



1 Angel Court,  
London, EC2R 7HJ  
[ukfinance.org.uk](http://ukfinance.org.uk)

[davidpostings1@ukfinance.org.uk](mailto:davidpostings1@ukfinance.org.uk)

Dr Lisa Cameron MP  
Chair of the Crypto and Digital Assets APPG  
By email: [appg@cryptouk.io](mailto:appg@cryptouk.io)

22 November 2023

Dear Lisa,

Thank you for your letter dated 27 October 2023 regarding access to UK bank accounts for crypto and digital asset businesses. I fully appreciate the importance of this issue and I am pleased to be able to liaise with yourself and the All-Party Parliamentary Group (APPG) for Crypto and Digital Assets on this topic. I would also like to take this opportunity to commend the APPG's important work in understanding the opportunities and challenges for this sector.

Both in 2022 and earlier this year, UK Finance have utilised our convening power to bring together the different sides of the industry on a number of issues. UK Finance runs an Industry Strategic Threat Management process, through which members share intelligence about new Fraud and Scam threats, both to help prevent fraud happening in the first place and deliver consistency across the industry in terms of how best to respond.

Through this process, last year a bespoke working group focused on crypto was set up, and UK Finance has held roundtables with exchanges and Crypto UK and the Electronic Money Association (with the National Crime Agency observing). These were held to better understand the challenges faced and opportunities to mitigate the consumer harms and wider economic crime experienced. We will continue to host events designed to enhance industry collaboration, address misunderstandings, and share best practice. Feedback from both sectors to date is that they find the detailed operational projects more helpful than general risk and compliance discussions.

It is worth re-stating here, and as previously discussed with the Financial Conduct Authority and the Payments System Regulator, UK Finance is not able to set members' risk appetite. Members' risk decisioning is based on complex factors. Members are of course also very alert to the overall risk profile of the sector and the regulatory approach to it. Many members are positive about the work being taken forward to adapt the regulatory perimeter to bring appropriate controls for firms providing regulated activities.

However, a pressing area of concern for many members is the increased and often disproportionate risk and responsibility burden being placed on financial institutions (FIs) by regulators in cases of consumer fraud and scams (both for crypto and indeed more widely). The data from FI member firms currently shows a rate of fraud on bank transfers to crypto firms that is several orders of magnitude higher than to other firms. One bank noted a fraud rate of 19% on interbank transfers and 3% on card transfers – whereas the fraud rate is typically one payment in every several thousand transactions.

Furthermore, for FIs to take a comprehensive risk-based approach is often difficult given the lack of transparency infrastructure to help assess the relative risks of different crypto firms. Unlike much of the banking sector, the crypto sector does not have Confirmation of Payee or industry fraud communication initiatives (Best Practice Standards (BPS) for Authorised Push Payments (APP) messaging, Mules Insights Tactical Solution (MiTS), etc). The development of systems for communication of crypto transaction information is still ongoing and we at UK Finance are seeking to expedite these discussions.

However, it is still unclear how these will interact with payment information obligations on the fiat sector. The blockchain analytics tools are still at an early stage and do not compensate at scale for this wider market opacity. This challenging risk environment is being compounded by decisions made against FIs by the Financial Ombudsman Service (FOS) that do not follow the usual precedents. The FOS appears to have taken the approach that when payments leave the regulatory perimeter, they'll allocate the cost to the firm most recently in receipt of the funds. They have also required banks to take a highly manual and precautionary approach to such transfers.

Further uncertainty has been created by the APP fraud approach from the PSR, in particular, which is leading to a heightened risk awareness for firms. Blocks on payment to high-risk destinations is exactly the type of additional protection that will become more common as the new PSR rules come into effect.

In addition to the risk-averse environment created by the regulators' current approach, I also note that there are a number of legal and compliance factors specific to interactions by FIs and payment service providers with the crypto sector, including regulatory expectations that traditional financial firms screen outbound payments to avoid interacting with unregistered crypto firms.

UK Finance's goal is to support the government's ambition for the UK to be a crypto hub – a place where responsible and ethical innovators come to do business. UK Finance and its members want to balance security and service for end users. Adapting regulation to support crypto is a key part of this and I support the government and regulators to update the regulatory perimeter and rules for this sector.

But it is also important to distinguish that the problem is wider than the inherent characteristics of crypto with its potential volatility, its ease of disbursement and its immature regulations. Victims who lose money are commonly vulnerable to a false hope of investment growth through advertising and social engineering which diverts them from trusting the paying bank – and so consumer education and collaboration across the whole ecosystem is crucial.

I hope that as the regulatory perimeter becomes clearer, it will be easier for firms to assess their risk exposures.

Yours sincerely

A handwritten signature in black ink, appearing to read 'David Postings', with a horizontal line underneath.

David Postings  
Chief Executive, UK Finance