

The perimeter and the principal rights and protections should remain in legislation. Detailed and technical requirements should be delegated to the FCA.

Legislation should continue to define regulated payment activities, exclusions, the persons subject to the regime and the territorial scope. Legislation should retain the definitions on which the perimeter depends, including payment account, payment transaction, payment instrument, payment order and the forms of value capable of being used in a regulated payment service and add additional or amended definitions to accommodate tokenised payments.

Core rights and obligations should retain a statutory basis. These include the right to redeem relevant forms of regulated value, the basic allocation of liability for unauthorised or incorrectly executed transactions, the required safeguarding outcome, and the circumstances in which customer assets are protected on insolvency.

The FCA should set operational detail, including reconciliation frequency, record-keeping, reporting, authentication standards, prudential calculations, outsourcing controls and the technical application of conduct rules. This division provides certainty at the perimeter while allowing the FCA to respond to risks, new business models and innovation.

Both the legislation and the technical requirements must ensure that there is no overlap in requirements between the Payment Services regime and the Crypto Assets regime.

Question 2

Where you consider requirements should remain in legislation, are there any updates you believe need to be made to these requirements?

The legislation should be updated to ensure that tokenised payment activities are appropriately brought into scope.

- Introduce definitions that allow specified tokenised assets to be used in payment services without redefining every stablecoin as funds.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

- Clarify when a custodial wallet is a payment account and when a wallet provider is an account-servicing payment service provider.
- Extend payment transaction, payment instrument and payment order concepts to appropriate cryptographic credentials, APIs and smart-contract mandates.
- Create express exclusions for self-hosted wallet software and genuinely technical infrastructure where the provider does not contract to provide a payment service and does not control customer payment value.
- Allocate the statutory safeguarding outcome among payment service providers, stablecoin issuers and cryptoasset custodians.
- Provide coordinated commencement and transitional provisions so an activity is not simultaneously regulated twice or unintentionally left outside both the payments and cryptoasset regimes.

Question 3

Do current provisions relating to the regulatory framework for payment services and electronic money, such as key definitions, need to be updated? If so, please explain how.

The definitions were designed primarily for cash, bank-account money and electronic money. They do not provide a predictable perimeter for stablecoin wallets or on-chain payments.

The definition of funds does not clearly include a qualifying stablecoin. Simply adding stablecoins to that definition would imply that they share the legal characteristics of deposits or electronic money and could bring unintentional consequences.

GBBC suggests retaining funds and cash and introducing payment value as a limited umbrella term. Payment value would comprise funds and a permitted tokenised payment asset where received, held or transferred in providing a payment service. A permitted tokenised payment asset should initially cover tokenised deposits, UK-issued qualifying stablecoins and stablecoins issued under a recognised overseas regime.

A custodial wallet should qualify as a payment account only where a payment service provider maintains a relationship with an identifiable user, controls or shares control of access and enables the execution of payment transactions. The existence of a blockchain address should not be determinative.

The EBA's June 2025 Opinion on the interplay between PSD2 and MiCA provides a useful functional analogy. It treats a custodial wallet as a payment account where it enables the user to send and receive e-money tokens directly to and from third parties. The UK should use that functional test, but should keep the definition of 'funds' as currently drafted. A qualifying UK stablecoin should enter the



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

payments perimeter because of the regulated service being provided, not because its legal nature is recharacterised. (EBA/Op/2025/08, paragraph 23).

Given the complexity of determining new definitions, we suggest HMT run a specific workshop with relevant stakeholders on this topic.

Question 4

Which international regulatory developments, for example recent reforms in the EU, should the UK incorporate into an updated framework for payment services and electronic money?

The UK should pursue interoperability and equivalent regulatory outcomes, while avoiding the duplication that can arise where cryptoasset and payment regimes are layered without a clear activity boundary.

The EU experience under MiCA and the developing Payment Services Regulation and PSD3 framework demonstrates the importance of coordinating the legal status of a stablecoin with the regulation of services used to transfer it. The UK should preserve compatibility with SEPA requirements where relevant, but should not import definitions that assume all payment value has the same legal form.

The EBA Opinion is helpful because it identifies the practical consequences of overlap across scope, authorisation, capital, conduct, strong customer authentication and safeguarding.

It is important to note that because the interplay between payment services and MiCA was not addressed at the outset, the EBA had to use temporary supervisory forbearance. HMT should settle the UK perimeter, activity, permission, and safeguarding consequences before commencement.

Recognition of overseas stablecoin regimes should assess outcomes rather than require identical rules. HMT should, together with the FCA, publish the criteria, evidence requirements, decision timetable and treatment of applications pending determination. Recognition should be possible at regime level or, where justified, for a class of issuers or an individual issuer.

Question 5

Does the current regulatory framework need to adapt to unlock the opportunities arising from the use of tokenised deposits in retail payments?

Payment regulation should apply consistently to the payment function while preserving the legal characteristics of the underlying deposit claim.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Tokenised deposits should remain deposits for prudential, depositor-protection and insolvency purposes. Their use on distributed-ledger infrastructure should not create an additional payment category merely because the record or transfer mechanism is tokenised.

The framework should ensure comparable access to payment infrastructure, clear settlement finality and interoperability among tokenised deposits, conventional bank money, electronic money and regulated stablecoins. It should also address transfers between different banks' tokenised deposit arrangements and the conversion of tokenised balances into conventional account money at par.

It should be clarified that the use of technology service providers by banks does not change the nature of the liability and thus does not preclude banks from outsourcing arrangements.

Technology-neutral treatment must not create institutional bias. Equivalent payment activities should attract equivalent conduct outcomes, but differences in the issuer, claim, backing, deposit protection and failure treatment should remain visible to users.

Question 6

Do you agree that only stablecoins issued in the UK or from a 'recognised jurisdiction' should be treated as 'money-like' for the purposes of payments, and brought into the UK payments perimeter?

GBBC agrees with a controlled gateway, subject to a workable recognition process and appropriate treatment of established cross-border stablecoins. It is important to note that cross-border settlement and treasury use cases run on globally liquid stablecoins and a domestic-only payments category would push that activity offshore or possibly back into the cryptoasset regime.

A payment stablecoin should meet credible standards for backing, redemption, governance, safeguarding and supervision to support payment service protections. UK issuance under article 9M provides one route. Recognition of an overseas regime can provide another.

Recognition should be transparent, proportionate and outcomes-based. HMT should allow regime-level recognition and, where appropriate, recognition of a defined class of issuers or an individual issuer subject to supervisory cooperation and consider a transitional regime for existing UK activity whilst recognition is assessed.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Question 7

Should firms authorised to issue 'UK-issued qualifying stablecoins' be allowed to provide payment services without additional permissions, but be subject to relevant requirements?

Yes for payment services integral to issuance, redemption and transfer, but not as an automatic permission for every payment activity.

A second full authorisation process would add cost without improving outcomes where the FCA has already assessed the issuer's governance, systems, controls, financial resources and stablecoin arrangements. The issuer should be able to perform the payment functions necessary to issue, redeem and transfer its own stablecoin, subject to the applicable payment conduct requirements.

Broader activities such as merchant acquiring, money remittance or operating payment accounts for multiple forms of value may create additional risks. These activities should be added through a streamlined variation of permission rather than deemed automatically permitted.

The FCA should reuse evidence from the cryptoasset authorisation and operate a coordinated assessment. The activity boundary and evidence requirements should be published before firms finalise their applications under the cryptoasset regime.

The EBA opined on a similar approach: payment conduct and security protections can be applied or cross-referred within the cryptoasset framework without requiring a second authorisation for the same service. For the UK, the legislation should identify the payment activities included within an issuer's or cryptoasset firm's permission and use a variation of permission where additional payment services are introduced.

Question 8

Do you agree that safeguarding of UK-issued qualifying stablecoins, where that is within new article 9M RAO, for the purposes of payments should eventually be regulated under the payments regime and not the cryptoassets regime?

GBBC supports removing duplicate safeguarding, but does not support moving token custody wholesale from CASS 17 into CASS 15. The governing regime should follow the protected asset or entitlement and preserve equivalent outcomes.

Three protections need to be distinguished. CASS 16 protects the assets backing the issuer's stablecoin. CASS 17 protects a customer's cryptoasset and the means by which a custodian holds or controls it. CASS 15 protects relevant funds held in the course of providing payment services. A single transaction may involve all three, but each protects a different asset or entitlement.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Pure custody, including control of a holder's stablecoin or means of access, should remain subject to CASS 17 unless legislation expressly transfers that protection without reducing it. CASS 15 should govern relevant funds and other payment value held in payment execution only to the extent that the same asset or entitlement is not already protected under CASS 16 or CASS 17. Payment conduct and liability rules may still apply to the service even where CASS 17 remains the governing custody regime.

The EBA also draws a conceptual distinction between payment safeguarding and cryptoasset safekeeping. It recommends that MiCA Article 70 govern e-money tokens and their means of access, and that PSD2 safeguarding should not be duplicated for those assets (EBA/Op/2025/08, paragraphs 48-50 and 115-121). The UK outcome should be to designate one primary CASS regime for each protected interest and permit reliance on equivalent controls.

We request HMT and the FCA to publish an end-to-end matrix allocating the regime, responsible entity, reconciliation duty and failure treatment across issuer, custodian, wallet provider, payment service provider and infrastructure operator.

Question 9

Do you agree with the proposed broad split of regulated activities for payments and electronic money issuance?

We see a need for a revised set of definitions and worked examples for stablecoin services.

The proposed activity split can accommodate tokenised payments, but Table 1 continues to rely on cash, funds, payment accounts and payment instruments. Clarity is needed on how a wallet-to-wallet stablecoin transfer maps to operating an account, executing a transaction or money remittance, or when a wallet credential is a payment instrument.

Stablecoin issuance should, as provided for in the Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026, remain distinct from issuing electronic money. The legislation should also ensure a clear distinction between issuing the asset, safeguarding it, operating a customer payment account and providing the infrastructure that validates or records a transfer.

The publication of worked examples for custodial wallets, self-hosted wallets, merchant acceptance, remittance, omnibus custody, smart-contract payments, fiat on- and off-ramps and infrastructure-only services would be an invaluable resource for the industry.

The EBA's mapping offers useful worked analogies. A transfer of a regulated stablecoin carried out by a provider on behalf of a client is analogous to execution of a payment transaction. A custodial wallet that allows direct transfers to and from third parties may be analogous to operating a payment account. By contrast, exchange of cryptoassets for funds or for other cryptoassets, and



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

intermediation of a cryptoasset purchase using a stablecoin, should not be treated as payment services merely because a stablecoin is used. (EBA/Op/2025/08, paragraphs 23, 27 and 66-70.)

The EU treatment also exposes an issue the UK should resolve expressly. Because an e-money token is deemed to be 'funds', the EBA considers a transfer between two wallets of the same holder to be a payment transaction. HMT should not allow that outcome to arise by implication. Legislation should state if stablecoins are to be treated as 'funds' and address the consequences that flow from such inclusion.

Question 10

Do you agree with the proposal to have a single set of regulated payments activities for both tokenised and non-tokenised payments? Are there any risks associated with combining activities in this way? If so, should these risks be mitigated by framing regulated payment services activities differently?

A single functional framework is preferable, but technology neutrality should not erase differences in the underlying form of value or control model.

The same payment activity should produce comparable conduct, transparency and liability outcomes whether it uses a bank deposit, electronic money, tokenised deposit or qualifying stablecoin. Separate activity lists would create artificial distinctions and encourage perimeter arbitrage.

However, risks arise from a single set of activities built on definitions designed only for conventional funds. Stablecoins may involve token custody, public ledgers, irreversible execution, third-party smart contracts and de-pegging risk. These features should be addressed through revised definitions, conduct rules and proportionate permissions rather than separate payment activities.

Question 11

Do you agree that authorised and registered firms should require a variation of permission to carry out payment services using tokenised payments?

A proportionate change process is appropriate, but a full variation should not be required where the firm's existing permission and controls already address the material risks.

The FCA needs visibility of the tokenised assets, custody arrangements, ledgers and third parties used by a firm. That does not justify repeating an authorisation assessment where the regulated activity and customer risk are substantially unchanged.

GBBC recommends a tiered process. A notification should be sufficient for low-risk changes within an existing permission. A streamlined variation should apply where token custody, settlement or



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

operational dependencies create additional risks. A fuller assessment should be reserved for firms adding a materially different regulated activity.

Evidence already provided under the payments, cryptoasset or banking framework should be reusable. The FCA should publish service standards and coordinate the timing with the cryptoasset authorisation process.

Question 12

How does the payment services regulatory framework need to adapt to support the use of smart contracts and programmable payments underpinning them?

The framework should regulate the payment service and the party exercising control, not smart contract code as a technology.

A programmable payment may be initiated automatically when a coded condition is met. The rules should identify who authorised the mandate, what conditions and limits apply, when authority may be revoked and which regulated provider is responsible for execution.

Liability should follow contractual responsibility and practical control. The framework should address coding errors, oracle failure, unauthorised changes, duplicated execution, failure to execute and transactions that cannot be reversed on the underlying ledger. A PSP should remain accountable where it selects, operates or materially controls the smart contract used to provide the service.

Retail users should receive clear information about conditions, fees, finality and available remedies. Sophisticated parties should be able to agree tailored arrangements for wholesale transactions where this does not remove protections owed to third parties.

Question 13

Are the current conduct of business requirements in the payment services regulatory framework suitable for tokenised payments? Please explain your answer.

Current requirements provide a useful baseline but require targeted adaptation for tokenised value and on-chain execution.

- Disclosures should identify the legal nature of the payment value, issuer, redemption right, relevant safeguarding regime and any de-pegging or network risk.
- Execution information should distinguish initiation, ledger confirmation, settlement finality and any subsequent redemption or conversion into conventional funds.
- Liability rules should address loss of credentials, compromised smart contracts, chain reorganisations, forks and failures by outsourced wallet or infrastructure providers.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

- Refund and error resolution rules should recognise that an on-chain transfer may be technically irreversible while preserving the provider's obligation to compensate or recover value where liability rests with it.
- The Consumer Duty, payment conduct rules and cryptoasset disclosures should be coordinated so the same service is not subject to inconsistent or repetitive communications. The EBA Opinion identifies practical adaptations that the FCA should consider: permit an estimate where network fees or maximum execution time cannot be known in advance; determine whether a public key or other ledger credential is the relevant unique identifier; apply strong customer authentication (see response to Q42 below) to remote access to custodial payment wallets and initiation of token transfers; and specify liability and fraud-reporting rules for unauthorised, non-executed, defective or late transactions (EBA/Op/2025/08, paragraphs 41-47).

Question 14

Are the current prudential requirements in the payment services regulatory framework suitable for tokenised payments? Please explain your answer.

The principal concern is the interaction between payment service prudential requirements, COREPRU and CRYPTOPRU. COREPRU provides common prudential standards, CRYPTOPRU introduces requirements specific to regulated cryptoasset activities and COREPRU 4.1.3G expressly envisages payment institutions and electronic money institutions meeting their PSR and EMR capital requirements separately and additionally. For firms operating across both regimes this creates a risk of cumulative requirements.

Under the PSRs, authorised payment institutions generally hold the higher of initial capital and an ongoing requirement calculated using one of 3 methods, based on overheads, payment volumes or income. COREPRU uses a different calculation method based on fixed overheads and K-factors and has explicit liquidity and risk assessment requirements.

The interaction between these requirements must be considered, overlapping obligations identified and their cumulative application justified. A simple application of separate prudential regimes results in unnecessary financial burden for firms.

For systemic stablecoin payments, we welcome the proposed allocation of responsibilities between the Bank of England and the FCA together with the transition arrangements in the Bank of England and Financial Conduct Authority's approach to joint regulation of systemic stablecoin issuers. Moving forward, clarity is needed on how the approach will extend to systemic issuers also providing payment services. The Bank of England and FCA have committed to avoiding duplication in capital, liquidity and resolution requirements. A mapping is necessary to identify which of the different



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

prudential requirements will apply and avoid duplicate capital for the same risk within the same entity.

Question 15

How does existing payment services regulation need to adapt to support agentic payments? For example, do provisions relating to authentication and consent of payments transactions, and liability for unauthorised payment transactions, need updating?

The framework should recognise verifiable delegated mandates and allocate responsibility where an agent acts outside authority or selects the payment asset and rail.

Consent should be capable of covering a defined mandate rather than requiring a fresh instruction for every transaction. The mandate should state the permitted purpose, transaction and aggregate limits, duration, counterparties or merchant categories, available forms of payment value and conditions for revocation.

The regulated provider should maintain evidence of the mandate, the agent's decision and the transaction instruction. Customers should be able to pause or revoke authority and should receive intelligible records of the payment and the basis on which it was made.

Liability should be determined by whether the transaction was within the mandate, whether the provider applied required controls and whether an agent or model failure was reasonably detectable. Standards should work across bank accounts, electronic money, tokenised deposits and regulated stablecoin wallets.

Question 16

Are there any other innovations across the payments landscape that the Government should take into account when reforming its payment services regulatory framework?

The framework should anticipate multi-asset wallets, machine-to-machine payments, privacy-enhancing technologies and the convergence of payment and settlement infrastructure.

A customer interface may hold or route bank money, electronic money, tokenised deposits and stablecoins. Regulation should allow the service to select or convert payment value under a transparent mandate while ensuring that the user understands the asset, fees and protections that apply.

Machine-to-machine and embedded payments may involve high transaction volumes and low individual values. The framework should support automated limits, credentials and audit trails without assuming a conventional screen-based customer journey.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Digital identity, verifiable credentials and privacy-enhancing proofs may improve authentication and financial-crime controls. Rules should permit their use where firms can evidence reliability, data minimisation, auditability and appropriate customer recourse.

Question 17

How can the Government ensure these reforms support an inclusive payments landscape?

Tokenised payment services should be designed for accessibility and convertibility, while cash and conventional payment options remain available.

Stablecoins may reduce costs in cross-border payments and enable new services, but wallets can create barriers through smartphone dependence, digital identity requirements, unfamiliar fees and key management. Firms should provide accessible onboarding, authentication, support and recovery arrangements proportionate to the customer group.

Customers should receive clear information about how to convert tokenised value into bank money or cash, the time and cost involved and the effect of issuer or intermediary failure. HMT should measure effective access and use rather than the number of payment methods technically available.

Innovation policy should preserve cash and conventional account-based payments as inclusion and resilience options.

Question 18

What are the key risks which have emerged to consumers and businesses in the payments and electronic money sector over recent years, and how well do the current regulations address this?

The main risks for adoption of tokenised payments are fragmented responsibility across firms and regulatory regimes, fragmented safeguarding allocation, operational dependency and financial crime across multiple firms.

- Unclear responsibility where the issuer, custodian, wallet provider, payment service provider and infrastructure operator are different entities.
- Loss, compromise or misuse of cryptographic credentials and failures in wallet or smart-contract controls.
- Reconciliation gaps between customer records, omnibus custody records, on-chain positions and issuer liabilities.
- De-pegging, delayed redemption and liquidity stress, particularly where customers treat a stablecoin as money-like.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

- Concentration in cloud, custody, bridge, oracle and ledger infrastructure providers.
- Fraud, sanctions evasion and money laundering involving rapid movement across assets, ledgers and jurisdictions.
- Regulatory gaps or duplication where a single payment combines conventional funds, electronic money, tokenised deposits or stablecoins with different firms responsible for conversion, custody, transfer, redemption/payout.

Question 19

Would enhanced accountability of senior managers in the payment services and electronic money sector support better management of financial crime risks? What benefits, costs or risks, including to the UK's international competitiveness, should the Government consider?

Clear senior accountability can improve outcomes, but payments and cryptoasset activities within the same legal entity should operate under one responsibility map.

Cryptoasset firms will be subject to the FCA's Senior Managers and Certification Regime and financial crime requirements. A separate payments layer should not duplicate prescribed responsibilities, fitness and propriety assessments or governance maps.

Responsibility should encompass the end-to-end payment chain, including outsourced wallet, custody and transaction-monitoring arrangements. Firms should be able to evidence shared or allocated responsibilities where more than one regulated entity participates.

Duplicative regimes would raise entry and operating costs without necessarily improving control. International competitiveness is better supported by clear accountability, common evidence and coordinated supervision.

Question 20

Are there targeted amendments that could be made to current regulation which would tackle sector risks in a proportionate way?

Targeted perimeter, safeguarding and information-sharing amendments would address the principal risks more effectively than creating new overlapping activity categories.

- The definitions and applicability to tokenised payments require careful consideration to mitigate any unintended consequences.
- There is also a need for a mapping exercise for payment services with tokenised money to the existing regulated activities in Annex 1.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

- Determine the perimeter between CASS 15, CASS 16 and CASS 17 to ensure that there are no overlaps or gaps.
- Enable proportionate information sharing among issuers, custodians, PSPs and relevant infrastructure providers for fraud, sanctions and transaction monitoring.
- Require incident notification where loss of keys, smart-contract failure or ledger disruption materially affects execution or access to customer payment value.
- Coordinate commencement and grandfathering across payments and cryptoasset permissions.

For the first 3 points above, we suggest that HMT run specific workshops with all relevant stakeholders to determine the optimal definitions, the perimeter between the CASS regimes and the scope of regulated activities in Annex 1.

Question 42

Are there any other areas of feedback on issues raised in this consultation?

We welcome the proposed allocation of responsibilities between the Bank of England and the FCA together with the transition arrangements in the Bank of England and Financial Conduct Authority's approach to joint regulation of systemic stablecoin issuers.

CASS 15 is already in force for payment and e-money relevant funds. The FCA has finalised much of the cryptoasset framework, including CASS 16 for qualifying stablecoin backing assets and CASS 17 for client cryptoassets. The payments perimeter and tokenised payment permissions remain under development. Firms should not be required to build an interim authorisation and safeguarding model that must be replaced shortly afterwards.

The Bank of England and FCA joint approach of 30 June 2026 improves coordination for systemic issuers, but it is focused principally on issuance. The payment chain may also include wallets, custodians, PSPs, payment-system operators and infrastructure providers. The FCA will determine later which rules are disapplied when a firm becomes systemically regulated, and the Bank's Code of Practice remains in draft at the time of this response.

Before the payments regime commences, the FCA and the Bank should publish a consolidated allocation covering issuance, backing assets, custody, wallets, payment execution, infrastructure, redemption and failure and identify the lead authority, applicable safeguarding regime, evidence that may be reused and rules that will be disapplied.

The final framework should clarify how authentication and payee verification apply to tokenised payments.



THE TRUSTED RESOURCE: PEOPLE, EDUCATION, ACCESS

Where a firm controls a customer's wallet and executes a payment, it can authenticate the customer before releasing the transaction. Firms already govern on-chain transactions through a policy layer (per-transaction limits, multi-party approval, permitted counterparties and contracts, pre-execution checks, immutable logs). The rules should let a firm demonstrate consent and authentication through that layer rather than prescribe an authentication method that assumes a person at a screen.

FCA rules should permit suitable consent and authentication.

A genuinely self-hosted wallet has no provider able to impose SCA on the transfer and should be out of scope.

This approach aligns with the outcomes-based authentication rules envisaged in paragraph 2.8, supported by clear legislative boundaries for regulated wallet and payment activities.