Barclays PLC
1 Churchill Place
London
E14 5HP

barclays.com

27 February 2015

Data Sharing and Open Data in Banking
Banking and Credit Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Call for evidence on data sharing and open data in banking

Dear Sir / Madam,

We welcome the opportunity to respond to this Call for Evidence and share the Government's ambition that the UK remains at the forefront of digital innovation. The impacts of the creation of an open API standard are significant, and therefore deserve detailed consideration.

In view of the complexity of the issues involved, we are concerned that the time for responding is very short. The BBA plans to establish a working group to look at banking and finance open APIs and data sharing with a range of financiers, and we look forward to participating. We are keen to find a way to build on Midata through the use of APIs, recognising that customers should have access to their data to make informed decisions. As with any proposals around customer data, significant care needs to be taken to ensure that genuine privacy and security matters are addressed in the right way. We also need to ensure that innovation naturally occurring in the private sector is recognised and supported.

Trust, consent and liability

Customers expect their bank to protect their money and safeguard their data. The ODI/Fingleton report says that banks should not carry liability for customer information after it has been extracted for use by a third party, and we support this approach. However the Call for Evidence suggests banks 'should be responsible for setting out precisely what information will be accessed and how that data will be used'. It will not be possible for banks to control how data is used once it has been released to a third party, including where customer detriment may arise. It is therefore considerably important to build customer education and understanding into the development of a banking API standard.

- Our experience suggests that ensuring customers understand risks around their data and are therefore able to provide genuinely informed consent is not straightforward. We have seen a number of situations where customers have provided signed authority agreeing to third parties accessing all the data we hold about them; their feedback suggests that even where such a formal written authority has been given, customers do not always appreciate the nature or volume of data which will be disclosed. Customers are also not always in a position to make an informed decision about the specific risks that certain types of data may create. For example, a customer may not appreciate exactly what pieces of data are likely to put them at risk of certain types of fraud.

- We have a duty of care towards our customers, and believe they will continue to expect this to apply even where they consent to third party access. This creates a mismatch in customer expectations which may undermine their trust in us and our relationship with them in the event

that something goes wrong. Allied to this, the very fact of the bank's involvement may encourage customers to take on risks that they would otherwise be uncomfortable with because the banks are involved.

- We would also note that third parties may make decisions based on data held by the banks. Despite the banks' best efforts, it may be that this data is no longer accurate or does not provide a full picture of the customer (e.g. those who are multi-banked). For example, an alternative lender may make a lending decision based on customer addresses provided to them by a current account provider. There is a question as to where liability would rest for any resulting customer detriment if this information turns out to be incorrect.

Privacy

As Midata was developed, Barclays played an active role in considering the privacy risks and the industry put mitigating actions in place to protect customers. A person's transactional history can reveal a huge amount about them - anything from shopping habits to religious affiliation. It can also reveal personal information about other people connected to them, e.g. names of family members. In addition, it can show details of their relationships with other organisations such as political parties and trade unions. In the context of Midata we decided to mask certain data to support customer privacy, but an open API standard may not automatically come with this safeguard. It can be argued that this information is available through bank statements or a Subject Access Request; however, there is a difference between giving information directly to customers and providing it 'on tap' to third parties. We are keen to find a way to build on the Midata experience, leveraging the good practice that has emerged.

Fraud and security

The protection of customer data is a top priority, and we believe more consideration should be given to addressing the security implications as open data proposals are developed.

- Even the act of sharing data with third parties creates greater risk of hacking, identity theft, and targeting of individuals. These risks ought to be considered alongside the perceived customer benefits of open APIs.

- Banks devote considerable resource and experience to protecting the data they hold. It would be unreasonable to expect that every other organisation, particularly those who do not have a background in financial services, to be able to guard against the level of threat that financial data may be subject to across a variety of channels. For example, the openly available data may allow criminals to identify the type of transactions customers are making and potentially account numbers for utility providers. That information could be 'enriched' using web analytics or by calling suppliers to phish for further details. The fraudster would then have enough information to complete an identity takeover, which would then allow them to open credit card accounts, request loans etc. to the detriment of the customer.

- We do not believe the level of security proposed in the Call for Evidence is strong enough. While the security proposed (OAuth) is appropriate for anonymised data, it is not suitable for transferring individualised customer data via APIs. OAuth is an authorisation protocol with an identity within it; it does not itself authenticate users. Strong authentication relies on identity verification and registration, lifecycle management and fraud detection processes. OAuth on its own would not be secure; and it would not meet the requirements for strong customer authentication under the Payments Services Directive II or the EBA Guidelines on security of internet payments.

Investment and priorities

We understand that the Government believe there are strategic benefits to banks from open APIs. This depends on the plans and priorities of each institution. It should be balanced against the costs of implementation and the opportunity costs of pursing this venture over other innovations (both regulatory and competitive).

- Providing open APIs would inevitably require resource that banks are currently using to fulfil competitive and customer-centric priorities, as well as regulatory and voluntary initiatives. There are further developments in train, including the Payment Services Directive II which covers similar ground to open APIs so we are keen to find an aligned way forward.

- We believe the costs of creating an open API standard would be vastly more than the ODI/Fingleton Associates report suggests. This is particularly the case if there is a requirement to archive and retrieve historic data, and to present it in a useful format. Needless to say, the costs of implementation inevitably increase with the need to communicate to customers about the new ways in which their data may be used and in building extra security so data can be transferred in the right way. Clearly the costs of an open API standard would not only comprise set up costs but ongoing maintenance as well.

- Currently where we provide external APIs, we often do so for a fee which reflects the underlying work involved. The Data Protection Act also enables companies to charge a small fee to customers for providing them with their data, again recognising that there is a cost to the banks in doing so. The ODI/Fingleton Associates report, by contrast, carries the expectation is that banks provide this data for free.

- Customers rightly expect a very high level of protection from their bank. This is reflected in the significant investment banks have made in their security and the way they manage and correct customer data. Our data architecture and structures therefore naturally contain elements of our intellectual property which can fall under copyright.

- Where we currently share data with other providers, we do so for a specific purpose - e.g. for fraud prevention or credit scoring - and the use of the data is limited to that purpose. The Call for Evidence proposes a significant extension to enable competitors to potentially use data that Barclays has built with a customer, which gives us cause for concern. Further thought should be given to a balanced approach that supports challengers while respecting the legitimate commercial relationships of existing finance and banking providers. It should also be noted that customer banking data can reveal not only information about the customer, but their relationships with other companies which may represent a competitive edge in their respective sectors.

In view of the concerns outlined above and those highlighted in the BBA and Payments Council responses, we feel uncomfortable with the speed at which the Government is seeking to progress. However, we would welcome more detailed discussion on the use of open data in banking and finance, recognising that customers have a right to access their data. We are also more open to the publication of aggregate data, and again would appreciate more in depth exploration. We support the BBA plans to convene an expert working group to focus in on these issues, taking in a broader range of financiers. Their work could also include considering alternative proposals, such as leveraging the data sharing activities finance providers currently undertake which could support the Government's policy aims.

Yours sincerely,

Matt Hammerstein
Head of Client and Customer Experience

Catherine McGrath
MD, Transactional Banking and Products