

6 October 2026

By email: Modernisingpaymentservices@hmtreasury.gov.uk
Payments and Fintech Team
HM Treasury
1 Horse Guards Road
London SW1A 2HQ

Re: Modernising Payment Services Regulation

To whom it may concern,

CCI and GDF welcome the opportunity to respond to HM Treasury's consultation on modernising payment services regulation. We have focused on the areas of greatest relevance to our members, in particular the treatment of tokenised payments, and so have not sought to answer every question.

About CCI and GDF

Crypto Council for Innovation ('CCI') and Global Digital Finance ('GDF') are the two leading global members' associations representing firms delivering crypto and digital assets solutions. Our members span the digital asset ecosystem and include the leading global crypto exchanges, stablecoin issuers, digital asset Financial Market Infrastructure providers, innovators, and investors operating in the global financial services sector.

Together, our members share the goal of encouraging the responsible global regulation of crypto and digital assets to unlock economic potential, improve lives, foster financial inclusion, protect security, and disrupt illicit activity.

We believe that achieving these goals requires informed, evidence-based policy decisions realised through collaborative engagement between regulators and industry. It also requires recognition of the transformative potential of crypto and digital assets, as well as new technologies, in improving and empowering the lives of global consumers.

We support and encourage a comprehensive UK digital asset regulatory approach which is robust, proportionate, and pro innovation. Appropriate regulatory guardrails are crucial to ensure the continued growth of the UK ecosystem, to further attract the predominantly global industry, and to realising the goal of making the UK a digital finance hub.

As always, we remain at your disposal for any further questions or clarifications you may have, and we would welcome a meeting with you to further discuss these matters in more detail with our members.

Yours faithfully,

Laura Navaratnam – UK Policy Lead, CCI

Adriana Ennab – Head of Global Policy & Regulation, GDF

Chapter 2: Approach to updating existing regulatory requirements

Question 1: Which requirements should remain in legislation, and which should be delegated to the FCA?

We support delegating detailed, firm-facing and technical requirements to the FCA, and agree with the government's reasoning on Strong Customer Authentication in particular.

Requirements of that kind need to change as technology and fraud typologies change, and the FCA is better placed than the legislative timetable to make those changes.

We believe the following should remain in legislation.

- **The perimeter and its boundaries.** We agree with the government's intention to retain the perimeter and key definitions in legislation. For tokenised payments, we would extend that to the boundary between the payments perimeter and the cryptoasset perimeter, including the intermediary carve-outs described at paragraphs 3.14 and 3.15 and the safeguarding allocation described at paragraph 3.17. A firm decides which permissions to apply for, what to build, and whether to serve UK users, on the basis of that boundary. If there is uncertainty, firms will likely instead default to restricting UK access altogether.
- **The definitional gateway for tokenised payments.** Whether a qualifying stablecoin or a tokenised deposit constitutes "funds", and whether a wallet constitutes a "payment account", determine whether the regime applies at all. We address these at Question 3.
- **Rights and liability allocation.** We agree with the government's position on framework contract termination notice periods, and would apply the same logic to the core

liability provisions for unauthorised and incorrectly executed transactions. These allocate loss between parties and are relied on by users and firms in contract.

Where requirements are delegated, we believe three things could assist:

- We would encourage HM Treasury to ask the FCA to consult on carrying the existing requirements in the PSRs and EMRs across in substance as a first step, and to consult separately on any substantive change it wishes to make. The transfer of responsibility and any change to the requirement itself would then be considered on their own merits, and the FCA could take the substantive questions at a point when the cryptoasset regime has bedded in rather than during the same period.
- Firms will find it difficult to assess the consequences of delegation tranche by tranche without knowing what else is moving. CCI and GDF would encourage the FCA to publish, at the point the legislation is made, an indicative list of the provisions it expects to transfer and the order in which it intends to consult on them.
- Handbook rules can be changed more quickly than legislation, which is much of the reason for delegating them. Firms making multi-year investment decisions in payments infrastructure need some visibility on the pace at which requirements will change. We would encourage HM Treasury to ask the FCA to commit to a minimum implementation period for changes to requirements transferred from the PSRs and EMRs, except where consumer harm requires faster action.

Question 3: Do current provisions relating to the regulatory framework, such as key definitions, need to be updated?

We believe there are five definitions which warrant updating.

“Funds”. Regulation 2(1) of the PSRs defines funds as banknotes and coins, scriptural money and electronic money. If tokenised payments are to be regulated as payments, the definition needs to include UK-issued qualifying stablecoins, stablecoins issued in recognised overseas jurisdictions, and tokenised deposits explicitly, where used in providing regulated payment services.

“Payment account”. The definition assumes an account held by a payment service provider in the name of a user. Tokenised payments may involve a wallet controlled by the user, a wallet controlled by a firm on the user’s behalf, or an omnibus arrangement. We believe the

framework should be capable of accommodating each of these arrangements, while the definition of “payment account” should make clear that a self-hosted wallet is not itself a payment account and that a transfer to one does not create obligations on the sender’s provider in respect of a receiving provider that does not exist.

The boundary between electronic money and qualifying stablecoin. A UK-issued qualifying stablecoin may satisfy the existing definition of electronic money in regulation 2(1) of the EMRs, being electronically stored monetary value, representing a claim on the issuer, issued on receipt of funds, and accepted by persons other than the issuer. The relationship between article 9M of the RAO and the EMRs should be resolved in legislation so that an issuer is not required to hold both permissions, and so that a firm can determine which regime applies to a given instrument without a perimeter opinion.

“Money-like instruments”. The term is used in this consultation and has been used by the FCA, including in CP25/14, without a statutory or regulatory definition. As CCI and GDF said in our joint response to that consultation, it would be useful to have a clear definition of ‘money-like instruments’ and some guidance as to what would or would not constitute such an instrument. The term now carries consequences for perimeter treatment, and should be defined accordingly.

Execution and receipt. The definitions of execution, receipt and the point of irrevocability were drafted for transfers between accounts held with payment service providers. For an on-chain transfer, the relevant points are broadcast, inclusion and finality, which do not map onto the existing terms. We address the consequences at Questions 12 and 13.

Knock-on effects of definitions. The treatment of qualifying stablecoins as “funds” may have consequences beyond the perimeter itself, including for requirements designed around account-based payments such as strong customer authentication and payee-verification requirements. Similar questions arise for concepts such as “payment transaction” and “payment order”, which may not map cleanly onto blockchain-based payment journeys. CCI and GDF would therefore encourage HM Treasury and the FCA to test the relevant definitions end-to-end against tokenised payment use cases before finalising them, including through targeted industry workshops. This would help identify cascading consequences across conduct, authentication and liability requirements and reduce the risk that technical definitions create unintended operational or perimeter outcomes.

Question 4: Which international regulatory developments should the UK incorporate?

We would encourage the government to align with EU reforms where alignment reduces cross-border friction and supports interoperability, while preserving the coherence and proportionality of the UK framework. Two elements of the EU package merit incorporation.

The first is consolidation of the electronic money regime into the payment services framework. PSD3 and the PSR bring electronic money issuance within a single authorisation and conduct regime and remove the separate electronic money institution category. The UK faces the same question in a sharper form, because a UK-issued qualifying stablecoin may also meet the definition of electronic money, as we set out at Question 3. Consolidating the EMRs into the payments framework would resolve that boundary and remove a permission category that firms increasingly hold alongside others.

The second is the EU's treatment of access to payment systems and to payment accounts held at credit institutions. Payments firms and stablecoin issuers consistently report difficulty obtaining and retaining the banking relationships their authorisation assumes. CCI and GDF would encourage HM Treasury to consider whether the UK framework needs an equivalent right of access, particularly as firms authorised under article 9M will need settlement and reserve accounts from the point of authorisation.

For our combined membership, alignment on stablecoins is a major priority. MiCA is in force, the GENIUS Act has established a federal framework in the United States, and Singapore, Hong Kong, Japan and the UAE have each brought stablecoin issuance within their perimeters. Given the global nature of digital asset markets, divergence from peer jurisdictions risks creating regulatory friction, discouraging cross-border issuance of GBP stablecoins, and undermining the UK's stated ambition to be a world leader in digital finance.

Accordingly, we would encourage the government to prioritise three points of alignment. The criteria and process for recognising an overseas stablecoin regime, which we address at Question 6. The treatment of stablecoins used as settlement assets in wholesale markets, so that a sterling instrument is usable in the same contexts as its peers. And mutual recognition of comparable regimes more generally, to avoid fragmentation of liquidity and to ensure the UK captures, rather than displaces, globally mobile activity.

SEPA. The UK's participation in the SEPA schemes rests on adherence criteria set by the European Payments Council, which take account of the legal framework applying in the participant's jurisdiction, including its alignment with the Payment Services Directive. Moving PSD-derived provisions from the PSRs into the FCA Handbook may therefore engage those criteria even where the substance of the requirement does not change. We would encourage HM Treasury to confirm with the European Payments Council, before the delegation decisions in Chapter 2 are settled, that requirements set in FCA rules rather than in legislation will continue to satisfy them.

Chapter 3: Responding to new developments in payment services

Question 5: Does the current regulatory framework need to adapt to unlock the opportunities arising from the use of tokenised deposits in retail payments?

We support the 'same risk, same regulatory outcome' principle and the treatment of tokenised deposits as deposits. We offer two subsequent points which arise for the payments framework.

Firstly, the framework should be neutral between forms of digital money. Tokenised deposits and qualifying stablecoins are structurally different instruments with different risk profiles, and will be used by different institutions for different purposes. The payments framework should not be designed around a preference for one and should permit a payment chain that involves both, including a conversion between them, without imposing an additional regulated activity or permission solely because the payment involves different forms of tokenised money. Any applicable requirements should follow the economic activity and risks involved.

Secondly, regulatory obligation should be located at the layer where control sits. Where a tokenised deposit is transferred on a shared ledger, the accountable person should be the regulated firm performing the regulated activity, not the network on which the transfer occurs. As we set out in our response to the FCA and Bank of England Call for Input on tokenisation, accountability should attach to the entity performing the regulated activity and should not default to the underlying network, its validators or node operators. Reaching into the infrastructure layer to impose responsibility on an infrastructure participant that does not control the regulated service is impractical, unenforceable, and risks constraining the

infrastructure while failing to capture the layer where control of regulated services genuinely lies.

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?

We support the principle that money-like treatment should follow issuance standards, and consider that a stablecoin issued under article 9M meets those standards. Our comments relate specifically to the sequencing and the practical reach of the proposal. Our support is conditional on a transparent, outcomes-based recognition mechanism being operational when the revised payments perimeter takes effect. The framework should also permit recognition of an individual stablecoin or defined regulatory class where jurisdiction-wide recognition would be unnecessarily broad or impracticable.

Reach of the proposal. The GBP-denominated stablecoin market remains relatively nascent and is currently negligible when compared to global stablecoin activity. In practice, it is highly unlikely that firms operating in the UK will engage solely with UK-issued qualifying stablecoins. Instead, most firms will continue to interact with non-UK-issued stablecoins such as USD-denominated stablecoins, whether for liquidity, settlement, or cross-border payment use cases. Cross-border payments are the clearest current application of stablecoins in payments, and are the application in which non-UK instruments will remain predominant for the foreseeable future. A payments perimeter that reaches only UK-issued instruments will therefore not apply to most stablecoin payment activity affecting UK users.

Consumer protection. A payment made in an overseas-issued stablecoin may instead fall within the cryptoasset dealing or arranging perimeter, where those activities apply, rather than within the payments framework (paragraph 3.12). The conduct protections in the payments framework, including information requirements, execution obligations and the unauthorised transaction provisions, would not apply. Where the intermediary activities do not apply either, the transaction attracts neither the payments-specific protections nor the protections attached to regulated cryptoasset intermediation.

Timing of the recognition mechanism. We welcome the government’s indication that money-like treatment may be extended to stablecoins issued from a recognised jurisdiction. We believe the value of that mechanism depends on when it arrives. CCI and GDF would encourage HM Treasury to publish the criteria for recognition, an indicative assessment

timetable, and an indication of the jurisdictions under consideration, so that the mechanism is capable of operating from the point at which the payments perimeter changes rather than at an unspecified later date.

We recognise the concern that extending money-like treatment beyond UK-issued stablecoins could reduce incentives for firms to issue domestically. In practice, the development of a robust UK stablecoin market is likely to depend on the broader adoption and integration of stablecoin-based payments infrastructure. Enabling firms to operate efficiently across globally dominant stablecoins in the near term may therefore support, rather than undermine, the conditions necessary for UK-issued stablecoins to scale over time.

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. A firm authorised under article 9M will have been assessed by the FCA on governance, systems and controls, prudential resources, safeguarding of backing assets and operational resilience. Requiring a second authorisation to move the instrument it has just been authorised to issue would add process without adding supervisory information.

We agree that such firms should be subject to the relevant conduct requirements of the payments framework in respect of the payment services they provide, and to FCA rules on the same basis as other providers. We would suggest that the FCA be able to require notification of the payment services a 9M issuer intends to provide, so that supervision is informed without a separate authorisation gate.

We would ask the government to consider the corresponding point in the other direction. Once the new payments framework takes effect, an authorised payment institution or electronic money institution should be able to provide payment services in UK-issued qualifying stablecoin under its existing permissions, subject only to any proportionate notification, supervisory engagement or variation requirement applicable in accordance with the approach discussed at Question 11. It should not require an additional cryptoasset permission for the same activity, including an article 9N safeguarding permission where the payments safeguarding regime applies. Reciprocal treatment between the two regimes is required to remove duplication.

Question 8: Do you agree that safeguarding of UK-issued qualifying stablecoins for the purposes of payments should eventually be regulated under the payments regime and not the cryptoassets regime?

Yes. Requiring a firm to hold both payments and cryptoasset safeguarding permissions in order to provide a single payment service would be duplicative, and we welcome the government's conclusion. We offer four related considerations below.

Interim safeguarding requirement. The government notes that consultation responses indicated the residual safeguarding requirement would in practice represent a material barrier to facilitating stablecoin payments in the interim. That remains our members' assessment. The interim period will cover the first phase of the cryptoasset regime, during which firms will be deciding which permissions to apply for and whether to launch stablecoin payment products in the UK. CCI and GDF would encourage HM Treasury to confirm its approach to the interim safeguarding requirement urgently, before firms materially progress or finalise their cryptoasset applications, and to remove the requirement for firms safeguarding UK-issued qualifying stablecoin in the course of providing payment services, or to provide a transitional modification with the same effect.

Drafting the rules for on-chain assets. Segregation, reconciliation and record-keeping requirements designed for fiat client money do not translate directly. Omnibus wallet structures, real-time reconciliation and attribution in the absence of complete Travel Rule data present operational challenges that we set out in detail in our joint response to FCA CP25/14. A principles-based approach that accommodates omnibus and segregated models, allows risk-tiered reconciliations, and leverages blockchain transparency would meet regulatory outcomes without creating unnecessary operational friction.

Equivalent safeguarding outcomes. The same stablecoin may be held by a payment institution under the payments regime and by a custodian under the cryptoasset regime. Customers should receive equivalent core protections against loss, misuse and firm insolvency, irrespective of the applicable permission. However, this does not require identical rules. The detailed requirements should reflect the distinct legal, operational and insolvency characteristics of payment safeguarding and cryptoasset custody, including differences in segregation, wallet structures, key control, reconciliation and asset return.

Multiple-permission firms. The framework should also address firms that combine stablecoin issuance, dealing or arranging and payment services within the same business model. The

same stablecoin or customer asset should not become subject to overlapping safeguarding requirements merely because the firm holds multiple permissions. HM Treasury and the FCA should set out clearly which safeguarding regime applies to each activity and how the regimes interact, including where one set of requirements disapplies or takes precedence, so that duplication or double-counting is avoided while equivalent customer protection is preserved.

Question 9: Do you agree with the proposed broad split of regulated activities for payments and electronic money issuance?

Yes. Merging the cash placement and withdrawal activities, merging the credit line and non-credit line execution activities, and separating issuing from acquiring each reflect how firms are organised in practice.

We would ask that the legislation be accompanied by a published mapping from existing permissions to the new activities, and that firms holding a permission that maps cleanly onto a new activity be transitioned without a fresh application. Firms will be managing the cryptoasset authorisation gateway and any variation of permission process at the same time.

Question 10: Do you agree with the proposal to have a single set of regulated payments activities for both tokenised and non-tokenised payments?

Yes. This will reduce friction for our members, and it is consistent with the technology-neutral approach the authorities have taken elsewhere. It also reflects how firms actually operate. Many firms providing stablecoin payment services also provide, or rely on, fiat payment services, and mixed models are already the norm rather than the exception.

The risk to manage is that a single activity delivers little if the requirements beneath it are drafted for fiat. Several existing conduct and prudential provisions assume a fiat leg, an identifiable payment service provider on each side of a transaction, and a reversible transfer. We set out the specific provisions at Questions 12 to 14. We would encourage the government to ask the FCA to review the requirements attaching to each new activity for technology neutrality as part of the Handbook work, rather than after firms have begun to apply them.

We do not consider that framing the activities differently would mitigate this. Splitting tokenised and non-tokenised activities would reintroduce the dual-permission problem the reforms are designed to remove, and would require firms operating mixed models to hold two permissions for a single customer journey.

Question 11: Do you agree that authorised and registered firms should require a variation of permission to carry out payment services using tokenised payments?

We understand the rationale; however, we do not consider that a variation of permission should be required solely because an existing payment service is provided using tokenised money. The appropriate regulatory response should depend on whether the proposed service materially changes the firm's regulated activities or risk profile. Where it does, we agree that the FCA may need to assess the firm's readiness through a targeted variation process. Where the firm's existing permissions and controls already address the relevant risks, notification or supervisory engagement should be sufficient.

Two considerations support that distinction. A firm that executes a payment in a UK-issued qualifying stablecoin it neither holds nor safeguards presents a different risk profile from one running its own wallet infrastructure, and a uniform requirement applies the same gate to both. A uniform requirement would also operate in practice as the second authorisation that the single set of regulated activities at Question 10 is designed to remove. The Electronic Money Regulations 2011 offer a precedent, separating advance notification of a significant change from an application to vary the requirements attached to an authorisation, and CCI and GDF would encourage HM Treasury and the FCA to consider a comparable approach here.

When a variation is required, it should be a proportionate assessment of the incremental capability required, not an authorisation in substance. A firm that has already been authorised as a payment institution has been assessed on governance, prudential resources, and systems and controls. The incremental questions concern key management, ledger operations, on-chain reconciliation and the safeguarding of tokenised assets. We believe the process should be scoped to those questions, with a published service standard for determination.

On timing, firms are now applying, or preparing to apply, for cryptoasset permissions, and in some cases article 9M permissions, during the same period. We would encourage HM Treasury and the FCA to confirm that a firm may apply for the variation of permission in parallel with its cryptoasset applications rather than sequentially, and that material already assessed under the cryptoasset regime, in particular safeguarding and operational resilience, will not be reassessed from the beginning.

Given the importance of this boundary to firms' authorisation strategies, HM Treasury and the FCA should also publish a clear mapping showing when a variation of permission is required for tokenised payment services, how that requirement interacts with article 9M and other

cryptoasset permissions, and how existing permissions will be recognised. This is particularly important for firms operating integrated business models across issuance, dealing or arranging and payments.

Question 12: How does the payment services regulatory framework need to adapt to support the use of smart contracts and programmable payments?

We offer four areas for further HMT consideration.

Consent and authorisation (regulations 67 and 77). The framework assumes consent given transaction by transaction, or through a mandate lodged with a provider. A programmable payment may involve consent given once, in advance, to a condition that will later be satisfied without further user involvement. We believe the framework should recognise conditional consent given at set-up, with the parameters and limits disclosed at that point, as valid authorisation of the resulting transactions, rather than requiring confirmation at the point of execution.

Revocation (regulation 67(3) to (5)). A user cannot revoke consent to a transfer that has already settled on a ledger. The framework should address what revocation means for a conditional instruction, which we would expect to mean a right to cancel the mandate prospectively rather than to reverse a completed transfer, and should not impose an obligation that the technology cannot deliver.

Liability where the contract executes as coded. The existing allocation of liability distinguishes authorised from unauthorised transactions and correctly from incorrectly executed ones. A smart contract that executes exactly as coded, but not as the user understood, sits outside both. We would encourage the government to consult specifically on where that loss should fall, taking account of who set the parameters, who disclosed them, and who controlled the code.

Where the obligation sits. Programmable payments may involve a firm that sets the conditions, a firm that provides the interface, and infrastructure on which the contract executes. The more durable approach is to locate regulatory obligation at the layer where regulated activity, and the control associated with it, actually resides. We would encourage the government to state that principle in the framework, so that obligations attach to the regulated firm relying on the infrastructure rather than to the infrastructure itself.

Question 13: Are the current conduct of business requirements in the payment services regulatory framework suitable for tokenised payments?

Broadly yes, however we offer the following specific areas where amendments may need to be made.

CCI and support equivalent consumer protection outcomes where comparable risks arise. However, the mechanism through which those outcomes are achieved should reflect the characteristics of tokenised payments, including where control sits, whether a transaction is reversible, and whether there is an identifiable receiving payment service provider.

Information requirements (Part 6). These assume a framework contract and an identifiable provider on both sides of a transaction. Where a transfer is made to a self-hosted wallet, there is no receiving provider. We believe the requirements should be scoped so that a sending provider is not obliged to supply information about a counterparty relationship that does not exist, while retaining disclosure to its own customer.

Unique identifiers (regulation 90). A wallet address functions as the unique identifier, and a transfer to an incorrect address is generally irreversible. The provision should set out what reasonable efforts to recover funds mean in that context, and firms should be able to satisfy it through pre-transfer verification and address validation rather than post-transfer recovery.

Unauthorised transactions (regulations 76 and 77). The refund obligation was designed for transactions initiated through a provider's systems. Where a user holds their own keys, the provider has no ability to prevent or reverse a transfer. We believe the allocation of liability should follow control of the means of authorisation.

Disclosure specific to stablecoins. Clear disclosure of reserve composition, redemption terms, and the distinction between issuer redemption and intermediary conversion is critical. Redemption involves a token being removed by the issuer from circulation and the corresponding backing assets being liquidated, while conversion refers to the exchange of a stablecoin with an intermediary into another form of money.

We would encourage the government to consult separately before extending the authorised push payment reimbursement requirement to tokenised payments so that the mechanism reflects the different fraud patterns, reversibility assumptions and allocation of control, and in some cases the absence of an identifiable receiving payment service provider. The question warrants its own evidence base.

Question 14: Are the current prudential requirements in the payment services regulatory framework suitable for tokenised payments?

The structure is broadly workable, and we do not believe tokenised payments justify a separate prudential regime. However, we believe three areas require clarification.

Own funds calculation. Methods A, B and C in the PSRs are based on overheads, payment volume and income. It is not clear how tokenised payment volumes are to be counted, particularly where a transaction involves a conversion between a stablecoin and fiat, or between two forms of digital money. We would encourage HM Treasury and the FCA to confirm the treatment before firms model their capital requirements.

Interaction with the cryptoasset prudential regime. A firm may hold payment permissions alongside permissions under the new prudential regime for cryptoasset firms. CCI and GDF would encourage HM Treasury and the FCA to calibrate the two frameworks so that a firm does not hold capital twice against the same underlying risk, while capitalising the incremental risks that distinct regulated activities add. Where a firm is subject to payment-services prudential requirements alongside COREPRU or CRYPTOPRU, the interaction between those regimes should be explicit, including how supervisors will assess the combined requirement. We would also encourage them to publish the aggregation or consolidation methodology a dual-permission firm should apply.

Cumulative burden. As we said in our joint response to FCA CP25/40, the cumulative and ongoing compliance burden arising from the current programme of consultations may be understated, particularly for early-stage firms and stablecoin issuers. Greater clarity on how requirements scale by activity and size, and how prudential and conduct obligations interact in practice, would support proportionate implementation and reduce barriers to entry.

More broadly, where a firm is subject to payment-services prudential requirements alongside COREPRU and/or CRYPTOPRU, the interaction between those regimes should be explicit. This is particularly important for integrated business models that combine stablecoin issuance, dealing or arranging and payment services within one legal entity. The final framework should distinguish between genuinely incremental risks and the same risk being captured more than once, and should explain how supervisors will assess the combined prudential requirement.

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?

Existing payment services regulation already recognises consent to a series of payments and distinguishes authentication from authorisation. The next step is to make delegated authority explicit: what a customer has allowed an agent to do, how those limits are enforced, and who pays when something goes wrong.

Consent and authentication requirements should support clear, revocable mandates, with limits on spending, duration and permitted activities. Customers should be able to authorise a bounded task without approving every subsequent payment individually, provided appropriate safeguards are in place. That requires a clear regulatory route, including how strong customer authentication applies when the final amount or payee is not known at the outset. Each payment should be checked against the mandate by the relevant payment or agentic system, with fresh customer approval required to expand the agent's authority. A valid credential alone should not establish that a payment was authorised.

Liability rules should preserve protection against unauthorised payments and clarify responsibility when an agent exceeds its mandate or is compromised. Customers should have a clear route for submitting and resolving reimbursement claims without first having to determine whether responsibility lies with their bank, wallet provider or agent provider. The rules should also distinguish unauthorised payments from poor purchases made within authority, and explicitly address circumstances in which an agent is being deceived by a fraudster.

Chapter 4: Unlocking the future of Open Banking

Question 27: Are there any other adjustments needed to current regulation which would better support Open Banking?

Open Banking and tokenised payment rails will develop alongside each other, and some payment journeys will involve both, for example where a payment is initiated through a payment initiation service and settled in a UK-issued qualifying stablecoin, or where a conversion between fiat and a stablecoin sits within an account-to-account flow. We believe

the settlement asset should not determine whether the Open Banking framework applies, and would encourage HM Treasury to ensure that the FCA's rulemaking under the Data (Use and Access) Act 2025 and the tokenised payments framework are designed to interoperate rather than in isolation from each other.

Other areas of feedback

Question 42: Are there any other areas of feedback on issues raised in this consultation?

Sequencing. These reforms are being delivered after the cryptoasset regime has opened for applications and after firms have selected the permissions they intend to hold. Firms are already assessing their business models against the proposed regulated activities and determining the scope of permissions they will need to apply for. In this context, uncertainty as to the final perimeter, particularly in relation to the treatment of stablecoin-related arranging and dealing, creates a material risk that firms will be required to make authorisation decisions without sufficient clarity. Absent clarity on the final scope of key elements of the regime, firms will either apply for broader permissions than ultimately necessary, increasing cost and complexity, or take a narrower approach and risk delays or disruption if their permissions prove insufficient once the regime is finalised.

CCI and GDF believe a published sequencing map would assist. We would suggest it cover the date the amending statutory instrument takes effect, the intended position on interim safeguarding, the point at which the payments perimeter changes for UK-issued qualifying stablecoin, the point at which the recognition mechanism for overseas regimes becomes operational, and the window for variation of permission applications. The order and approximate timing would be sufficient at this stage.

Interim supervisory clarity. Pending completion of the legislative update, firms using stablecoins for payments or treasury management purposes face uncertainty as to the supervisory treatment of that activity. We therefore recommend that HM Treasury and the FCA provide interim perimeter guidance, or a joint statement, clearly setting out the regulatory treatment of stablecoin payments and treasury use during the transitional period, including the supervisory approach pending implementation of the payments reforms. This would give firms greater certainty on how stablecoin payment and treasury activities will be

treated during the transition, while preserving the FCA's ability to supervise and enforce the applicable regulatory framework.

Financial promotions. We welcomed the government's proposal in the draft amending statutory instrument to exclude transactions in UK-issued qualifying stablecoin from the scope of the financial promotion restriction. As stablecoins are brought into the payments perimeter, we would encourage HM Treasury to confirm that a communication about a payment service provided in a qualifying stablecoin is treated in the same way as a communication about the equivalent fiat payment service.

Transitional treatment of existing permissions. Firms that obtain cryptoasset safeguarding, dealing or arranging permissions in order to provide stablecoin payment services in the interim will need to know what happens to those permissions once the payments framework takes effect. We would encourage HM Treasury and the FCA to confirm that such permissions can be surrendered or varied without a further application, and that no gap arises in which a firm holds neither the cryptoasset permission nor the payments permission for the same activity.

Integrated business models. More broadly, the reforms should be tested against firms that hold or seek multiple permissions. The consultation at times considers issuance, cryptoasset intermediation and payment services as distinct activities carried on by different types of firm, whereas digital asset firms may combine several of these activities within one operating model. The final framework should therefore be designed around activities and risks rather than assumptions about organisational form, with clear rules on how permissions, safeguarding, prudential requirements and supervision interact when those activities sit within the same legal entity.