Implementation of the revised EU Payment Services Directive II – Barclays Response

1. About Barclays

1.1. Barclays is a transatlantic consumer, corporate and investment bank offering products and services across personal, corporate and investment banking, credit cards, and wealth management, with a strong presence in our two home markets of the UK and the US.

1.2. With over 325 years of history and expertise in banking, Barclays moves, lends, invests, and protects money for customers and clients worldwide. For further information, please visit home.barclays.

2. Summary

2.1. Barclays welcomes the opportunity to respond to HM Treasury’s consultation on the implementation of the revised EU Payment Services Directive II (PSD2). Barclays has contributed to and supports the response submitted by Payments UK, the UK Cards Association, and the British Bankers Association.

2.2. The introduction of regulation for two discrete types of payment services – Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) – has the potential to revolutionise the way consumers and businesses manage and spend their money and receive payments.

2.3. Barclays wants to ensure customers can make the most of these innovative services, and that customers are protected from fraud and risks in this new environment. This paper highlights the most significant areas which Barclays believes HM Treasury should address so that customers can benefit from PSD2 whilst not being exposed to additional risk.

2.4. We also caution against seeking to expand the scope or timelines of PSD2 or blurring it with the CMA’s open banking remedy, which has a very clear and specific focus. Providers with products in scope of the CMA remedy must focus on delivering this regulatory requirement on time and in a way that is compliant with PSD2 where the two initiatives intersect. Successful delivery of the CMA remedy in this way should lay appropriate foundations for the future development of third party services.

2.5. We are particularly keen that HM Treasury recognise the distinct nature of banking services provided to large corporates and more sophisticated smaller businesses. The existing ecosystem of corporate banking services and third party services is multi-faceted and complex. Thoughtful application of PSD2 in this area is necessary to preserve client experience.
3. AISP and PISP access

3.1. Barclays commissioned Ipsos MORI to conduct consumer research into third party access. The study found that if consumers experience a negative consequence as a result of sharing their data, three-quarters say they would be less likely to give permission for their bank to share their information in future. Around half say they would be less likely to use digital banking services and indeed trust their bank less in general as a consequence.¹

3.2. Instilling confidence from the outset is therefore critical, especially given the intimate and emotive relationship customers have with their current accounts. Tooley Street Research explored customer attitudes towards their current accounts, concluding that “if something were to go wrong… this would be a source of considerable anger as there was felt to be ‘more at stake’ with a current account than…other services.”²

3.3. A separate report recently commissioned by Barclays looks specifically at consumer perspectives and it highlights potential negative consumer consequences if consumer protection does not lie at the heart of third party access. It cited potential risks such as data loss; misuse of data; disempowerment; and a reduction in privacy or security.³ The report sets out a series of useful recommendations. One of which is the effective regulation of this new market. We would like HM Treasury and the FCA to work together to ensure that the regulation of those providing third party services is suitably robust. Authorisation criteria and on-going supervision should match the sensitivity of the data and payments functionality that third parties will be able to access. While not the subject of this consultation, this needs to be a core consideration for Government.

3.4. The Government should also consider whether regulators have sufficient oversight, capability and resource to address any new conduct risks that may emerge from an open banking environment. This should include ensuring Account Servicing Payment Services Providers (ASPSPs) have real-time access to the FCA register and that there is capacity for industry-wide fraud intelligence sharing, as happens today with merchant payments.

3.5. HM Treasury should be careful to avoid creating new risks. We note that in the directive AISP cannot request sensitive payment data.⁴ The draft regulations change this to the storage of sensitive payment data.⁵ We hope and assume that this is a transposition error. We consider that if AISP are routinely requesting sensitive payment data, the risk of fraud would increase. We caution that adding, for example, customer contact details, into the information that third parties can access exposes customers to additional risks which are not necessary to achieve PSD2’s policy objectives.

3.6. The Ipsos MORI research found that a sufficiently appealing use case can “trigger unquestioning adoption…without considering security issues”⁶ even if people say they care about their data. A recent Citizens Advice report finds that people do not fully understand the terms of data exchange in the digital world and so “cannot make a judgment call on whether it is fair or not”.⁷ The Barclays commissioned report Open banking: a consumer perspective therefore recommended that “the whole industry should take steps to understand what ‘positive friction’ might look like for consumers”.⁸

3.7. With this research in mind, we believe that replaying consent is an important step in the process. Under PSD2 a customer must give consent to the third party to access their data or make a payment. We believe it is vitally important that ASPSPs retain the ability to replay to the customer what they have consented to share. This minimises the risk of that consent being distorted. For

---

⁴ Directive (EU) 2015/2366, article 67, 2, (e)
⁵ Page 3, Ipsos MORI (October 2015), Ibid.
⁷ Page 28, Reynolds (January 2017), Ibid.
instance, a customer could consent to share their balance data, but this could be changed and, without adequate controls, result in a request to the ASPSP for transaction history data. PSD2 is silent on this, but it is a critical fraud mitigation measure.

3.8. Fraud and cyber-crime is already increasing dramatically; in 2014 only five incidents of cyber-attack were reported to the FCA, in 2016, 75 were reported,9 financial fraud losses across payment cards, remote banking and cheques were £399.5 million in the first half of 2016, a 25 per cent increase on the same period in 2015.10 PSD2 and open banking create a new ecosystem which fraudsters will be looking to attack. HM Treasury should consider whether existing and upcoming legal protections are sufficient to protect customers.

3.9. We also believe it is important for the long-term sustainability of third party access to find a suitable balance between third party access and safeguards to preserve core banking systems. ASPSPs should be able to manage unreasonable third party usage through throttling and to enable scheduled maintenance to take place. We believe this is in line with HM Treasury’s thinking, and that of the Implementation Entity for CMA open banking.

3.10. We support innovation and competition by ASPSPs, and want to offer customers the best possible digital experience. HM Treasury and the FCA should not adopt an approach to PSD2 that negatively impacts the incentives of ASPSPs to offer enhanced services to their customers. We encourage HM Treasury to be explicit that overlay services, such as personal financial management tools, provided by ASPSPs and products and services beyond payment accounts are not accessible to third parties.

4. Corporate banking services

4.1. Corporate banking services and those services provided to more sophisticated smaller businesses are very different from those provided to retail customers. Complex configurations for payments authorisation entitlements are common, as are distinct accounts payable process and purchase order systems. This complexity poses a different set of challenges for the implementation of PSD2. These challenges suggest an API only approach is not appropriate. APIs will form part of the solution but, we do not support restricting innovation or degrading customer experience by focusing on one technical approach.

4.2. There already exists a rich and complex ecosystem of third party providers and services in corporate banking services. For example, Barclays enables its corporate customers to use Xero, a cashflow forecaster and reconciler. The use of payroll service providers, like ADP, is common; as is the use of a comprehensive payment system platform like those provided by Bottomline Technologies. Some of these arrangements will involve a contractual relationship with banks, but some will not.

4.3. We also urge care from HM Treasury when defining what is and what is not an AISP or PISP service. Existing corporate functions like shared service centres, in-house banks and central treasury may appear on a literal level to provide third party services. However, Barclays does not believe that they should have to register as an AISP or PISP or be regulated as such.

4.4. Considering the complex environment and existing third party ecosystem, we would like to offer assistance to HM Treasury and FCA to understand and navigate the challenge of implementing PSD2 in the area of corporate banking services.

5. Third party liability

5.1. The Ipsos MORI study asked how consumers would react to a loss resulting from a third party provider. While the majority of consumers felt that the third party was responsible for the loss, most would contact their bank first to resolve the situation.11 The directive acknowledges this
situation and ASPSPs are expected to compensate consumers for unauthorised transactions in
the first instance, before later pursuing the third party. However, there remains an issue of how
will an ASPSP be able to pursue a third party responsible for causing consumer or client loss. For
example, what protections are there if the loss is not monetary, but instead relates to customer
data that could lead to a risk of financial loss, customer distress or detriment? Even in a payments
scenario, what if the third party does not have sufficient funds, walks away from the liability or if
the insurance is not sufficient?

5.2. The consultation suggests that the industry should lead efforts to design a workable approach to
resolving such disputes. We do not think this will be possible without further guidance from the
Government or regulators. Third parties will be from any EEA country, and will be authorised by
competent authorities outside the purview of the FCA. There will be no contract between the
ASPSP and the third party. There will be no obligation on the third party to participate in any
dispute resolution scheme. This is why further guidance would be helpful. As discussed above, it
is critical to ensure proper regulation of third parties to minimise the risk of client loss occurring
in the first place – whether financial or data loss – and to provide a suitable enforcement and
redress mechanism.

6. Amendments to the Consumer Credit Act and the extension of right of termination to overdrawn
current accounts

6.1. Barclays was surprised by HM Treasury’s proposals regarding changes to the Consumer Credit
Act. Implementation of any necessary amendments should form part of HM Treasury’s ongoing
review of the consumer credit regime as a whole.

6.2. For example, paragraph 4.7 of the consultation document mentions that the Government is
considering giving customers a right to terminate a framework contract while in overdraft and
require PSPs to rely on contract rights to recover the debt. The PSP’s approaches and rights to
recover the debt reside within the framework contract. If the Government allows these rights to
be avoided, customers could be incentivised to incur overdrafts and then terminate their
agreements. We do not consider that such an incentive would be a responsible policy outcome.

7. Monthly statements

7.1. The consultation’s proposals on monthly statements would reduce flexibility for consumers,
businesses and corporates and does not align with the FCA’s encouragement of smarter
communications and the Government’s support for digital innovation. FCA research shows that
annual summaries “have no effect on consumer behaviour in terms of incurring overdraft charges,
altering balance levels or switching to other current account providers”;12 whereas by contrast,
giving customers relevant information in an engaging way with a clear call to action has a
considerable effect. The CMA remedies recognise this and rightly champion digital
communication as an alternative to regular, monthly communications. We believe HM Treasury
should adopt the language in PSD2 which allows providers to make the information available.

7.2. Barclays welcomes the opportunity to discuss these matters in more detail with HM Treasury and
other stakeholders in PSD2 regulation. If you would like to discuss Barclays’ response in the
meantime, please contact James Meyrick (0207 116 1096) or Louise Pancott (0203 134 7303).

Catherine McGrath
MD, Transactional Product and Community Banking
Barclays UK

---

12 Page 3, FCA (March 2015), Message received? The impact of annual summaries, text alerts and mobile apps on consumer banking behaviour. FCA occasional paper No. 10,