

EMAIL SUBMISSION TO: [FCA-PSR-digitalwallets@psr.org.uk](mailto:FCA-PSR-digitalwallets@psr.org.uk)

To whom it may concern,

**Re: FCA & PSR Call for Information on Big Tech and Digital Wallets**

**About Global Digital Finance (GDF) and Crypto Council for Innovation (CCI)**

GDF and CCI 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.

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.

The input to this response has been curated through a series of member discussions, industry engagement, and roundtables, and both GDF and CCI are grateful to their members who have taken part.

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,

Elise Soucie – Executive Director – GDF  
Laura Navaratnam - UK Policy Lead, CCI

## Response to the Call for Information: Executive Summary

Overall GDF and CCI are supportive of the aim of the Call for Information (referred to henceforth as the CFI). We firmly believe in the UK's stated intent to support innovation and provide end-to-end regulation for the evolving digital finance ecosystem while following the principles of same risk, same regulatory outcome and simultaneously developing new regulatory requirements for new risks. We also appreciate the industry engagement and thoughtfulness with which the UK authorities have started to develop their approach to digital wallets. Our response to this CFI looks to provide suggestions of areas which may be encompassed by the broad term 'digital wallet' but may not be reliant on by Big Tech companies. The ecosystem is fast evolving, and our collective members firmly believe that the FCA and PSR should consider the broad range of digital wallets which are being developed, and how to apply any future regulatory frameworks both proportionately and appropriately.

Noting our focus on digital wallets used for crypto and digital assets, we have worked with our members to provide additional context and technical feedback on how these types of wallets are evolving, and their place in the digital wallet landscape set out in the CFI. Through this process our members identified key areas that we believe the FCA and PSR should consider as they move forward to develop a regulatory regime for digital wallets. The core areas identified are:

- 1. The FCA/PSR's Broad Definition and Discussion of 'Digital Wallet' Does Not Distinguish Between Digital Wallets that Rely on Centralised Intermediaries and Self-Hosted Wallets, Which Do Not;**
- 2. Different Types of Wallets May Require Different Regulatory Treatment – Requirements Should be Proportionate & Appropriate;**
- 3. Emerging Frameworks Should be Technology Neutral and Future Proof as the Digital Wallet Ecosystem is Fast Evolving.**

### **1. The FCA/PSR's Broad Definition and Discussion of 'Digital Wallet' Does Not Distinguish Between Digital Wallets that Rely on Centralised Intermediaries and Self-Hosted Wallets, Which Do Not**

The CFI defines digital wallets as “[...] apps, software, or online services that allow consumers to make payments, quickly and conveniently, using mobile phones or other electronic devices.” It goes on to identify several ways in which digital wallets differ, including through the types of payments that they enable, the technology that they use, the payment instruments they work with, the retailers that accept them, and whether they hold funds. However, while we appreciate the FCA and PSR's elaboration of common types of digital wallets offered by big tech companies, we note that the FCA and PSR did not distinguish between digital wallets that rely on centralised intermediaries and “self-hosted wallets,” which do not. We are concerned that the CFI's broad definition of “digital wallet” could capture self-hosted wallets, even though they are fundamentally different from Big Tech wallets, which we define as digital wallets that generally rely on and are controlled by large, well-established, centralised intermediaries.

Unlike Big Tech wallets, self-hosted wallets are tools that enable users to interact with blockchain networks by allowing them to sign and send cryptographic messages to blockchains without depending on centralised intermediaries. They are operated on a user's own device and do not rely on servers or any third-party hosting. Individuals use self-hosted wallets as a convenient way to interact with blockchain networks, just as web users use web browsers to access the Internet. With a self-hosted wallet, users are able to hold their private keys and digital assets, as well as send and receive digital assets in a peer-to-peer manner.

Self-hosted wallets are thus a key innovation in digital wallets because they enable full user ownership and control of assets, mitigating risks traditionally associated with users having to rely on centralised third-party intermediaries, such as capitalisation and misappropriation risks. Rather than relying on a centralised intermediary such as a financial institution to custody assets, self-hosted wallet technology enables users to store and utilise their assets. Self-hosted wallets also offer enhanced data privacy and security because users are not reliant on third-party hosting, which can otherwise expose them to the risks of hacks, exploits, and data breaches.

Because centralised intermediaries do not control self-hosted wallets, they do not pose the same risks that the FCA and PSR associate with Big Tech wallets. For example, as the CFI notes, Big Tech wallets can utilise their control to raise barriers to alternative wallet solutions, limiting competition. As self-hosted wallets are tools controlled by users, they do not pose this risk. For these reasons, we caution the FCA and PSR against applying rules to "digital wallets" in an overly broad manner that extends the same regulation to self-hosted wallets or other wallets which may have unique risk profiles, and mitigants.

## **2. Different Types of Wallets May Require Different Regulatory Treatment – Requirements Should be Proportionate & Appropriate**

There are many types of digital wallets which are very different in use case, technical composition, and risk to the common digital wallets used broadly for payments such as ApplePay and GooglePay set out in the CFI. As such, and given they perform a different market function, we believe that one-size-fits-all regulation for 'digital wallets' as defined could create an unlevel playing field for crypto and digital asset markets. As self-hosted wallets enable users to fully control their assets they should not be required to comply with requirements that could extend to a Big Tech wallet based on the latter's reliance on a centralised intermediary. For example, a self-hosted wallet should not be considered a "payment instrument" under regulation 2 of the Payment Services Regulation because they do not involve an agreement between a payment service user and a payment service provider. Indeed, in the case of self-hosted wallets, there is no "payment service provider." For this reason, we caution against seeking to regulate self-hosted wallets like Big Tech wallets.

We also believe it is important to clarify the difference between digital wallets used for tokens, and mobile wallets such as most of those used by Big Tech companies.

## **3. Emerging Frameworks Should be Technology Neutral and Future Proof as the Digital Wallet Ecosystem is Fast Evolving**

The digital wallet landscape continues to evolve and there are now many types of crypto and digital asset wallets in particular. The digital wallet industry in crypto is also highly diversified and competitive. There are varied and numerous market participants which results in strong competition and innovation as well as focus on customer outcomes which is paramount to ensuring the trust and engagement required for repeated product usage. While these evolutions

continue we would encourage regulators not to stifle responsible innovation but to instead maintain the UK's principles and outcomes focused approach in order to develop comprehensive, proportionate, and appropriate frameworks for the unique and diverse types of digital wallets.

### **Response to the Call for Information: Questions for Public Consultation**

Please note that given our focus areas set out in the executive summary that we have not responded to each question in the Cfi. Instead, we have provided feedback and input on the specific questions and chapters that are relevant to the key areas. We would also note that our response primarily focuses on digital wallets used for crypto and digital assets, rather than digital wallets provided by Big Tech firms more broadly.

*1. What are the benefits of digital wallets for consumers, businesses and other parties in the payments value chain? Your answer might include comparison to alternative ways of initiating payments and consideration of the impact of digital wallets on UK payment trends and metrics, such as:*

- *the impact on consumer and business experience of payments*
- *the speed and convenience of checkout processes*
- *the rate of fraudulent transactions*
- *the cost of making or receiving retail payments for different types of party*

We would note that as defined in the Cfi there are several benefits to digital wallets. These include but are not limited to greater privacy for sensitive payment information which may be more visible if paying with a physical card; speed, accessibility, and ease of use and access for the consumer, and reduction in the need to carry physical cards and wallets which may be stolen or lost.

In addition to this, it is important to also highlight the benefits of crypto and digital asset wallets which are unique when compared to other digital wallets and have benefits specific to their use cases. A crypto or digital asset wallet, “Stores the public and private keys required to buy cryptocurrencies and provide digital signatures that authorise each transaction.<sup>1</sup>” Crypto wallets may take different forms, but they can include physical devices, software, or both. The different types of crypto and digital asset wallets are further discussed under Q3. They support the transfer of crypto and digital assets blockchains and may also provide links for users to access decentralised applications (dApps). Most importantly, by enabling full user control, self-hosted wallets protect consumers by mitigating several legacy risks associated with custodial assets with a trusted intermediary such as capitalisation and misappropriation risks. – as such, they are a key part of the crypto and digital asset ecosystem.

Furthermore, digital wallets specialised at present to cryptocurrencies are able to seamlessly switch between payment methods - able to send, for example, a stablecoin or bitcoin at the user's discretion, as they direct. This makes them more flexible and delivers competition and choice directly to users in what forms their value transfer takes.

The digital wallet industry in crypto is also highly diversified and competitive. As noted above, there are varied and numerous market participants which results in strong competition and innovation as well as focus on customer outcomes which is paramount to ensuring the trust and engagement required for repeated product usage.

---

<sup>1</sup> <https://crypto.com/university/crypto-wallets>

Using some form of a digital wallet to store private keys is a critical part of the crypto and digital asset ecosystem. It is important that as the FCA and PSR develop regulations and requirements for digital wallets, that they also consider how these requirements will complement their broader framework for crypto and digital assets. Regulation of crypto digital wallets should be proportionate and appropriate to both the type of digital wallet and its use case. Any future approach should ensure that digital wallets can continue to guarantee that the end user is able to assert the same choice and the same control as they would with their current physical wallets.

As further explored within our response to this consultation, the varying types of crypto and digital asset wallets also have their own specific benefits and use cases. This is further discussed throughout Q3.

*2. Please provide information on the use of digital wallets in the UK. We welcome information on the current situation as well as trends over time. We are interested in the percentage of retail transactions overall (by value and volume) that involve digital wallets, as well as more detailed information on usage – for example, by digital wallet provider, customer type and/or for different transaction types, such as:*

- *in-store/face-to-face retail payments*
- *retail payments using mobile web browsers, including on tablets*
- *retail payments using mobile apps, including on tablets*
- *retail payments using desktops/laptops*
- *other*

*3. Are there likely to be any significant developments in the UK over the next five years regarding digital wallets – for instance, in terms of their usage, functionality or features? This could include the launch of entirely new functionalities/services or ones that are already available in other countries. As far as possible, please explain the likelihood of these developments, their expected magnitude and their implications for competition, innovation and service users.*

First, we would note that overall, there are many types of digital wallets which are very different in use case, technical composition, and risk to the common digital wallets used broadly for payments such as ApplePay and GooglePay set out in the CfI. As such, and given they perform a different market function, we believe that one-size-fits-all regulation for ‘digital wallets’ as defined could create an unlevel playing field for crypto and digital asset markets.

Additionally, we believe it is important to clarify the difference between digital wallets used for tokens, and mobile wallets such as most of those used by Big Tech companies. Digital wallets, used for crypto and digital assets are further discussed and delineated throughout our response.

We agree that as noted in the question there are likely to be significant developments. As noted in the introduction the digital wallet landscape continues to evolve and there are now many types of crypto and digital asset wallets in particular. These can be broadly categorised into two overarching types of wallets, with further sub technologies that can be applied to either type of wallet:

- **Exchange/Custodial Wallets:** These wallets hold the keys of individuals who are the customers of the exchange or other third-party intermediary (noting not all custodial

wallets are held by exchanges), meaning a custodian or third party has control of the private keys. This arrangement may also be vulnerable to hacking and requires trust in the custodian – hence the work already in train by the UK authorities to establish a robust regulatory regime for custody. However, it is also easier for the consumer as the custodian will have key recovery mechanisms in place.

- **Self-Hosted/Self-Custody Wallets:** A self-hosted wallet is hosted and controlled by the user, as opposed to being hosted by a third-party service, like an exchange. In this instance, the user is provided with full control over the means of access to their keys, and is therefore solely responsible for how they access blockchains and blockchain protocols, and their control and use of their digital assets. Whilst this places greater responsibility on the user, these wallets protect from counterparty risk, and minimise other intermediary operational risks, such as hacks or fraud.

Crypto digital wallets can be further characterised:

- **Hot Wallets:** These wallets are connected to the Internet and are applications that can be used on a computer or phone. They are easy to use for fast online payments but may be more susceptible to hacking or online leaks or threats.
- **Cold Wallets:** These wallets store private keys offline on hardware. They are generally safer from hacks or online threats, as to withdraw digital assets the wallet must be connected to a computer or phone. However, while generally more secure, they may be less convenient for frequent use and more expensive.
- **Multi-signature (or Multisig) Wallets:** These wallets require two or more private key signatures to authorise a transaction. This adds an extra layer of security, but also typically requires multiple people to share ownership of the private keys.
- **Other (or a blend of some of the above categories):** Some new types of wallets are also emerging (such as Bitkey<sup>2</sup>) which combines characteristics like exchange management of keys, hardware security, and key recovery tools.

Given these different types of digital wallet, we would note that depending on the use case or the individual/business, there may be a need to utilise a different type of wallet. For example, for those making frequent transactions with a higher risk tolerance a hot wallet may be appropriate. For those who wish to hold their digital assets longer in a more secure way, a cold wallet may be a better solution.

The benefits, particularly for some consumers, to using a secure crypto or digital asset wallet that is self-hosted (or self-custodied), is that they may be a safer alternative to storing digital assets on an exchange. Most importantly, a self-hosted wallet gives the consumer more direct control over their assets.<sup>3</sup> Exchanges and other custodial businesses manage the private keys required for customers to access their crypto, which means access to consumers' money could, in some instances, potentially be limited or cut off for various reasons. Hackers may also target such entities because of the large amount of crypto they hold. If an exchange or custodial business is hacked or shut down, crypto or digital assets may not be recoverable.

Conversely though, for many individuals, they may not wish to self-custody their private keys. Crypto exchanges and custodial wallet providers usually take steps to enhance the security of their customers' crypto and digital assets and may also use cold storage as part of their custodial

---

<sup>2</sup> <https://bitkey.world/en-US>

<sup>3</sup> <https://bitkey.world/en-US>

solution. GDF and CCI members are supportive of the FCA's proposals to develop a robust and proportionate regime for digital asset custody. We look forward to the UK finalising a comprehensive regime for crypto and digital assets, of which custody and custody requirements are a crucial element. Appropriate custody requirements will ensure, for example, that custodians have backups in place to help users regain access to their private keys if lost. When self-custodying (where the sole responsibility for a private key lies with the individual) loss of keys may mean total loss of funds, so exchange/custodial wallets may be more consumer friendly and offer some additional protections.

We note that digital wallets, especially those natively designed for use with crypto and digital assets, are at the start of their technological evolution. Some future iterations are expected to be able to include:

- Decentralised sign-on (passkeys) for websites - e.g., allowing stronger storage of financial and nonfinancial information;
- Increased customer UX experience - e.g., APIs & integrations, beginner products, key recovery features to enhance security;
- Storage of tokenized assets - stocks, t-bills, intellectual property, tickets;
- Digital Identity - streamlined KYC, privacy-focused information sharing, secure authentication;
- Direct Payment integration - e.g., 'pay with wallet' functions on commerce websites
- Remittance / portable travel wallet - use of stablecoins or similar coins with stabilising mechanisms;
- Digital voting and 'Internet of Things' integrations.

*4. Are there any features related to the supply of digital wallets that cause harm to (or mean that payments could otherwise work better for) service users? We are particularly interested to hear about any features that may limit competition in payments or otherwise adversely impact service levels, degree of innovation or fees. Where available, please provide supporting evidence.*

As noted under Q3, we are concerned that one-size-fits-all requirements for digital wallets may limit innovation, competition, and prevent the scaling and use of crypto and digital asset wallets. It is critical to consider the unique use cases of these types of wallets and how they may be used in a future digital finance landscape.

In particular, we would note that a self-hosted or self-custodied wallet is very different to the digital wallet solutions provided by Big Tech firms. They are software or hardware solutions, more akin to a leather wallet that holds a range of important credentials, whether a local library card, an identification card, or credit or debit cards that enable the user to access funds. Like producers of these physical wallets, developers and providers of self-hosted wallets do not have, and are not required to have, the same type of customer account relationships with users as do traditional financial services providers. In turn, self-hosted wallet providers do not perform, execute, or 'effectuate' transactions on behalf of users. As a result, self-hosted wallet providers will often partner with third-party service providers, such as digital asset exchanges, to ensure users have a secure and seamless experience of moving digital assets between their exchange accounts and their self-hosted wallets. Because self-hosted wallet providers do not have account relationships with their customers, they do not have information about relevant transactions, nor collect other data, as do more common digital wallets. In the interests of protecting freedom of competition, choice, and privacy, to impose similar requirements on

individuals as those required of Big Tech providers would be disproportionate and harm consumer choice.

*5. Please explain whether any harms identified in your response to Question 4 could be outweighed by benefits associated with those same features – for instance, in terms of greater convenience or security. Where available, please provide supporting evidence.*

*6. If you think that there are features that result in harm, what measures would be effective and proportionate to improve outcomes? Please explain:*

- *any technical standards that would need to be specified – for instance, through regulation*
- *whether the measure would be effective in isolation or other steps would also be required (if the latter, please specify what these might be)*

Globally, steps are already being taken to ensure that crypto and digital asset transfers are subject to appropriate requirements.

Furthermore, in regards to self-hosted wallets, it should also be noted that they at present do not themselves undertake - and therefore do not preclude - exchange or identity authentication services or facilities. These are undertaken at the exchange or issuance level and whilst the self-hosted wallet provider would not be required to take additional steps to know or verify the identity of the wallet holder, that holder would regardless have to go through these checks when receiving or using their relevant assets to their respective wallet, ensuring that exchangers or issuers would have sufficient information regarding the transaction. The publicly verifiable aspect of a ledger, based on pseudo-anonymous addresses, means that the ability is retained to track assets across multiple addresses or users. The ‘on/off’ ramp should be considered the gate at which holders are checked and verified to abide with regulatory principles.

Finally, as noted above under Q3 evolving custody regulatory requirements are another key way to mitigate risk, and proportionate and appropriate requirements for custodial wallets will be a crucial part of the UK’s regulatory regime as it continues to evolve. We are supportive of the FCA developing clear and proportionate requirements for digital custody. In a recent report, “Digital Asset Custody Deciphered”<sup>4</sup>, GDF aimed to support regulators and industry in considering a balanced approach to digital custody. The report sets out to provide financial services professionals, investors and policymakers of all experience and levels with a starting point, covering nine factors in subsections across three section domains:

- Legal, Regulation, and Financial Crime
- Settlement & Finality, and Asset Segregation
- DLT Governance, Staking, Key Management, and Interoperability.

*7. If not covered in your other responses, please explain what fees (if any) digital wallets charge and how these have changed over time. What impact do these fees have on UK service users? Please provide any evidence available to support your answer.*

We do not have a view on this question at present as it seemed primarily to focus on fees and their evolution in BigTech wallets.

*8. Aside from fees charged to issuers, are there any other sources of potential revenue available to pass-through digital wallet providers? If so, what are their impacts on service*

---

<sup>4</sup> <https://www.gdf.io/resources/digital-asset-custody-deciphered-a-primer-to-navigating-the-challenges-of-safeguarding-digital-assets/>



users?

**9. What role could digital wallets have in increasing the take up of account-to account payments in the UK retail sector? Please explain the reasons for your answer.**

We would note that peer-to-peer payment is more prevalent in the crypto and digital asset ecosystem than it is in the more traditional payments landscape. While it has been evolving in traditional payment rails as well, this is an area where it may be beneficial to consider and analyse the innovation occurring in digital assets and how it can be applied to the broader transformation and digitisation of the UK's payments systems.

**10. Are digital wallets likely to integrate existing and potential account-to account payment types, including for spontaneous purchases? If not, what barriers exist and what do you think needs to happen for digital wallets to integrate account-to-account payment types in a manner that enables effective customer access to them? Please explain your answer and provide any evidence you have.**

As discussed under Q9, peer-to-peer payments are already common within the crypto and digital asset landscape. Noting however, that peer-to-peer transfer is not equivalent to account-to-account.

**11. How do you think digital wallets should best develop to encourage effective competition between payment systems that benefits service users? This could involve:**

- *the fees involved in account-to-account payments*
- *the commercial agreements underlying the digital wallet user experience*
- *whether consumers are able to use one or multiple digital wallets*
- *how the underlying payment system is chosen*
- *any operational issues, including necessary investments in infrastructure*
- *whether any technical standards should be set, including through regulation*
- *whether other payment providers, such as PISPs, will be able to access digital wallets*

As noted under Q4 and also Q16, as digital wallets continue to evolve, it is likely that consumers may have both traditional digital wallets, as well as crypto and digital asset wallets. As such, we would encourage the FCA and PSR to develop proportionate requirements, which are also harmonised with their broader framework for crypto and digital assets, in order to support the usage of broader forms of digital wallets for consumers in the UK.

**12. What harms are likely to arise in the event of a digital wallet provider's operational failure, either now or over the next five years?**

The key issue that we would like to raise at this early stage in the UK's thinking around digital wallets as a broad term, is that there are many types of digital wallets which may require different regulatory approaches – and this is also reflected in the fact that the failure of different types of digital wallet would pose very different risks to each other – for example, a failure of a self-hosted wallet or small digital wallet provider would likely pose harm on a vastly different scale to the failure of a widely used BigTech wallet.

As noted throughout our response, the many different types of digital wallets have unique use cases, technical compositions, and risks, and wallets used in the crypto and digital assets ecosystem are vastly different from the wallets used broadly for payments such as ApplePay and GooglePay set out in the CfI. As such, and given they perform a different market function, we would urge the FCA and PSR to consider how future regulatory treatment can be

proportionate and appropriate. One-size-fits-all regulation for ‘digital wallets’ as defined could create an unlevel playing field for crypto and digital asset markets. We caution the FCA and PSR against applying rules to “digital wallets” in an overly broad manner that extends the same regulation to self-hosted wallets and wallets that rely on centralised intermediaries.

As noted throughout our response, there could be significant harm caused to freedom of competition, consumer choice, and privacy, if the FCA and PSR impose similar regulatory requirements for all types of digital wallets.

*13. We are interested in how the growing use of digital wallets, and the allocation of responsibilities between parties involved in transactions, affects the security of payments. Your response might include consideration of the following questions:*

- *Do security features such as biometric authentication mean that digital wallets are less prone to fraud than alternative means of payment? Alternatively, do the speed and convenience of using digital wallets to make a payment make them a greater target for fraudsters? What evidence is there regarding the impact of digital wallets on the incidence of fraud? Big tech and digital wallets: Call for Information CP24/9 Payment Systems Regulator July 2024 29*
- *Does the current responsibility/liability model for payments initiated by pass-through digital wallets, set out in Chapter 6, provide the right incentives and controls for parties involved in transactions to implement appropriate anti-fraud measures?*

*We are interested in both the benefits and risks of digital wallets, arising now or in the future. Where possible, please provide evidence to support your answer.*

*14. What do you think are the likely impacts of digital wallets integrating with open banking – for example, in terms of users’ access to financial services, security, or any privacy issues that may arise?*

*15. Are there any significant issues in relation to consumer rights and protections that could become relevant in the future? For instance, how significant is the risk that payment firms start to introduce new payment services through digital wallets that could disadvantage consumers without smartphones?*

We agree that this is a risk. First, it is important for education to continue in parallel to digitisation in order to support future generations and narrow the divide in generational digital skills. Yet, additionally consumers should also retain their choice of which payment products and systems to use, be that physical currency, cards, or digital wallets. It is important that throughout the process of digitisation that choice and accessibility remain so as not to cause harm to consumers or leave any in the UK without access to fundamental banking rights. In that regard, we support existing work streams by the Bank and England and FCA to ensure continued access to cash.

We would still support a variety of different digital wallet options can in turn support improved outcomes for financial inclusion and benefit consumers that may have different needs. As noted above under Q12, outcomes focused, proportionate regulatory treatment will support diversity and innovation across wallet providers and will protect competition as well as consumer choice. In addition, robust competition in the digital wallet market should also spur on innovation in the market for analogous non-digital services, just as new and innovative digitally focussed

banking offerings have arguably led to increased innovation by traditional banking providers in order for them to remain competitive.

***16. Do you consider that the current regulatory framework is effective, so that digital wallets develop and work to promote the best interests of service users? If there are any current or future potential harms that you consider could be mitigated through changes to regulation, please explain what these are and provide evidence to support your answer.***

We would note that first, emerging frameworks should be technology neutral and future proof as the digital wallet ecosystem is fast evolving, but that also as discussed throughout this response that different types of digital wallets may require different regulatory treatment. This is particularly important for self-hosted wallets which are owned and controlled by the end service user. It would be disproportionate to apply regulation for Big Tech companies to the end consumer, or to other types of digital service provider with different risk profiles.

***17. Please share any further views or evidence on digital wallets and their impact that are not captured by your responses to the previous questions.***

We would reiterate that it is important for the FCA and PSR to consider how this framework will be linked to other digital regulatory frameworks such as those for crypto and digital assets. As discussed throughout the response, it is important for these evolving regimes to support responsible innovation while also seeking the appropriate regulatory outcomes. We are supportive of a comprehensive and future-proof regulatory framework as the financial services industry continues to digitise.