Written Evidence Submitted by Global Digital Finance (GDF), Crypto Council for Innovation (CCI) and UK Cryptoasset Business Council (UKCBC)

SUBMITTED VIA PORTAL

28 August 2026

APPG Inquiry on Access to Banking Services for the UK Crypto and Digital Assets Sector

To whom it may concern,

GDF, UKCBC, and CCI are grateful to our members, industry contributors, and the public sector agencies who have been engaged on this topic of access to banking services for the UK crypto and digital assets sector.

The input to this response has been curated through our member discussions, industry surveys and reports, and engagement with the UK public sector over several years.

Importantly, our submission, which draws on published evidence, is fact-based[1]:

- Don't Bank On It (Startup Coalition, UKCBC and GDF, January 2025)
- Locked Out (UKCBC, January 2026), and
- Self-Custody Wallets and Their Role in Digital Finance (GDF and Block, with TRM Labs and Coinbase, June 2026).

The evidence indicates that banking access for crypto, digital asset and fintech firms is restricting fair competition in the financial services market, a material issue impacting firms choosing the UK as a jurisdiction for new and innovative financial services, and restricting consumer access and choice.

The answer is not to lower standards. It is to improve the precision with which those standards are applied. Greater supervisory clarity, individual risk assessment, better transparency, stronger data-sharing and modern compliance tools would support the shared objectives of banks, regulators, consumers and industry.

Aligning regulation with practical market access will help the UK protect consumers, preserve financial integrity, foster competition, and capture the economic benefits of responsible digital finance.

---

[1] Global Digital Finance, UK Cryptoasset Business Council and Startup Coalition, Don't Bank On It: Crypto and Web3 Firms' Experience of Accessing Banking Services (January 2025) ("Don't Bank On It"); UK Cryptoasset Business Council, Locked Out: Debanking the UK's Digital Asset Economy (January 2026) ("Locked Out"); Global Digital Finance and Block, in partnership with TRM Labs and Coinbase, Self-Custody Wallets and Their Role in Digital Finance (June 2026) ("Self-Custody Report").

We remain at the disposal of the APPG for any further questions or clarifications you may have, and we welcome a meeting to discuss these matters in more detail with our members.

Yours faithfully,

Lawrence Wintermeyer, Chair, Global Digital Finance

Simon Jennings, Executive Director, UK Crypto Business Council

Laura Navaratnam, UK Policy Lead, Crypto Council for Innovation

Introduction and Summary

GDF, UKCBC, and CCI welcome the opportunity to contribute to the APPG Inquiry. The evidence reviewed indicates that access to banking and payment services has become a material constraint on the effective operation of the UK's regulated digital asset market.

The problem is two-sided, and our evidence base addresses each side separately. **De-banking** describes firms being refused or losing their own business bank accounts and payment services and is evidenced here principally by Don't Bank On It. **Bank blocks** describe restrictions applied to consumers making payments from their personal bank accounts to fund accounts at FCA-registered cryptoasset businesses and are evidenced here principally by Locked Out. The two are distinct problems with a common root, which is the application of sector-wide risk categorisation in place of firm-level and transaction-level assessment.

On de-banking, Don't Bank On It found that 67% of crypto and digital asset firms responding on their account applications with the major banks considered had applied and been rejected; 50% had either been rejected or had an account closed, and only 14% had successfully opened an account without it later being closed. 89% viewed difficulties accessing banking as a significant barrier to succeeding in the UK, 76% said those difficulties had pushed them towards a bank they viewed as riskier, and 70% said the problem made them more likely to leave the UK.[2]

On bank blocks, UKCBC's Locked Out survey of ten major centralised exchanges estimates that 40% of payments made by customers from their personal bank accounts to fund exchange accounts are blocked or delayed; 80% of exchanges saw increased customer friction in the preceding year, 70% said restrictions reduced their appetite to invest, scale and hire in the UK, and 100% said banks provided no clear explanation for payment blocks or account restrictions.[3]

We fully recognise banks' responsibilities to prevent fraud, money laundering, sanctions evasion and other forms of financial crime. The question for the Inquiry is not whether controls should exist, but whether broad sector-wide restrictions remain proportionate when digital asset firms encompass different business models, regulatory statuses and risk profiles.

Both de-banking and bank blocks rest on an implicit assumption: that exposure to the sector carries an elevated risk that justifies restriction at the level of the whole category. That assumption is testable, and it has now been tested.

GDF's Self-Custody Wallets and Their Role in Digital Finance analysed approximately $40.6 billion across 318,930 wallet addresses. It found only 1% of analysed transaction volume had direct exposure to illicit counterparties, falling to 0.1% in the UK-linked subset. It also found that 37.7% of volume interacted with regulated virtual asset service providers, rising to 42% in the UK-linked subset, meaning that the great majority of this activity is not disconnected from regulated infrastructure but passes through it, creating natural points at which customer due diligence, transaction monitoring and sanctions controls already apply.[4]

The relevance to this Inquiry is direct. If measured risk is 0.1% in the UK-linked subset, and 42% of UK-linked volume already passes through regulated virtual asset service providers, then category-level restrictions at the banking layer are not targeting the risk.

---

[2] Don't Bank On It, "Firms' Experience: The Headlines" and "Firms' Sentiment: The Headlines".

[3] Locked Out, Introduction and Survey Findings.

[4] Self-Custody Report, Executive Summary. The study covered 318,930 wallet addresses and approximately USD 40.6 billion in transaction volume across five blockchains, supplemented by Coinbase data on approximately 1.95 million wallets.

They are duplicating controls that already exist while excluding legitimate firms and customers. This supports targeted, risk-based controls focused on actual behaviour and regulated touchpoints rather than assumptions about a technology or sector.

The Government and the FCA have set out an ambition for the UK's cryptoasset regime to support the growth of a competitive, world-leading digital assets sector. Yet the FCA opens applications for authorisation on 30 September 2026, with the regime implementing in October 2027, and firms will be applying for authorisation while unable to obtain the basic banking services required to operate. De-banking and bank blocks remain prevalent across the sector today, including for firms already registered with the FCA. The harms documented in this submission are occurring now and have been for some time.

We therefore recommend clearer supervisory expectations; more granular, risk-based banking decisions that distinguish between different business models, clients and banking products; greater transparency and review routes; better data collection; a permanent banking and digital finance forum; more consistent information requirements for firms seeking banking services; and wider use of blockchain analytics and information-sharing.

1. How significant are issues relating to access to banking services for the UK crypto and digital assets sector?

We consider access to banking one of the most significant operational and commercial challenges facing the UK's regulated digital asset sector. The issue goes beyond inconvenience. Businesses need bank accounts and payment services to receive customer funds, pay staff and suppliers, meet tax obligations, manage liquidity and comply with regulation. Don't Bank On It describes this basic access as fundamental to the ability of firms to operate and, for some, an existential issue.[5] This access is so crucial to financial service providers that provisions were added to the Payment Services Regulations to ensure statutory protections for payment service providers to have access to bank accounts. It is important, however, to distinguish access to basic banking and payment services from access to wider financial products. Lending and other products that create credit or balance-sheet exposure introduce additional risks and constraints for banks. Restrictions appropriate to those products should not automatically determine whether a firm can access basic banking services.

The problem is visible across firms of different sizes and business models. The Don't Bank On It survey covered firms from pre-seed start-ups to publicly traded companies; 60% of respondents were pre-seed or seed, with infrastructure representing the largest subsector alongside B2B and retail payments businesses. Importantly, 63% of respondents were not required to register with the FCA given the nature of their activities, illustrating that banking-access challenges extend beyond exchanges and other firms directly undertaking regulated cryptoasset activities. Some firms were sufficiently concerned about banking or regulatory repercussions that they were reluctant even to participate in the survey.[6]

The headline findings show persistent instability in business banking relationships. Of 102 responses on account applications, 67% had applied and been rejected outright. Respondents had held an average of 2.43 primary bank accounts. Half had experienced either a rejected application or an account closure, and only 14% had successfully opened an account with one of the banks

[5] Don't Bank On It, Introduction.

[6] Don't Bank On It, "The Data".

surveyed without it later being closed. Crypto, blockchain or Web3 involvement was often cited as the reason for rejection or closure, including for FCA-registered firms. The practical effect is that firms spend management time and resources maintaining multiple relationships, relying on more expensive payment service providers or seeking accounts overseas.[7]

The consumer side is equally important. Locked Out reports that almost all major UK banks and payment services firms impose either transaction limits or complete blocks on transfers to cryptoasset exchanges, often without differentiation by exchange-level fraud risk or whether the destination is an FCA-registered UK business. UKCBC estimates that 40% of transfers to exchanges are blocked or delayed. Locked Out benchmarking names 5 UK banks blocking transfers entirely and a leading money remittance bank, blocking bank transfers, with caps elsewhere ranging from £1,000 per day or per transaction (2 Tier 1 banks) to £2,500 per transaction and £10,000 per 30 days (2 other Tier 1 banks). Access therefore depends on the consumer's bank rather than the regulatory status of the recipient firm.[8]

The issue appears to be worsening. 80% of surveyed exchanges reported increased customer friction over the preceding 12 months; the UK scored 7.9 out of 10 for difficulty in securing banking access compared with other markets; one exchange observed close to £1 billion of declined UK transactions in a year through the payment routes it could directly measure; and one of the world's largest exchanges reported that the UK has the lowest 'pay-in rate' of all its international markets. The emergence of consumer campaigns challenging blanket restrictions further indicates that banking access is increasingly experienced as a consumer issue as well as an industry one.[9]

2. What impact do these issues have on businesses, consumers, innovation, investment, competition and the UK's competitiveness?

For businesses, unreliable access to banking increases cost, complexity and operational risk. Don't Bank On It reports that firms have been pushed towards overseas accounts and more expensive or less stable alternatives. A case study of a leading FCA-registered crypto payments company operating across more than 180 countries found that it had been unable to open an account with any UK bank despite complying with applicable UK requirements. It therefore relied on payment service providers that were frequently more expensive and whose risk appetite could change abruptly, creating continuing operational uncertainty. Another case study, Greengage, describes repeated account closures and reliance on expensive Banking-as-a-Service providers despite only indirect exposure to cryptoasset activity.[10]

The impact on investment is direct. In Don't Bank On It, 89% of respondents viewed banking access as a significant barrier to succeeding in the UK and 70% said it made them more likely to leave. Locked Out similarly found that 70% of major exchanges said transfer restrictions were reducing their appetite to invest, scale operations and hire in the UK, with several explicitly prioritising other markets. This matters because the surveyed exchanges collectively serve

[7] Don't Bank On It, "Firms' Experience: The Headlines" and "Firms' Experience: The Full Data".

[8] Locked Out, Introduction and Benchmarking (Figure 1: blocks and restrictions currently in place by banks).

[9] Locked Out, Survey Findings and Qualitative Responses.

[10] Don't Bank On It, Case Studies (Greengage; A Leading Crypto Payments Company).

millions of UK consumers, have processed hundreds of billions of pounds for UK users and employ highly skilled workers.[11]

Consumers experience a different but related harm: lack of predictability and choice. A customer can complete onboarding with an FCA-registered firm, receive mandated risk disclosures and still be unable to transfer funds because their bank applies a blanket policy. This creates confusion about the significance of FCA registration and can undermine trust in the regulated perimeter. It may also encourage some users to seek less familiar routes or overseas providers, potentially reducing rather than improving regulatory visibility.

Competition is also affected. Locked Out notes that exchanges are becoming dependent on a small and shrinking number of banks and fintechs that permit transfers without severe restriction, creating business continuity and concentration risks. For start-ups and smaller firms, the burden is proportionately greater: they have fewer resources to maintain multiple banking relationships, absorb extended onboarding or establish overseas arrangements. The result is a barrier to entry that can favour incumbents and reduce consumer choice.[12]

The cumulative effect is a competitiveness problem. The UK is investing significant policy and regulatory effort in building a comprehensive digital asset regime, yet firms report that access to basic financial infrastructure remains uncertain. If competing jurisdictions offer comparable regulatory standards with greater operational certainty, capital, jobs and product development can move accordingly. This affects not only exchanges, but the wider infrastructure, payments and technology ecosystem the UK is seeking to develop. Banking access should therefore be treated as part of the UK's digital finance competitiveness strategy, not as a narrow bilateral issue between individual banks and digital asset firms.

3. What are the main factors contributing to these issues?

The evidence suggests a combination of regulatory uncertainty, commercial risk appetite, operational capability and legitimate concerns about fraud and financial crime.

First, the regulatory framework is still in transition. The Financial Services and Markets Act 2000 (Cryptoassets) Regulations were laid in draft before Parliament in December 2025 and made in February 2026; the FCA continues to consult on the detailed rules, and full commencement of the regime is not expected until October 2027.[13] Banks must make commercial decisions while FCA rules and supervisory expectations continue to develop, and in this environment conservative internal policies may go beyond what regulation itself requires. UKCBC's response to FCA Discussion Paper DP24/4 repeatedly argues for proportionate, risk-sensitive regulation that differentiates according to actual risk and avoids unnecessary barriers to entry or competitiveness. The same principle is relevant to banking access.[14]

Second, digital asset businesses require specialist understanding. An exchange, custodian, payments business or technology infrastructure provider can present very different risks, as can the banking services each requires; effective risk assessment needs to distinguish between the firm's business model and activities, the individual client and the product being provided. There can also be a gap between a bank's stated risk appetite and how it is applied in client acceptance:

---

[11] Don't Bank On It, "Firms' Sentiment: The Headlines"; Locked Out, Introduction and Survey Findings.

[12] Locked Out, Introduction.

[13] Locked Out, Conclusion; Financial Services and Markets Act 2000 (Cryptoassets) Regulations 2026.

[14] UKCBC, Response to FCA Discussion Paper DP24/4 (2025).

where specialist knowledge is uneven across business, risk and onboarding functions, sector labels can become a proxy for assessing the underlying risk. For smaller firms in particular, the cost of due diligence can make a relationship commercially unattractive, and a blanket 'no crypto' approach becomes the simpler outcome.

Third, banks face real fraud, AML, sanctions and consumer-protection obligations. However, the empirical evidence supports more targeted controls. The Self-Custody Report finds that self-custody activity is not disconnected from regulated infrastructure: 37.7% of analysed volume involved VASPs, creating natural compliance touchpoints for customer due diligence, transaction monitoring and sanctions controls. Only 1% of analysed transaction volume had direct exposure to illicit counterparties, falling to 0.1% in the probabilistic UK-linked subset, where interaction with regulated VASPs was higher (42%). The UK's exchange-level controls are, on this evidence, working. The report also notes FATF's risk-based approach and argues that effective controls are best concentrated at regulated intermediaries and on transactional behaviour rather than the mere use of self-custody.[15]

Fourth, information asymmetry contributes to mistrust. Locked Out found 100% of exchanges surveyed said banks provided no clear explanations for restrictions. Don't Bank On It likewise found that 72% of respondents had changed how they described their business because of concern about being refused banking services. Where firms do not know why an account was refused or a transfer blocked, they cannot remediate legitimate concerns; where banks lack reliable sector data, they may default to broad proxies. Better information-sharing and transparency are therefore part of the solution.[16]

Finally, it is worth recording that existing law already points towards individualised assessment. Regulation 105 of the Payment Services Regulations 2017 requires case-by-case assessment of payment restrictions; the FCA's Consumer Duty requires firms to avoid foreseeable harm from unduly restricting legitimate customer activity; and the Competition Act 1998 guards against practices that distort markets. The recommendations below therefore ask that existing obligations be applied with greater precision, not that banks accept new burdens.[17]

4. Are there examples from the UK or other jurisdictions where these issues have been addressed successfully?

No jurisdiction has eliminated every banking-access challenge, but there are useful precedents for a more structured approach. Don't Bank On It highlights Hong Kong and France. The Hong Kong Monetary Authority has stated that banks should endeavour to support the legitimate need for bank accounts of VASPs licensed and regulated by the Securities and Futures Commission. France's framework includes a specific provision intended to prevent designated VASPs being denied banking access merely because of their status as a VASP.[18] The United States provides a further example: US regulators have clarified that payments to lawful digital asset platforms should be assessed under standard fraud and AML controls rather than subjected to sector-wide restrictions.[19] The lesson is not that banks must accept every applicant; it is that regulatory status

[15] Self-Custody Report, Executive Summary and UK-linked wallet analysis.

[16] Locked Out, Survey Findings; Don't Bank On It, Solutions ("What We Don't Know").

[17] Locked Out, Legal and Global Regulatory Context (Regulation 105 of the Payment Services Regulations 2017, the FCA Consumer Duty, and the Competition Act 1998).

[18] Don't Bank On It, Solutions ("Solving the Issue").

[19] Locked Out, Legal and Global Regulatory Context.

should carry meaningful weight in a risk-based assessment and blanket sector exclusion should not substitute for due diligence.

GDF's Self-Custody Report also notes risk-based approaches in Singapore and the Emirates, alongside FATF's emphasis on controls at regulated touchpoints. These examples show that strong AML/CFT expectations and market access can coexist when regulators provide clear expectations and firms invest in appropriate controls.[20]

The UK also has its own precedents. HM Treasury concluded in its June 2022 consultation response on the Money Laundering Regulations that self-custody transactions should not automatically be viewed as higher risk, finding no good evidence that such wallets present a disproportionate risk of use in illicit finance, and requiring enhanced information collection only where elevated risk is identified. The UK-linked findings of the Self-Custody Report now provide empirical validation of that judgement.[21] UKCBC's FCA consultation response applies the same logic, arguing that requirements should be calibrated to the different risks presented by different market participants and warning that disproportionate obligations can deter listings, investment and innovation. For the Inquiry, the key lesson is to apply that logic to banking access: distinguish regulated from unregulated activity, distinguish higher-risk from lower-risk customers and transactions, and use data rather than sector labels wherever possible.[22]

5. What potential solutions or changes should the APPG consider?

We recommend a package of measures designed to improve access without weakening banks' responsibilities for financial crime and consumer protection.

> **1. Reinforce risk-based banking decisions.** The Inquiry should encourage the FCA and PRA to make clear that crypto and digital asset firms should be assessed according to their business model and activities, the individual client's risk profile and the banking product or service being requested. Restrictions appropriate to lending or other products involving credit or balance-sheet exposure should not automatically determine access to basic banking and payment services, and banks should apply their risk appetite consistently across business, risk, compliance and onboarding functions. Locked Out makes the same core recommendation and explicitly argues that differences between exchanges should be recognised.[23]
>
> **2. Improve supervisory clarity.** HM Treasury, the FCA and PRA should clarify expectations for banking relationships with regulated crypto and digital asset firms as the new regulatory perimeter matures. Regulatory status should be a meaningful factor in banks' risk assessments, while preserving their responsibility to undertake appropriate due diligence on each relationship.
>
> **3. Improve transparency and review routes.** Where legally permissible, firms and consumers should receive meaningful reasons for account refusals, closures or transfer restrictions, together with a clear route to review. Don't Bank On It argues that, absent of

[20] Self-Custody Report, Introduction and discussion of international regulatory approaches.

[21] HM Treasury, Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017: Response to the Consultation (June 2022), discussed in the Self-Custody Report.

[22] UKCBC, Response to FCA Discussion Paper DP24/4 (2025).

[23] Locked Out, Policy Recommendations.

national-security constraints, explicable reasons should be given; Locked Out found a complete lack of clear explanations among surveyed exchanges.[24]

4. Establish a standing Banking and Digital Finance Forum. Government should convene HM Treasury, FCA, PRA, banks, payment firms, UK Finance, social-media platforms and regulated digital asset firms to share fraud typologies, data and good practice. The Forum could also develop a common information framework for firms seeking banking services, covering business model, regulatory status, transaction profile, client asset arrangements and financial-crime controls, giving banks a more consistent basis for assessment and reducing information asymmetry. This mirrors a recommendation in Locked Out and would help break the current information impasse.[25]

5. Build a better evidence base. The FCA should collect anonymised data on refusals, closures, transfer restrictions and complaints. Don't Bank On It specifically argues that without robust data the FCA cannot assess the scale of the issue or banks' behaviour against consumer-protection and competitiveness objectives.[26]

6. Use technology-enabled financial crime controls. Banks and regulators should expand the use of blockchain analytics, transaction monitoring and information-sharing. The Self-Custody Report shows that public blockchain data and regulated touchpoints provide tools for risk-sensitive supervision that are unavailable in many traditional cash-based channels.[27]

7. Support consumer access to regulated markets. Consumers should, as a matter of ordinary routine, be able to transfer their own funds to FCA-registered firms unless there is evidence of elevated risk relating to the customer, transaction or recipient. This is not a request for special treatment; it is a request for proportionate treatment that recognises regulatory status and actual risk. Where additional safeguards are needed, banks could consider trusted-recipient lists, transaction history, customer vulnerability and other granular indicators rather than universal caps or blocks.[28]

Timing matters. Authorisation under the new FSMA regime should ultimately give banks greater confidence in regulated platforms, but full commencement is not expected until October 2027 and the harm documented above is occurring now, while jurisdictions including Singapore, Hong Kong and Dubai actively court the firms the UK risks losing. The measures above bridge that gap and help ensure the UK can capitalise on the framework it has legislated for.[29]

6. Is there any other evidence or information that would assist the APPG?

The Inquiry should consider banking access as part of the UK's wider digital finance strategy. Parliament, HM Treasury, the FCA and the Bank of England are building a more comprehensive regulatory perimeter. That work will not deliver its full benefits if legitimate businesses cannot

[24] Don't Bank On It, Solutions; Locked Out, Survey Findings.

[25] Locked Out, Policy Recommendations (forum recommendation).

[26] Don't Bank On It, Solutions ("Mapping the Issue").

[27] Self-Custody Report, discussion of blockchain intelligence and analytics.

[28] Locked Out, Policy Recommendations (nuanced approach to retail customer risk).

[29] Locked Out, Conclusion.

access basic banking services or if consumers cannot reliably reach regulated firms through the payment system.

Two further evidence points may assist. First, transaction-size data: 92% of self-hosted wallet transactions in the Coinbase dataset analysed for the Self-Custody Report were below USD 1,000, consistent with ordinary consumer payments and remittances rather than the high-value flows sometimes assumed. Second, industry cooperation on financial crime is already delivering results where data is shared: the Beacon Network, built by TRM Labs with industry partners, has enabled real-time freezing of illicit funds before withdrawal, including USD 1.5 million in a single law enforcement case, and the T3 Financial Crime Unit has frozen over USD 250 million in criminal assets since September 2024. Banks citing financial crime as grounds for blanket restrictions have willing and capable partners in the regulated industry; what is missing is a mechanism, which the proposed Forum would provide.[30]

The Inquiry should also note the House of Lords Financial Services Regulation Committee's recent report, Stablecoins: waiting for regulation (June 2026). The Committee concluded that the UK's regulatory regime should be designed to allow a sterling stablecoin market to establish and grow, that regulation must be proportionate and enable innovation while mitigating risk, and that the regime must create a level playing field allowing stablecoins to compete with other forms of payment in the UK.[31] The same principle should apply to banking access. Restricting regulated firms' access to payment infrastructure risks undermining the Government's wider policy objectives, including the National Payments Vision and the development of more innovative, competitive payment systems.[32]

We put forth that the Inquiry should reinforce a simple principle: regulation and access should evolve together. A well-regulated market requires legislation and supervision, but also practical access to the financial infrastructure that allows firms and consumers to participate in that market. Improving access through proportionate, risk-based and technology-enabled controls would strengthen, not weaken, consumer protection and financial integrity by encouraging activity to remain within transparent, regulated channels.

---

[30] Self-Custody Report, Coinbase / Base App transaction-size data; Beacon Network and T3 Financial Crime Unit discussion.

[31] House of Lords Financial Services Regulation Committee, Stablecoins: waiting for regulation (June 2026).

[32] HM Treasury, National Payments Vision (November 2024).