HM Treasury

Payment Services Regulations

Review and Call for Evidence

Response on behalf of Barclays Bank UK plc and Barclays Bank plc

April 2023

Submission by Barclays

Barclays is a universal consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management. With over 330 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

We welcome the opportunity to respond to HM Treasury's consultation on the review and call for evidence on the Payment Services Regulations.

Executive Summary

Barclays strongly supports policymaker efforts to ensure the UK has strong, efficient and resilient payment networks that provide consumers and merchants with a choice of innovative and safe payments options. As such, it is positive that the government is looking to review the current payments regulatory framework, in order to identify emerging risks and potential opportunities to improve the landscape going forward.

SEPA Participation

The opportunity to review the payments regulatory framework in the UK is welcome. However, it is crucial for the UK's ability to compete internationally that the UK must continue to be a leader in the movement of money around the world. Central to this is the UK's access to SEPA. Throughout this response we have highlighted that, whilst there may be opportunity for divergence from the framework of EU regulation (primarily the Payment Services Directive), there is a careful balance to ensure the UK does not become too estranged to such an extent that it no longer meets the SEPA equivalence standards. We strongly encourage government to have continued dialogue with the European Payments Council and further consultation before settling on any changes impacting the payments landscape to ensure any divergence does not impact the UK's ability to compete in the global market.

Movement towards FCA Handbook rules

We would be supportive of conduct and information requirements in the PSRs being moved to FCA Handbook rules/guidance. The current construct of regulation means changes cannot progress with effective agility due to the need to having to follow a legislative process. It also means much of the development and expansion on the requirements set out in the PSRs is dispersed across the FCA Approach Document and the FCA Perimeter Guidance, with guidance on other areas like the Cross Border Payment Regulations being limited to that provided at a European level.

Provision of Information

The concept of a framework agreement, and the requirements and specificity of what and how information must be provided to customers is cumbersome and dose not deliver a real customer benefit. The FCA Consumer Duty is much more intuitive in guiding how firms can convey information to customers to help customers understand the information being provided to them across a range of medium. We ask for reform in this area to bring the provision of information requirements in the PSRs up to date with other forms of regulation.

Fraud

The provisions in the Payment Services Regulations protecting customers from fraud are now outdated. The pace and agility at which fraud evolves means that naturally firms are trying to catch up with the practices of fraudsters, and working within an outdated framework is limiting. The PSRs do not envisage authorised push payment fraud, and only deal with unauthorised transactions, or transactions made through use of incorrect unique identifiers. This has left a regulatory vacuum and consequently a vulnerability that can be exploited. Whilst there are some conduct requirements for firms regarding unauthorised transactions, there are very limited conduct requirements for firms regarding authorised push payment fraud, such as payment warnings; customer education; obligation for remitting firms to make recovery attempts; obligations for repatriation; and obligations for data sharing. We recommend authorised push payment scams being put on the same regulatory footing as unauthorised transactions, with the same caveats that we made in our response to the PSR Consultation,[1] in particular with a replacement of the gross negligence standard.

These requirements do not need to be embedded in legislation, and would be more appropriate in FCA Handbook rules which could easily be amended and updated.

We reiterate the need for government to take a holistic view of the prevention of fraud and scams. We stress the importance that liability must be shared across the fraud and scams eco-system to incentivise all parties (not limited to financial services) to take preventative action to prevent fraud and scams from happening.

Strong Customer Authentication

The prescriptiveness of the Strong Customer Authentication Regulatory Technical Standards does not necessarily lead to better fraud outcomes in a way that granting firms the autonomy to develop risk based controls could. Reform could remove friction in a payment journey without compromising on security and safety. We ask for less prescription in this area, with a focus on outcomes based regulation allowing firms the discretion to design their own fraud prevention controls and authentication standards depending on their metrics, including customer type and type of transaction. As demonstrated through the adoption of 3D Secure across the industry, firms are already incentivised to act to reduce their volumes of fraud, and will collaborate and work together without this having to be specifically instructed by regulation. Potentially, with regulation being so prescriptive and standardised, it is easier for fraudsters to predict how firms will behave.

Open Banking

Paragraphs 51-58 in the Call for Evidence set out that Open Banking will be considered as part of JROC's work and that government is not considering the development of Open Banking as part of this review. Notwithstanding this, and acknowledging that we are still waiting for the outcomes from the JROC work and its finalised recommendations, we have taken the opportunity to remind government of the need for the work to transition Open Banking to the future entity to happen at pace. Regarding the roadmap for Open Banking, we reiterate (alongside our separate responses and engagement with SWG and JROC) the need for the future evolution to be balanced, fair and proportionate. It is important that a customer need is identified, allowing firms to design a service that delivers fair value in accordance with the new FCA Consumer Duty.

Payment Services and Corporate Clients

[1] CP22/4

The definition of micro-enterprises is not only difficult to apply (which creates inconsistency in its use and application), but is not the right test as to whether an entity should receive protections under the regulatory framework.

Consultation Questions

General Questions

1. **How should the payment services framework evolve – and what should be the government's priorities – to better promote the following government objectives for payments regulation:**

A. Achieving agile and proportionate regulation, which facilitates the international competitiveness of the UK economy through growth and innovation in the UK payments sector

B. Ensuring appropriate trust and protection for consumers

C. Ensuring the resilience and integrity of the UK's payment market

D. Fostering competition, in the interests of consumers

In answering the above, the government would welcome concrete reflections from stakeholders for future policy, rather than the principles which should underpin regulation/regulatory change.

Given much of the payments regulatory framework has been shaped by the Payment Services Directive, we welcome the opportunity to review its adequacy against the developments in the payments sector to see how we can foster competition and innovation whilst maintaining resilience in the UK.

Payments are international, and that is only accelerating. Therefore, the language of payments, the established processes, and the information that must be transmitted with a payment are all becoming even more standardised globally to better facilitate cross border payments. In light of this, and in light of the government objectives set out above, review of the framework of payments regulation (including Payment Services Regulations, Cross Border Payment Regulations and Wire Transfer Regulations) must be done against a comparison of its European equivalents to ensure any divergence does not impact the UK's ability to compete in the global market. Any regulatory developments must continue to support payment system interoperability to allow Payment Service Providers (PSPs) from different systems or jurisdictions (SEPA/nonSEPA) to exchange payment data, and clear and settle payments across systems securely with minimal friction. Practically, many Corporate clients will have European entities; providing banking and payment services to these clients will become overly complex and cumbersome for them as a payment services user if the UK departs from the EU regulatory framework.

The government is aware the UK's continued SEPA participation following the UK's withdrawal from the European Union is contingent on our continued compliance with the participation criteria. This includes a country legal opinion to demonstrate that UK on-shoring of EU laws met the equivalence standards required. However, this legal opinion is only valid for the laws that applied at that time and so we ask that the government includes in its assessment criteria for any new payment regulations the potential risks to the UK's continued participation in SEPA and seeks the views of industry and regulators before proceeding with any changes that endanger that participation. Whilst smaller changes to payments regulation may not impinge on our SEPA participation (for example, our increased contactless limits), any more fundamental change to payments regulation could impact our SEPA participation.

The framework is currently made up of various pieces of regulation which includes conduct requirements. In reviewing this framework, we would be supportive of moving these into FCA

Handbook rules/guidance which would allow them to be more agile and respond to industry developments more easily than a legislative process.

2. **To what extent would you support rationalising and/or removing the distinctions in regulation between payment institutions and electronic money institutions – in effect, combining the two sets of legislation? Would this be easier for the sector to navigate and/or lead to better outcomes?**

Barclays has no strong views in relation to this section of the consultation paper.

Scope and definitions

3. **Are (a) the definitions and (b) the scope of the regulated activities in the payments services and e-money framework clear and do they capture the right actors and activities within regulation?**

There are some terms that could benefit from a clear definition, whether this is in FCA Handbook glossary or perimeter guidance:

Provide, make available, and durable medium	Interpretation of what is meant by these terms, and the requirements for something to meet the test of "durable medium" has been led through EU case law[2]. If these terms are to be used in any future payments regulatory framework (and we do not think this should be an assumption - see our response to Question 10), it would be helpful to have clarification on the meaning of these terms to give firms more certainty as to their application. It is also a welcome opportunity for the UK to review the original decision in the CJEU case to see if this is still appropriate with developments in this area.
Immediately /as soon as possible	It would be helpful to have guidance on the practical implication and meaning of these terms, including examples of what is/is not likely to meet these definitions.
"Regular occupation or business"	PERG 15 Q9 provides guidance on the scope of the PSRs and what activity is likely to amount to "regulated activity" which requires a business to be authorised or registered under the PSRs. It sets out that it is only where activity is carried out *"as a regular occupation or business activity"*. Whilst some examples are provided, it relies on a subjective interpretation. Further guidance would be helpful to aide understanding of potential regulatory obligations. We would also welcome confirmation to provide assurance to ASPSPs that they are not required to perform their own regulatory assessment of another party.

We consider the European notion and definition of "micro-enterprise" is not the optimal test for applying consumer protection to relevant businesses. There are a number of reasons for this which include:

1. UK businesses tend not to be familiar with this term/concept, and therefore they are unable to know when they should receive 'micro-enterprise' protections. Explaining to a successful,

[2] (BAWAG PSK Bank v. Verein Fur Konsumenteninformation (Case C-375/15))

small business that they are a 'micro-enterprise' also potentially has pejorative connotations, as this sounds like the successful business they have built up is a 'hobby business'.

2. The test for a micro-enterprise is based on European law (enterprise meaning an entity engaged in economic activity for the purposes of EU law), and therefore does not translate well to English trust law (e.g. trusts, pensions, associations).
3. The test applies a foreign currency (euro) which fluctuates with Sterling, and requires the bank to apply foreign law ("Recommendation 2003/361/EC of the Commission of 6th May 2003 concerning the definition of micro, small and medium-sized enterprises") in more complex cases.
4. Although it is possible to consolidate company structures in some instances, a sophisticated business may deliberately create a structure (e.g. an SPV held by a trust) that means group data cannot be combined, and the SPV must be treated as a micro-enterprise. This is likely to deny this SPV access to banking products (for instance, given micro-enterprises must be given 2 months' notice of interest rate changes, it means they may end up with interest bearing products with a lower interest yield).
5. The FCA applies a different test for "micro-enterprise" in different regulatory texts. For instance:
    - In the FCA Handbook it is: "an enterprise which: (a) employs fewer than 10 persons; and (b) has a turnover or annual balance sheet that does not exceed €2 million,".
    - Whereas in the PSRs ""micro-enterprise" means an enterprise which, at the time at which the contract for payment services is entered into, is an enterprise as defined in Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC of 6th May 2003 concerning the definition of micro, small and medium-sized enterprises(e).
6. The test is based on matters including "Annual Worker Units". This excludes, for instance, employees on maternity or parental leave. It is difficult for firms to maintain an accurate insight into a company's data across the year (for instance, how is the bank supposed to know if a company with 10 staff has two on maternity leave), and therefore it is difficult for banks to be satisfied it has applied the test accurately. Businesses may also not want to be classified as micro-enterprises if they understand they may not be eligible for certain products, and may therefore not provide the bank with accurate information.

We recommend that any proposed amendment to this definition is subject to separate further consultation and engagement with firms to assess the practical implications of a revised definition and the provision of the ability for corporate clients to self-opt out.

We note the interpretation of "payment account" adopted by the FCA is broader than that adopted in various jurisdictions in Europe and, in particular, includes credit card accounts. This has a number of consequences given the extensive references to "payment account" in the PSRs.

One specific example relates to Regulation 68, which requires confirmation of the availability of funds. While availability of funds is one aspect of whether a payment will be successfully processed, it is not the only one. In addition, there may be some time period between the confirmation of funds response, and the transaction being applied to the card account. Therefore, the confirmation of funds is not always an accurate representation of whether a payment request on the card account will be honoured. This issue is compounded in respect of corporate cards where there are additional controls that are in place which could be bypassed. For example, a corporate client may have restricted the use of the card for certain merchant types (e.g. online gambling) but this could be bypassed through the use of a Card Based Payment Instrument Issuer.

We are also aware that Regulation 69 for payment initiation is impacting on instances where credit card transactions can be used to fund credit transfers, again due to a broad interpretation by the FCA. This means ASPSPs have had to develop functionality for payment initiation services for credit and charge card accounts. We have seen no customer demand for these services and an extension of the regulatory requirements through a broad interpretation is resulting in unnecessary costs for industry, hindering more useful product development.

We would therefore welcome the government's reconsidering whether such broad interpretation continues to remain appropriate.

Further we ask the government includes in its assessment of this appropriateness analysis of whether the original intentions of such broad definitions have been achieved in the several years since the Payment Services Regulations 2017. We consider that government should publish this analysis, as well as its view of the broad definition, in its response to the call for evidence. If the view of government is that the adoption of broad interpretations, as described above, should be unchanged, we would suggest the corporate opt out is extended.

4. Do the exclusions under the PSRs and the EMRs continue to be appropriate (includes limited network, electronic communication, commercial agent etc)?

The exclusions under the PSRs are now outdated as innovation in payments technology has developed at a much faster rate. We therefore think the exclusions need to be reviewed and amended to bring new and emerging types of providers into the framework of payments regulation[3]. Therefore, we suggest that government should consider whether other types of firms, payment processing services, operating schemes and technical service providers (including Big Tech) – should be appropriately regulated where they are deemed to pose a significant stability risk to the payment system.

Equally, the development and expansion of marketplaces[4] means these platforms typically own the infrastructure and contractual relationships to enable payments to be taken from customers. In many instances, marketplaces will hold (and in some instances safeguard) funds and will provide settlement with the supplier, but will not be regulated as a payment institution due to the exemptions to the PSRs and their interpretation of whether this is part of their occupation or business (see also our reference in Question 2 regarding clarification to PERG for *"regular occupation or business").* Given the sophistication of these types of business, and the rate of development in their functionality and the services they provide, we would encourage government to review the need for these to be regulated, with providing clearer guidance as to when and how they are regulated to remove the current ambiguity.

The regulatory treatment of payment services and e-money (Q5-Q9)

Barclays has no strong views in relation to this section of the consultation paper.

Information requirements for payment services

Considered against the government's objectives for payments regulation:

[3] We refer HMT to the Barclays' response to the following separate consultations: *FCA – The Potential competition impacts of Big Tech entry and expansion in retail financial services (DP22/5); and PRA/FCA Operational Resilience: Critical Third Parties to the UK Financial Sector (DP22/3).*

[4] Whilst this term captures a broad range of business models, we refer here to those platforms that operate as an online store enabling third party products to be sold to customers.

10. Is the current framework for the provision of information to payment service users effective? If not, how should its scope change?

We consider the current framework for the provision of information to payment service users to be reasonably effective. Notwithstanding this, there are areas where improvements could be made.

Whilst we note consumer credit has been subject to separate consultation[5], the overlap with the Consumer Credit Act 1974 and the PSRs is complex and creates customer confusion. For example, in respect of unauthorised transactions and a payment service user's liability there are different information requirements set out within the two regimes. We welcome the opportunity for this to be reviewed in this Call for Evidence and in the CCA Consultation, and hope for cohesion to be brought to the intersection in this respect.

We consider the Consumer Duty and its focus on Consumer Understanding and the importance of delivering the right information at the right time to be a better indicator of determining when and what information should be given to customers. We consider it necessary to review the level of prescriptiveness from the information requirements in the Payment Services Regulations, including the framework contract requirements in favour of more principles-based regulation allowing firms to think more holistically about the information needs of its target market. This should extend to consideration of how information is provided to customers, with no assumption that paper, or another durable medium, is the best format.

Regulation 50(1) requires two months' notice before *any* proposed changes to the framework contract. However, the reality is that not all changes require the customer to know about it a) two months' in advance or; b) in advance at all. As a general principle, firms should be able to give effect to beneficial changes as early as possible. This should be clarified in the regulations to ensure firms can pass on beneficial changes to payment users without incurring regulatory risk. More specifically, firms should also be able to make changes to information contained in a framework contract, the content of which is prescribed by Schedule 4, at varying amounts of notice depending on the change and the impact that change actually has on the customer (for example changes to ancillary offerings to payment accounts that are captured by the two months' notice requirement because they are technically included in a "framework agreement"). It is a crude assumption that all potentially detrimental changes are equal, and therefore all require two months' notice when the reality is more nuanced. For example, in relation to foreign currency, foreign currency exchange rates are by their nature variable and fast-paced. It is also an area where customers are free to shop around and there is no barrier to exit. Provided notice periods are agreed at the outset, and in line with the Consumer Duty and the Consumer Understanding outcome, firms should be permitted to communicate changes in foreign currency pricing (and other similarly transparent and competitive areas) at less than two months' notice.

Regulations 53 and 54, essentially the requirements to provide bank statements, is predicated on certain banking transactional information only being available periodically (i.e. monthly), and in a paper format (or a durable medium). The progression and development of digital banking means for a large proportion of customers (accepting not all customers), they will engage with transactional banking information far more regularly than monthly, and they do not see the need or value in a monthly statement in paper or in a durable medium being provided. As an example, c90% of customers accessing their online/App based banking view their transactions, compared to just c7% accessing their banking and viewing their bank statements. The information is always available to

[5] https://www.gov.uk/government/consultations/reform-of-the-consumer-credit-act-consultation

them and so they do not require the provision of a regular bank statement which they cannot decline to receive. Digital advancements have also meant that customers can chose to receive certain transactional information through more interactive means (i.e. SMS notifications). Bank statements should therefore be a choice for consumers as to whether one is provided at all; and a choice as to whether they would like this in paper or a durable medium with no default option to a paper version,.

A further example of where the PSRs are overly prescriptive, firms must provide details of all charges, interest and exchange rates in the framework contract[6]. This would include charges for services that a customer may not want to use which must be included at the outset in the framework contract. Instead of being able to provide information on those charges at the point a customer wants to use a particular service (and importantly still before they do so), firms must include a "shopping list" of all potential charges making the charging information overly detailed for customers and difficult for them to really assimilate. Consideration of right information at the right time, in line with the Consumer Duty principles and outcomes, is not possible as there is an assumption all of this information is needed by all customers at the outset in their framework contract.

11. Are there particular changes that you would advocate to the Cross Border Payments Regulation in relation to the transparency of currency conversion, and what would these entail?

The Cross Border Payments Regulations are by their nature designed with the intention of bringing transparency to internal payments within the euro area. Their relevance to Member States not within the euro has always been stretched. We consider there to be potential for these requirements to be revised focussing on what information is actually useful to consumers in the UK. For example, we question the usefulness to consumers to be informed of the percentage mark up over the most recent euro foreign exchange rate issued by the European Central Bank prior to a transaction taking place. The expectation that a consumer will use this rate and make a comparison at a point of sale is not realistic and in the majority of circumstances is confusing for consumers.

Transparency requirements for outbound FX credit transfers that are made through an interactive channel (online/in app) are achievable. However, providing the estimated amount to be transferred to a payee could fluctuate depending on when an inbound payment is processed which, for firms that use a live rate, is not possible. For example, a customer who enters their payment information in an online interface, and then reviews that information and the currency conversion disclosures required by the Cross Border Payments Regulations, could find that by the time their payment is processed a live exchange rate has changed and the disclosure they had reviewed, which their bank had to provide, does not reflect the eventual position. The provision of the estimated total amount of the credit transfer is confusing to customers, and is an area on which we receive customer complaints, particularly from payees who have not been made aware of the estimate provided.

In our view the government should amend the Cross-border Payments Regulation to allow firms greater flexibility to decide the most appropriate way to deliver information about foreign exchange rates applicable to the payments they are making.

There is reference in the Cross-border Payments Regulation Article 3(b) to "transaction fee". This term is incongruous as there is no other reference in the Cross-border Payments Regulation to a "transaction fee". There is no expansion in the CBPRs as to how disclosure of a transaction fee is supposed to apply in the different charging scenarios (OUR, BEN, SHA) or what accompanying information (if any) should also be provided to explain, for example, how this would apply to BEN or

[6] Para 3(a) Schedule 4, Payment Services Regulations 2019

SHA charging. We would welcome further guidance from government as to the expectation for disclosure of transaction fees in this context.

Rights and obligations in relation to the provision of payment services

Considered against the government's objectives for payments regulation:

12. **What has been the experience of a) providers and b) users/customers in relation to the termination of payment services contracts? Does the existing framework strike an appropriate balance of rights and obligations between payment service users and payment service providers, including but not limited to a notice period applying in such cases?**

The existing legal framework strikes the right balance of rights and obligations in relation to termination of payment service contracts, recognising the need for nuance to cater for the variety of circumstances a firm may look to terminate an account. Our terms and conditions reflect this balance of obligations in accordance with the PSRs and other regulation, for example the Money Laundering Regulations 2019.

As a responsible firm we also want to make sure we give customers enough time to find new banking arrangements wherever the circumstances of the case permit that. Therefore, we consider whether we can give the standard notice of at least two months' notice rather than closing an account immediately. In some instances, with some customer types (financial services providers for example), once we understand their issues, we will look at how we can give more than two months' notice to help them to re-bank.

We have little scope to close an account immediately. Recognising the propensity for this to cause customer harm, particularly for business and corporate customers where the consequences of closing a business account could be very severe, impacting salary and tax payments, and the future operation of the business, we only do this for very limited reasons.

In some cases, immediate closure of accounts is a necessary response to changes in public policy. For example, many firms had to close accounts immediately once governments announced sanctions against Russian individuals and firms.

The current regime sets out further requirements for Account Servicing Payment Service Providers (ASPSPs) when they close an account held by a PSP. Under Regulation 105(3) PSRs we are required to notify the Financial Conduct Authority in a prescribed format, including setting out our reasons for the withdrawal at the same time that we notify our customer of the decision. This gives the FCA greater oversight of how/when accounts of PSPs are closed.

13. **With reference to paragraph 31 of the accompanying review, do stakeholders have any feedback on the government's view: • that, as a general principle, a notice period and fair and open communication with a customer must apply before payment services are terminated? • that the regulations and wider law operate here as set out under paragraph 29?**

Barclays echoes the governments views in paragraph 31 of the consultation. Barclays' terms and conditions reflect the requirements set out in Regulation 51 PSRS, as well as the Consumer Rights Act 2015 where applicable, and the FCA's Principle 6.

As a responsible firm, where we can, we have early communication with customers when we are considering termination of payment services. Where possible, we will work with customers to see if there are changes they can make that mean we can continue to provide services to them.

The Consumer Duty will supplement this. Firms will need to make sure they meet the new principle and the associated cross-cutting themes in all their dealings with customers and meet the four outcomes in the relevant circumstances. For example, firms will further need to consider the effects of harm on customers and the clarity of their communication when taking action, including closing accounts.

14. How and when do providers cease to do business with a user, and in what circumstances is a notice period not applied?

In accordance with the PSRs, Barclays retains the right in its terms and conditions to terminate a contract on the giving of at least two months' notice.

However, there are some limited circumstances when we can close an account on less notice, or even immediately. These reasons are set out in our terms and conditions and include, a customer uses their account illegally, or they put us in a position where we might break a law/regulation/code/duty if we maintain the account.

15. How effective are the current requirements in the Payment Services Regulations, notably under Regulations 51 and 71 – are these sufficiently clear or would they benefit from greater clarity, in particular to ensure that notice-periods are given and customer communication is clear and fair?

The requirements in the PSRs Regulation 51-71 are clear. We also note the FCA's Approach Document, which, although it is not legal text, helps ensure consistency across the industry for these and other PSRs requirements.

Regulation 55 is clear in terms of what it is trying to achieve. However, we would question its continued relevance in light of the FCA's Consumer Duty. The Consumer Duty goes further than requiring that communication is, for example, "made available in English or in the language agreed by the parties"[7] and instead requires a broader look at whether the information is actually information that could be understood by the customer, as well as the timing and method of delivery.

Regulation 71, amongst other things, permits a PSP the right to stop the use of a payment instrument on certain reasonable grounds relating to, the security of the instrument, the suspected unauthorised or fraudulent use of the instrument, or a significantly increased risk that the payer may be unable to fulfil its liability to pay. Given these limited reasons a PSP may stop the use of a payment instrument, we question the effectiveness of a requirement of having to provide prior notice, and whether this is ever actually possible.

Regulation 71(7) allows an ASPSP to deny an Account Information Service Provider (AISP) or Payment Initiation Service Provider (PISP) access to a payment account only for *"reasonably justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account".* However, of relevance to access by a PISP, this does not consider authorised push payment scams where the access to the account has not been unauthorised or fraudulent, but the ASPSP may need to take action. For example, if a PISP has a particularly high volume of APP scams for a customer, an ASPSP

[7] Regulation 55(1)(d)

may have concerns as to the protections being provided to the customer by the PISP, and may need to restrict access from that PISP. In light of the obligations on firms to play an active role to reduce fraud and scams there will be an increasing need for ASPSPs to be able to restrict access for authorised push payment fraud in the same way as they can for unauthorised payments and to be able to do this without incurring an element of regulatory risk for breach of Regulation 71(7). We would recommend ASPSPs can deny access to a payment account for reasonably justified reasons, not limited to reasons relating to unauthorised or fraudulent access.

16. **Should there be additional protections for payment service users against the termination of contracts? Should anything be specific to protect their freedom of expression – e.g. to ensure that adequate (or longer) notice is given in such cases, and what communication requirements should apply?**

We consider the existing limitations to termination of a contract by a PSP to be adequate.

Barclays considers there is no need to change the existing regime. We ask that if the government is considering any such changes, it provides quantitative and qualitative data that support the value of such a fundamental shift and the detriment customers currently face and how its proposed changes will address that detriment. We also ask that government works with industry from the start to understand this issue further.

Wider considerations in relation to the provision of payment services

17. **What provision, if any, should the regulatory framework make regarding charges for payment services?**

In relation to Regulation 66 which sets out the charging rights/obligations, whilst SHA is mandatory for SEPA payments, where possible outside of SEPA, we consider payers (especially corporates) should be permitted to select charging options BEN or OUR. Notwithstanding this, we would not want to jeopardise any continued participation in SEPA and would therefore need to ensure any change in this regard would not breach any aspect of equivalence.

18. **Does the existing framework strike an appropriate balance of rights and obligations between: • Sending and receiving payment service providers? • Account servicing payment service providers and payment initiation service providers/account information service providers?**

The existing framework strikes an appropriate balance of rights and obligations between sending and receiving PSP. However, we do not consider that it strikes the right balance between ASPSP and third party providers. This is demonstrated most notably in relation to PISPs and fraud liability.

Open Banking Payments are currently constructed in a manner where the end to end payment journey is shared between two parties (the PISP and the ASPSP). However, fraud controls are only mandated on one of these parties (the ASPSP). Furthermore, the liability for any fraud that takes place also sits primarily with only one party (the ASPSP) who, due to the nature of the role they play, actually has very little information to be able to effectively apply any fraud controls. There is an opportunity for the bank to ask the PISP to prove that deficiencies with their processes did not affect the "payment transaction". However, this can be viewed as being limited to the PISP merely having to prove that there have not been failings with its technical execution of the "payment transaction", therefore excluding factors such as inadequate KYC/AML and Fraud processes. This imbalance of liability means that PISPs are not incentivised to introduce the necessary controls to prevent fraud and protect

customers, which is particularly relevant to authorised payment scams and the impact this has on the data reporting of a firm's volume/value of scams. A further example of this is the lack of use of Transactional Risk Indicators in PISP initiated payments (see also our response to Question 20 and 21). Therefore, in addition to mandatory controls, a new liability model needs to be introduced that seeks to ensure that the party at fault can be identified and is then the party that is liable to reimburse the victim of fraud.

Additionally, in our direct payment channels, Barclays provides targeted and timely scam warnings to customers, which are tailored based on payment purpose (e.g. a specific warning is provided related to investment scams, if the customer indicates they are making an investment). This is a key opportunity to try to 'break the spell' of the scammer, and alert the customer to consider whether the payment they are making could be a scam. All PSPs should be required to present their customers with effective scam warnings (e.g. targeted based on payment purpose) and an ASPSP should be allowed to include these warnings as an additional step in the consumer payment journey. Whilst there have been concerns from some in industry that this could add 'friction' into the journey, it would be equivalent to what the customer sees when they make a payment through direct channels, and is a vital tool in helping prevent the victim from falling for a scam, therefore is a necessary step. Indeed, ASPSPs are required to ensure alignment between their customer interfaces and the journeys the customer faces with their third-party provider. Not having a fraud warning is not a regulatory breach on the part of the third-party provider but it is inconsistent and should be addressed. In the context of 'friction' in payments more broadly, the PSR note in their consultation on APP Scams (CP21/10, Nov 2021) *'that the small amount of 'friction' being added to payments would be proportionate for increased detection of APP scams and resulting protection from this fraud'*. Therefore, there needs to be an appropriate balance between consumer protection from fraud, and speed for the transaction to go through.

We believe that this imbalance needs addressing, to ensure that all parties are mandated and properly incentivised to prevent fraud. Given the complexities with establishing industry agreement to a liability model for authorised fraud, we consider this can only be achieved through legislative changes. Barclays recommends placing necessary and appropriate mandatory obligations on PISPs (aligned to those placed on ASPSPs), to ensure that there is a consistent approach being taken by all firms – reducing the opportunity for fraudsters to identify and exploit 'weak links' which may not have as strong fraud controls. For example: ensuring the same level of KYC due diligence; PISPs to share certain data points with the ASPSP relating to the payment, to support fraud profiling for these payments.

19. Are consumers adequately protected from evolving fraud threats under the existing legislation – is further policy needed to ensure this, and how should that policy be framed?

We consider that consumers are adequately protected from certain fraud threats under the existing legislation and future proposals.

As an industry, the development of cybersecurity controls has meant that we see lower levels of unauthorised payment fraud. The regulations also ensure prompt reimbursement for customers when they fall victim to unauthorised fraud. However, these regulations do not go far enough to *protect* customers from *authorised* payment fraud, and this is the biggest evolving fraud threat now facing customers.

We support the Payment Systems Regulator's work to enhance the regulatory regime for customers who fall victim to authorised fraud. However, whilst the Payment Systems Regulator is implementing systems rules to provide for mandatory reimbursement of authorised push payment fraud through

Pay.UK, there are limitations with this as to the effectiveness of actually protecting customers from evolving fraud threats. We have highlighted these deficiencies in our response to the PSR Consultations CP22/4.

Mandatory reimbursement is limited to reimbursement only, and will not put authorised fraud on the same legislative footing as unauthorised fraud. It does not seek to actually protect customers from that fraud. However, we do highlight that gross negligence is only relevant for unauthorised transactions because the customer is not physically making the payment and so they cannot be expected to play a role in preventing the payment from happening. It is not the right level in the context of an authorised transaction because the customer has made it themselves. Setting the standard of care expected of a customer in how they manage their own financial affairs and well-being cannot be set at such a low level that consumers can in effect abdicate any personal responsibility. We would also encourage a review of how authorised scams and unauthorised transactions are treated under the Financial Ombudsman Service with a greater education of the importance of the role a customer plays in protecting themselves, where possible, from the risk of fraud.

The amendments to the Financial Services and Markets Bill only enable the PSR to implement mandatory reimbursement; the PSR by its nature has a limited scope that only extends to financial services, and those using the Faster Payments scheme. To have any meaningful way of protecting consumers from being victims of scams, opposed to focussing solely on reimbursement through the PSR and Pay.UK, only the government is able to take a holistic look at the fraud ecosystem and seek to engage other upstream players outside of financial services. Many other firms and sectors in the 'scams ecosystem' (e.g. online platforms, telecommunications firms) play a major role in facilitating and enabling scams, so government should consider how these sectors should be required and incentivised to help prevent scams at their source. This would represent a welcome shift from managing and preventing authorised fraud in financial services alone, to a broader, coordinated public policy to prevent these scams happening in the first place, with many sectors required to take preventative action to protect consumers and businesses and reduce the APP fraud at its source – i.e. outside the FS sector.

Regulation 90 requires firms to recover funds in the event of an incorrect unique identifier being used. In these circumstances, firms must make "reasonable efforts to recover the funds". However, the PSRs set no requirement on payment services providers to recover funds and repatriate these back to the remitter for an authorised push payment fraud. This is currently done through banks operating in accordance with industry best practice standards, and informal indemnity structures, but notwithstanding this, there is still no prescribed timeframe firms have to satisfy. This also becomes increasingly difficult with international payments. We would encourage government to review this and to consider what improvements and enhancements could be made to the existing regime to standardise the process in these circumstances, with the benefit of extending the corporate opt out where applicable. We would be supportive of further consultation in this respect.

As mentioned in relation to Question 18, the existing liability construct for fraud set out in the PSRs is too limited in scope to make any meaningful impact in Open Banking, and payments stemming from PISPs. This is important today but, given the regulatory strategy to increase use of such payments as an alternative to card payments, the volume could increase substantially. This objective should not be achieved without addressing the liability issue. See also our comments regarding Regulation 71(7) in response to Question 15).

20. In relation to payment transactions which payment service providers suspect could be the result of fraud, is there a case for amending the execution times for payments to enable

enhanced customer engagement? What requirements should apply here to ensure the risk to legitimate payments is minimised and that such delays only apply to high-risk, complex-to-resolve cases?

We are supportive of amending the execution times for payments to enable firms to undertake enhanced checks on a payment instruction before acting to send the payment. As referenced in the House of Lords report "Fighting Fraud: Breaking the Chain": *"The UK's advanced payments infrastructure is one of the key reasons why it has become a global centre for fraud. The speed with which payments can be made must be delayed in certain circumstances to allow more time for banks to review risk signals and contact their customer about the proposed payment. The Payment Systems Regulator should consult on measures to achieve this*"[8]. As acknowledged in this Call for Evidence, in doing so there will be genuine payments that are unfortunately captured by this delay. To ensure firms are not unfairly penalised for delaying payments where they have genuine concern of the risk of fraud, we ask government to consider how firms can be excluded from any civil liability with regards to consequential loss stemming from delaying a payment in this regard.

Development of nuanced transaction monitoring to identify high-risk and complex to resolve cases and embedding and delivering operational and system changes will take time. We encourage government to consider timeframes for implementing any change and to engage and consult with industry as early as possible.

In relation to payments through Open Banking, we highlight in our response to Question 21 the lack of information an ASPSP receives from a TPP and the impact this has on the ability for a firm to undertake any meaningful transaction monitoring. We would be supportive of transaction risk indicators being made mandatory to assist ASPSPs in this regard, and to help prevent Open Banking remaining a weaker channel to be exploited by fraudsters.

Where legitimate transactions are delayed, customers are likely to be unhappy and confused about this. Barclays and other firms will ensure their customers are fully apprised of the changes and the reasons for them. However, we ask that the government, regulators and other consumer organisations educate customers about this change to reduce the potential of such confusion and frustration.

21. In relation to fraud, whether unauthorised or authorised, is there a need to a) complement rules with data sharing requirements; and b) for further reforms be made to make Strong Customer Authentication work more effectively and proportionately?

There are already a wide range of initiatives working on data sharing to improve fraud detection and prevention, both within the financial services industry and cross-sectorally. These include initiatives being run through UK Finance (including the Enhanced Fraud Data Sharing proposal), Stop Scams UK, Threatmetrix, the National Cyber Security Centre, as well as initiatives with specific telecommunication companies and email service providers. These initiatives, coupled with the Payment Systems Regulator Directions for authorised push payment fraud, mean PSPs will already be mandated to share a substantial amount of data.

That said, we have previously recommended the Payment Systems Regulator includes in its Directions for authorised push payment fraud a requirement to publish the data on the origin of a scam payment (i.e. identify and categorise the volume per enabler). This would help to highlight those areas or platforms where there is a greater risk of fraud, including outside the financial services sector. It would

[8] https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf

also help the government and other public authorities identify evidence-based opportunities to work with organisations that provide entry points for fraudsters (e.g. social networks) and would incentivise those third parties to take responsibility to prevent the scam at source.

PISPs should separately be required to publish scam data to aide with incentivising firms to reduce their volumes of scams, and to allow for customer comparison. As already referenced in Question 18, PISPs should also be required to capture and share additional payment information with ASPSPs (e.g. Transaction Risk Indicators, including payment purpose, as well as 'on behalf of' merchant data), so that ASPSPs can use this data in their fraud detection engines, to detect and prevent fraudulent payments. At present, the ASPSP does not always receive the 'payment purpose' from the PISP, which is a key data point for ASPSPs to consider as part of the assessment of fraud risk for that payment[9]. The 'on behalf of' field would allow the ASPSP to know which merchant is receiving the funds (i.e. who the payee is), again to provide vital information for fraud detection engines. Sometimes the data received regarding the payee is inaccurate, as the PISP may be using a holding account to receive payments into before passing it on to the merchant account (who is unknown to the ASPSP). Therefore, the ASPSP cannot effectively categorise the payment to determine whether it could be fraudulent as they only know which PISP the funds are being sent via, not who the ultimate payee is.

In relation to further reform for Strong Customer Authentication ("SCA") in the context of fraud, we note that SCA has had a positive impact on reducing levels of unauthorised payments. However, firms are incentivised to take action to reduce the volumes of fraud and scams without such action being prescribed by regulation. An example of this is the industry adoption of 3D Secure.

We strongly consider there is scope for the SCA Regulatory Technical Standards to be more effective and proportionate, removing unnecessary friction from a payment journey whilst still managing risk. The Regulatory Technical Standards are unnecessarily overly prescriptive and do not allow for innovation in solutions. Our concern is that such prescription and standardisation means firms are not able to adopt risk based controls which are subjective to each end user/payment transaction type/payment value. Not only does this add unnecessary friction to payment journeys, but it means that fraudsters can predict the types of information firms require and how firms behave, allowing them to exploit any identified gaps more easily.

Instead, we suggest an outcomes based regulatory regime would be more appropriate, with further scope for optionality based on firms' specific metric and data obtained from payments flow and customer behaviour. The requirement should be on firms to monitor the amount of unauthorised payment fraud (noting firms are already required to do this and to report this information to the FCA) and then implement the appropriate controls, which may require SCA, but we do not believe it is appropriate for this to be driven by regulatory requirements for all payments made by all end user. For example, large corporates and government departments could be exempted all together from SCA.

The Transactional Risk Analysis under Article 18 of the Regulatory Technical Standards permits the disapplication of SCA where the payer initiates a remote electronic payment transaction that firms identify as posing a low level of risk according to certain prescribed transaction monitoring mechanisms. However, the exemption threshold value is capped at £440, irrespective of whether a payment transaction could be classified as a low level of risk of fraud based on substantive firm-subjective data. There is now scope to review this.

[9] As at the date of writing this response, we have yet to receive an Open Banking payment authorisation that has contained a transactional risk indicator

A further example demonstrating the need for reform of Article 18 is the requirements at Article 18(2)(c) which essentially set out a shopping list of requirements for firms to meet before they can classify a payment as posing a low level of risk and can therefore apply the exemption. We consider these items should only be elements for firms to consider as being an indicator that a payment may be higher risk.

The need for a PSP itself to be the one conducting this real time fraud monitoring is also problematic. Given the disaggregation of payment services, and the increase of third party fraud services now available, many merchants are doing this, not the PSP. This is not monitoring that a PSP has to undertake for the merchant, and the prescriptiveness of the Article means that a PSP may not be performing that real-time risk analysis and so cannot properly utilise the exemption (even though that analysis is being done, and the metrics to evidence this can be produced). We also do not see the need for a separate auditing requirement for Article 18, in addition to the general audit requirement at Article 3 of the RTS; it is overly burdensome and is not replicated elsewhere.

Whilst we are supportive of the opportunity for SCA to be amended to work more effectively, we stress that any change would need to be carefully consulted on, allowing firms sufficient time to make complex technical changes to systems and processes. Change in this area should be approached cautiously due to the time and cost incurred in changing these systems.

Issuance and redeemability of electronic money

Considered against the government's objectives for payments regulation:

22. Are the requirements regarding issuance and redemption of electronic money still appropriate?

Barclays has no strong views in relation to this question.

Miscellaneous

23. Noting the intention to commission an independent review in due course, do you have any immediate observations on the efficacy of the operation of the Payment and Electronic Money Institutions Insolvency Regulations to date?

Barclays has no strong views in relation to this question.

24. Finally, do you have any other observations relating to the payments framework not encompassed above, and how this could be further improved, in line with the government's objectives?

With regards to paragraphs 51-58 of this Call for Evidence and the approach to Open Banking, our views on the expansion and improvement of Open Banking are reflected in our response submitted to SWG as part of the SWG's sprint process, and following the SWG's draft final report, which were shared with JROC. Notwithstanding that, we consider it worth highlighting in this response that a key objective for government must be the transition to the Open Banking Future Entity including establishing a new funding and governance model. All participants in Open Banking, including consumers, need certainty and until there is progress in this regard it is very difficult for innovation and expansion of Open Banking to be progressed.

We consider it fundamental to any design of future payments frameworks (not limited to Open Banking) that there must be empirical evidence demonstrating an underlying customer need. There are examples in relation to Open Banking where firms have built infrastructure for third party access

which has had very minimal usage by customers and TPPs. The government's Objective D *"Fostering competition in the interests of consumer"* is particularly relevant. To the extent that government considers there is a need to mandate creation of payment services/products for payment service users, we would stress the importance of utilising a corporate opt out, to allow firms the freedom to decide whether to build such services for their larger corporate clients. Against the backdrop of Consumer Duty, identifying a customer need and a target market is crucial for firms to ensure they are delivering value and helping customers to properly meet their financial objectives.