Which?
2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

11 September 2026

Consultation response

Which? response to Retail Payments Infrastructure Board (RPIB) consultation on the Design of the Future Retail Payments Infrastructure

Summary

Our main recommendations for the RPIB:

- **Prioritize public needs through strategic central direction:** The Future of Payments review and the National Payments Vision (NPV) identified that reliance on industry consensus to deliver payments innovations had resulted in regulatory congestion and delivery paralysis, and that greater central direction was required to coordinate activity. The Bank of England must provide this strategic direction via its leadership of the Retail Payments Infrastructure Board (RPIB) and in so doing it must ensure infrastructure design prioritizes public policy and societal needs over commercial interests.
- **Ensure consumer needs drive RPIB decisions:** Current efforts to capture the consumer interest in development of the new payments infrastructure fall short and threaten to undermine the NPV's core ambition to ensure consumers have a choice of payment methods that meet their needs. The RPIB must demonstrate that its actions will deliver what consumers want and need from payments.
- **Embed financial inclusion by design:** While payments currently work well for most, the advent of a new retail payments infrastructure presents a once-in-a-generation opportunity to build a system that works for everyone, including those currently excluded or underserved. Experience confirms it is unrealistic to expect commercial firms to deliver these financial inclusion objectives of their own volition. Financial inclusion must therefore be established as a standalone design principle, backed by a clear regulatory mandate. Adding this explicit principle will ensure the infrastructure is built from the ground up to facilitate accessible payment options for all.
- **Build security into the system's core to prevent fraud:** We need a step-change in fraud prevention. The new core infrastructure should offer built-in fraud prevention across all payment methods, featuring capabilities such as enriched messaging standards for real-time risk signaling, universal access to fraud analytics for all payment firms, and improved traceability and coordination mechanisms to detect, prevent, and reverse fraudulent transactions.
- **Design future-facing features with built-in safeguards:** Agentic, programmable, and delegated payments offer a range of potentially useful features for consumers. To ensure they deliver on their promise, they must include effective consumer safeguards and provide simple, customizable tools to empower consumers and allow them to retain control over their finances.

- **Design the core infrastructure to enable future consumer protections:** Ensure the infrastructure acts as the foundational platform, providing the necessary functional building blocks to facilitate robust protections. This ensures that future scheme rules and governance can implement safeguards from day one, rather than attempting costly, reactive retrofits later. This approach also helps to foster the consumer confidence necessary for adoption of new payment methods.
- **Match the reliability of cash:** Reliability of digital payment methods must match that of cash; the RPIB must demonstrate how digital methods will withstand extreme technical failures, cyber-attacks, and connectivity outages.

Introduction

Which? welcomes the RPIB consultation, which represents an important step in delivering the National Payments Vision.

To capture what consumers want from a future payments system, Which? conducted a groundbreaking public dialogue in Autumn 2025 with 41 consumers. Over 14 hours of in-depth discussion these participants explored their payment preferences, and what they want from future payments. Our response is informed by the report based on the public dialogue, *Payments: The consumer desire for control*, as well as the Consumer Vision for Payments, which sets out design principles and priorities for the RPIB to take into account, and which has been endorsed by a range of consumer organisations, including Which?.

Main points

The Bank of England must provide clear, consumer-focused strategic direction for the future retail payments infrastructure. Our research shows consumers expect the government to guarantee the resilience and direction of these essential systems. The Bank must ensure its design meets public policy and societal needs, rather than serving narrow commercial interests.

The RPIB must ensure consumer needs drive decisions about the development of the next generation infrastructure. It's imperative that what consumers want and need from payments is heard and reflected in what is developed. Both the NPV and the PVDC Strategy made this ambition clear, for example the Strategy asserted that it *"has been developed with the needs of users, including those of end users, at its core."* The RPIB consultation helpfully asserts that *"the high-level design must be grounded in the concrete outcomes we seek for UK households and businesses*". However, the current governance structure is not set up to deliver this and risks repeating historical mistakes - where infrastructure development was dictated by payments institutions rather than consumer needs. In particular, the RPIB has no consumer representation but is made up of industry representatives and regulators. Meanwhile, the Payments End User Forum, which focuses on the needs, experiences and perspectives of those who rely on payment services is purely advisory. The RPIB must ensure that consumer requirements are not only heard but act as a central driver of design decisions.

Our public dialogue with consumers about the future of payments revealed that members of the public are able to quickly grasp complex payments topics, assess trade-offs and conflicts, understand the different drivers which motivate actors in the payments ecosystem, and suggest pragmatic and realistic ways forward. Engaging with a cross section of consumers should be a mandatory and integral part of the policy and design process and there should be a clear line of sight from this to priorities for the future retail payments infrastructure. Earlier this year the Bank commissioned focus groups with members of the public across the UK to determine what images should appear on the UK's banknotes. We'd like to see similar efforts to seek out and take consumer views into account when making decisions about the next generation infrastructure, in particular, we would welcome:

- plans for more proactive and meaningful engagement with consumers and their representatives;
- clarity about how consumer views will be taken into account and acted upon by the RPIB when making decisions about the design of the future infrastructure; and
- the publication of measurable outcomes so that progress in delivering functionalities that benefit consumers can be monitored.

The future payment journeys supported by next-generation infrastructure highlighted in the RPIB consultation reflect many of the priorities identified in both the Which? payments research and the Consumer Vision for Payments. When considering these next generation retail payments, the RPIB should focus on improvements that make a clear positive difference to consumers' lives.

Our research surfaced a number of improvements that consumers want to see to *existing* payments journeys which should be taken into account when considering infrastructure upgrades. In particular:

- consumers were frustrated by weekend Direct Debit delays and prolonged 'pending' payment statuses. To address these issues, **the new core infrastructure should be designed to process, clear, and settle all retail payment types (including recurring batch payments like Direct Debits) instantly, 24/7/365**. In addition, the messaging layer must be capable of sending immediate confirmation of settlement back to the access/end-user layer so banking apps can provide consumers with absolute, real-time certainty about when money has left their account.

- currently, hidden Continuous Payment Authorities (CPAs) cause consumers to lose financial control, and can result in them making unwanted and unexpected payments and struggling to cancel them. Consumers want to easily see and manage recurring payments; during our research they were therefore very interested in the potential offered by commercial Variable Recurring Payments (cVRPs). Insights from a cVRP pilot conducted by Moneyline, a not-for-profit social lender, show clear benefits for customers, with 87% of consumers saying VRPs give them greater flexibility and 84% preferring VRPs to direct debits. While we acknowledge there are already positive developments underway to roll out cVRPs, **the future retail payments infrastructure must be optimized for cVRPs, and accompanied by purchase protections for all types of Open Banking payments**. For example, the messaging standard should allow consumers to view the exact mandate parameters, modify limits, and easily revoke consent for subscriptions or recurring bills directly from their banking interface, effectively eliminating the "hidden CPA" problem.

While consumers are excited about the prospect of enhanced control offered by cVRPs, they remain deeply concerned about the lack of purchase protections which currently apply to all types of Open Banking payments, and which mean they are potentially exposed when things go wrong (e.g. due to firm insolvency or retailer disputes). Consumers place a high value on payment purchase protections (e.g. chargeback and Section 75) regarding them as a crucial last line of defence. Yet, eight years after the launch of Open Banking - and despite repeated calls from regulators and authoritative commentators for reform - these payments still lack basic purchase protections, even as usage has continued to grow, and the PVDC confirming it sees the expansion of such payments at the point of sale as a priority.

We recognise that the RPIB has stated the new core infrastructure itself will not create a new consumer protection regime. However, design choices made now must ensure that the core infrastructure enables consumer protections to be integral components from the outset and to be applied consistently in all types of payments.

Reflecting the need to maintain confidence, a baseline of payment purchase protections should form an integral part of the initial build of any payment methods which may emerge rather than being relegated to something that may - or may not - be added at a later date. Integrating these safeguards at the outset is essential to foster the consumer confidence necessary for widespread adoption. Furthermore, this approach prevents the need for costly, reactive retrofits initiated only after consumers have already suffered avoidable harm due to a lack of protection.

The next generation retail payments infrastructure should also offer something better to consumers. Our public dialogue with consumers surfaced an appetite for many of the possible future payment journeys highlighted in the RPIB consultation, including:

- **Alias-based payments -** The Future of Payments Review called out the process of manually entering a sort code and account number to make a person-to-person payment as *"clunky"*. While some banks have innovated in this space, for many consumers the current process for setting up a new payee remains a source of frustration. The new infrastructure must replace this process with seamless, alias-based payments. The RPIB should prioritize infrastructure that improves user experience without sacrificing security - the solution must demonstrate to consumers that a simpler, alias-based process is not only more convenient but inherently safer and less prone to user error than existing methods.

- **Advanced delegated payments** - Our research found there is strong consumer appetite for features that allow people who need extra help with their money to safely give trusted individuals limited, controlled access to their funds. Currently, many vulnerable users are forced to adopt risky workarounds like sharing personal credentials, which significantly increases their vulnerability to fraud and financial abuse: recent research entitled 'Hidden Heroes' by Devon Fields Consulting has highlighted this issue, observing that nearly one-in-five (19.3%) of the UK adult population helps others with digital banking tasks yet 54% of helpers are providing help without any formal authority, often resorting to risky workarounds, such as sharing passwords or security codes and using their own devices to log in on someone else's behalf. Consideration should be given to how such functionality can be built into what is developed in order to enable widespread dissemination.

- **Programmability / conditionality -** Participants in our research were interested in conditionality (e.g. where a payment is made only after specific, pre-agreed conditions have been met such as an item being delivered) and reversibility of payments (e.g. where payment can be cancelled, allowing funds to be returned to the payer, if goods have not been received or are not as described) as mechanisms for improving their control of payments, suggesting that these may in future offer alternative or complementary ways to offer appropriate levels of purchase protection. As the RPIB considers the development of the future retail payments infrastructure, it should explore how to embed such functionality. Doing so would help to ensure that a consistent approach is developed, meeting the demands of consumers that all payment methods have a consistent baseline of payment purchase protections.

- **Deferred payments -** Consumers from our research were interested in how payments innovations could offer the benefits currently associated exclusively with cash, such as allowing offline payments. Even those consumers who rarely used cash to make payments in their everyday lives viewed cash as essential as a backup payment method when digital payments were not available due to problems with connectivity or system-wide outages.

  > *"But one thing I do like about [cash] is that you can just sort of keep it in your back pocket and it's something that you can kind of rely on in a way. And if your phone dies or something, then you can't use Apple Pay, that kind of thing, whereas [cash] you can kind of rely on it a little bit more."*
  >
  > ***Participant, Bristol, W1***

  As decisions about the future payments framework are made, it is imperative that the payments infrastructure is developed to allow consumers to make payments when there is low network connectivity or temporary loss of connectivity, which will be made once connectivity is restored. Enabling such functionality would help to give consumers confidence that digital payments offer a level of resilience that is currently lacking, and which may currently act as an impediment to encouraging people to rely on digital payments.

- **Agentic payments -** There is currently much excitement about the potential offered by agentic payments. Enabling such payments may offer a range of benefits to consumers, allowing them to delegate the effort involved in identifying the best deals and eliminate checkout hassle by allowing personalized AI assistants to, for example, buy household essentials, switch utility tariffs, or rebook travel securely within strict spending guardrails set by the user. While this currently remains a nascent area, it will be important for the future payments infrastructure to enable such payments but, importantly, to also integrate effective safeguards built in by default.

  In our payments research, the majority of consumers feared that frictionless payments would lead to them losing control and cause overspending. To address this risk, the core infrastructure must support complex, conditional logic and granular consent limits for agentic payments (e.g. *"AI agent can only spend up to £50 on groceries"*). Furthermore, the infrastructure should allow users to proactively inject friction - such as mandatory multi-factor authentication prompts for certain thresholds - so consumers retain control over automated processes.

Financial inclusion must be added as a standalone design principle. The PVDC Strategy expressed an ambition for infrastructure to be "inclusive by design" and support diverse needs. Unfortunately, this ambition has not been matched by the RPIB consultation which fails to make clear how the PVDC's ambition on financial inclusion will be turned into tangible action. This is a major oversight and one that must be addressed by adding a further design principle: that the future infrastructure must have at its heart the ability to foster and deliver financial inclusion. This is not about expanding the range of payment options open to the already well-served consumer segments. Rather, it's about tasking the new infrastructure with an explicit task to facilitate the expansion of the payment options offered to those consumers who currently struggle to access, or to use, existing payment methods. This view was voiced strongly by participants in the Which? payments research:

> *"Most of the time, participants didn't see an overarching need for greater choice in the payment options open to them individually. Instead, participants felt that greater choice should be deployed as a tool to ensure that payments become more accessible and inclusive, delivering greater control to a wider range of people."*

As the Consumer Vision for Payments notes *"For most people, payments already work well. The opportunity isn't about serving the same people's needs slightly differently on new technology. It's about inclusive design that removes key consumer pain points, builds financial resilience and drives new value both for consumers and society."*

Financial inclusion needs to be included as a standalone design principle or it will not happen. It is not realistic to expect commercial firms to come together to deliver financial inclusion objectives of their own volition. Experience suggests that a legislative / regulatory mandate is required, as was the case in relation to the provision of basic bank accounts and in the Competition and Markets Authority's Open Banking mandate. As well as building infrastructure that has an explicit obligation to facilitate products that are designed inclusively, the RPIB should think about how to ensure take-up by those reluctant to use digital payments. Consideration should be given to how to connect such products with human support so people can learn how to use them, build confidence and feel included.

In terms of the other proposed Design Principles, we make the following observations:

- **Platform for innovation and competition -** We agree that the core infrastructure should be designed to be modular and extensible. The process for renewal of the payments infrastructure should be dynamic and responsive to changing consumer expectations and new technology. The renewal of the retail payments infrastructure should not be a 'one and done' activity, with what is developed then allowed to stagnate. Rather, once an initial programme of infrastructure renewal is agreed, the PVDC and RPIB must ensure there are regular reviews of the state of UK payments infrastructure, with mechanisms put in place to enhance what is offered over time, in line with changes in consumer expectations and technological developments.

- **Security and resilience** - Consumers expect digital payment systems to withstand extreme events and system-wide outages. Since the system is critical for day-to-day life, the core infrastructure must deliver a level of resilience that matches the reliability consumers currently find in cash, ensuring the system remains operational even during disruptive technical failures or cyber-attacks.

  > *"I don't think with digital payment it can 100% work all the time. I genuinely don't think that that would be possible, because…it's digital."*
  >
  > **Participant, Bristol, W4**

  Despite being sceptical that resilience can be purely delivered through digital means, participants were open to solutions developed by industry to address challenges to resilience which can be experienced when making digital payments.

  At a system level, resilience of payment systems is critical - consumers need to be able to depend on them. Recent high profile cases of cyber hacking have shaken people's faith in digital systems. Indeed, a report by LINK found that two-thirds of people report experiencing a "payments failure" and a third of all those surveyed say they have experienced a system outage of some kind. Since the resilience of the payments system is extremely important to consumers, they expect it to be able to withstand extreme events and emergency situations. Currently consumers simply do not believe that resilience can be achieved through digital means. As long as this remains the case then the demand for cash as a store of value - kept by consumers 'just in case' - will endure. The RPIB should reflect upon this and consider:
  - how to retain cash as a core component in delivering resilience and interoperability; and
  - how new and emerging digital payment methods can be designed to help the millions of consumers who currently prefer to use cash to feel more comfortable and confident in using digital payments. Compelling evidence will be required to convince consumers that such payments can be relied upon so that the future core infrastructure continues to work even during disruptive events, such as high-severity cyber-attacks, prolonged third-party outages and technical failures.

- **Protection from fraud and wider financial crime -** Fraud is now the UK's largest category of crime and is costing our economy £14.4 billion in 2023–2024. Industry figures reveal that fraudsters stole £1.28 billion through payment fraud in 2025. But fraud also has a profound, hugely detrimental impact on consumers - it causes enormous amounts of consumer harm and impedes people's willingness to make, or transition to, digital payments. It is therefore unsurprising that the UK's Fraud Strategy makes clear that *"tackling fraud is essential to cutting crime and strengthening economic resilience."* Robust security is the fundamental bedrock of consumer trust and control in payments. The upgraded retail payments infrastructure has a critical role to play in combating fraud. The RPIB should recognise the scale of this challenge and seek to prioritise development of tools and functionalities which will help to design out fraud at the infrastructure level.

Historical challenges with Authorised Push Payment (APP) fraud reimbursement highlight the limitations of relying on individual firms to tackle systemic risks. System-wide action is necessary to prevent avoidable consumer harm and reduce disproportionate costs for firms leading the fight against fraud.

Enhanced capabilities should be introduced at the core infrastructure level to deliver a step-change in the ability to detect and prevent fraud, and to trace fraudulent payments and reverse them. The need will become more pressing over the coming years. As the recent Mills Review on AI and the future of retail financial services observed, AI will amplify fraud and cyber-risks by 2030 as they become faster, cheaper, more scalable and more persuasive, and *"capability therefore needs to evolve at system level, across firms, sectors and public authorities, particularly where no single organisation has the visibility, data or operational reach to act alone."*

Adopting this approach could help provide a uniform baseline which raises the defensive wall for the entire payments system, and enable system-wide fraud monitoring and disruption so that data is more easily shared, threats identified and dealt with. Getting it right also offers the potential to cut the reimbursement bill.

The RPIB consultation sets out design considerations that could be offered by the new core infrastructure to help tackle financial crime and fraud. We strongly support the introduction of functionality at the core infrastructure which would enable:

- **Consistent fraud and wider financial crime prevention across interoperable payments.** We have seen major improvements in efforts to prevent fraud across certain payment methods (e.g. confirmation of payee) but application is limited to individual payment methods. The discrepancies in the level of protection offered can be confusing to consumers, and also allow fraudsters to migrate activity to those payment methods with less developed preventative measures. In an increasingly diverse multi-money ecosystem, where there is interoperability between new and existing forms of digital money, there is a strong need for a more consistent and joined-up approach to fraud prevention which should be grounded in the new core infrastructure.

- **Better data to support prevention and detection.** Current data sharing initiatives, while welcome, are too often fragmented and piecemeal. Businesses can cite data protection concerns or commercial competitiveness for failing to fully engage with data sharing initiatives intended to prevent fraud. The redesign of the retail payments infrastructure offers the opportunity to improve and enhance data sharing to significantly boost efforts to detect and prevent fraud. We suggest the RPIB design the new core clearing and messaging infrastructure to mandate the exchange of enhanced fraud data as a fundamental scheme rule. Baking data-sharing standards directly into the core infrastructure offers the potential to remove the legal ambiguities and commercial disincentives that can currently hinder cross-Payment Service Provider (PSP) collaboration.

The RPIB should also consider how the core infrastructure can deliver improved messaging standards so that richer data payloads accompany payments, potentially highlighting risk signals (e.g. a flag indicating that a payment was initiated via a social media platform link that appears high risk).

Embedding fraud data analytics as a common utility via core infrastructure would also help to ensure all PSPs - no matter their size - have access to fraud intelligence, providing a baseline of protection for all consumers.

Finally, the new infrastructure will occupy a privileged position in seeing the entirety of payments. The RPIB should consider how it can safely share aggregate macro-level, anonymised intelligence about fraudulent payments with law enforcement and Report Fraud to tackle organised crime at scale.

- **Improved traceability and co-ordination when things go wrong.** Which? has been at the forefront of campaigning for better protections for consumers who are victims of fraud, including pushing for mandatory reimbursement for APP fraud. Ideally, fraudulent payments would be prevented in the first place. Where this is not possible, payments should be traceable, with fraudulent payments able to be swiftly investigated and recovered, potentially reducing the need for reimbursement schemes to protect consumers.

- **Default safeguards for new and emerging payment journeys.** Our payments research revealed that consumers are interested in the possibilities offered by payments innovations such as programmable payments. However, to convince them to try new payment methods or functionalities there is a need to ensure that they feature effective safeguards that are built in by default. We cover this point in more detail above when setting out the need for a baseline of payment purchase protections to feature as an integral part of the initial build of any other new payment methods which may emerge.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

For more information contact:
Tony Herbert, Senior Policy Adviser
tony.herbert@which.co.uk
September 2026