Ipsos MORI

BARCLAYS

OPEN API

Exploring the views of consumers and small businesses

In 2014, the Government published a report by the Open Data Institute and Fingleton Associates on open data and data sharing for banks.

In January 2015, HM Treasury launched a call for evidence on how best to deliver an open standard for Application Programming Interfaces (APIs) in UK banking and to ask whether more open data in banking could benefit consumers. The Government has since asked the banking and FinTech industries to work together on the creation of a framework to introduce an open API and open banking standard in the UK.

Barclays commissioned Ipsos MORI to explore consumer and small business perspectives on possible use cases and on the permission based data sharing that would underpin the framework (open APIs). The research also sought to examine consumer expectations about the role of banks, third party service providers and regulators, and to consider the implications for consumer communication and engagement.

KEY FINDINGS

- Some potential open API enabled use cases have clear consumer appeal, with aggregation of financial holdings perceived particularly favourably.
- 4 in 10 consumers responded positively to the concept of data sharing via open API.
- There is some caution about sharing personal data such as credit scores and account balances, but a significant number of consumers would be happy to do so.
- SMEs tended to be more cautious in their responses to open API use cases, but the most appealing example was accounting software linked directly to a company's bank account.
- A sufficiently appealing customer benefit can trigger unquestioning adoption, suggesting consumers could be at risk of sharing personal data without considering security issues.
- Brand is a key consideration for consumers when evaluating risk – a brand they trust is seen as 'short-hand' for strong security.
- When consumers apportion blame for possible negative consequences (e.g. security breaches), the third party provider is given the greatest share (but banks are also implicated).
- Many people's first point of contact for more serious breaches would be their bank, rather than the third party provider.
- In money loss and identity theft scenarios, there is a striking disconnect between where consumers feel blame lies and who they would turn to for resolution of the issue.
- Irrespective of who they believe is to blame, consumers think that the relevant bank should, or would, be involved when it comes to monetary compensation.
- There is also potential reputational risk for the parties involved – both third party and bank.
- Consumers generally expect third parties to be regulated.

RESEARCH DESIGN

The research consisted of two consecutive stages, qualitative followed by quantitative.

The qualitative stage was carried out in July 2015 and consisted of six focus groups, four with consumers and two with owners / decision-makers from Small and Medium Enterprises (SMEs). The groups included a spread of ages (consumers) or annual turnover (SMEs). Discussion was primarily focused on reactions to a series of use cases; practical examples of the kind of tools or services that may become available as a result of open API (as described in the Open Data Institute and Fingleton Associates report for the Government[1]). Participants were invited to offer their reactions, both positive and negative, and to share any concerns they felt.

The quantitative stage took the form of 2,027 online interviews, conducted in October 2015, with a nationally representative sample of consumers aged 18+. Respondents were introduced to one of three scenarios describing potential detriment arising from a security breach following adoption of an open API use case. The objective was to measure consumer response to these situations. As part of the analysis the responses of certain subgroups of consumers were reviewed, such as those who are highly tech savvy[2].

A further phase of quantitative research amongst SMEs is also likely to be conducted.

All numbers cited throughout this report have been rounded to the nearest whole number.

USE CASE SCENARIOS EVALUATED IN CONSUMER GROUPS

1. A current account comparison tool that looks at the way you use your current account to recommend the best account for you (you would give the tool permission to see your banking information directly).

2. A money management tool that gives you tips and advice based on your current account and credit card usage, while constantly updating your information (they would be able to see the way you use your financial products, with your permission).

3. A secure website where you can see all your financial information in one place, even if you hold products with different providers (e.g. bringing together your credit card, current account, savings account etc.). You can make transfers between them and make payments from this one site. You can also choose to add other things, like your utilities bills, so they are all visible in one place.

4. Getting a loan or mortgage in a faster and easier way because you give the lender permission to see your financial information directly.

[1] Data sharing and open data for banks - 3 December 2014

[2] Highly tech savvy: Those who access the internet on at least three devices, and perform at least twenty online "activities" across all devices (24% of sample).

RESEARCH FINDINGS – USE CASES

Some potential open API enabled use cases have clear consumer appeal

When evaluating possible use cases, consumers found a number of interesting and relevant elements. The most appealing use case was that which offered an aggregation of all their personal financial information to give them a clear presentation of their financial position. Many saw this as of real value and felt they would be likely to take up such a service, were it to be made available.

"It's about time something like this happened. When I was doing all the bills for my house it would be really nice just to see everything on one [screen]. So I imagine it more of a website than an app, just to see everything."
Female consumer, London, 26-35

"The benefit of it is that you're not keeping logging into various accounts; having to remember passwords, pin numbers."
Female consumer, London, 36-55

The other use cases were less immediately appealing, although some elements did offer relevant benefits.

A smart current account comparison tool could potentially save time and effort, but would be employed infrequently and many could not envisage when or why they would want to use it.

"I think it's a great idea because I am lazy and I don't look at what's best for me. I just opened an account and I've had that account [ever] since."
Female consumer, Manchester, 18-25

"I wonder what they can do with a current account. It's a very basic account. There's not an awful lot you can do with it, unless you've got lots of money in there."
Female consumer, London, 36-55

Faster and easier sourcing of loans and mortgages did not appear to be addressing an unmet need, although some did acknowledge that current processes can be too protracted.

"I have a sense that financial services organisations already have access to most of the information that I would give them permission to have in any case."
Male consumer, London, 55+

"Six weeks was a long time [to wait for a mortgage] because, obviously, you're... in a little bit of limbo in that time, even though you've had it approved, you're still waiting for it to come through."
Male consumer, London, 36-55

Money management tips and advice could offer elements of helpful support, but some felt it would be too intrusive or might lead to unwanted product promotion. Others wondered whether it would have comprehensive coverage of the market and so provide genuinely impartial recommendations.

"What I like about the idea is that you're less likely to forget or miss a payment date on a credit card."
Female consumer, London, 36-55

"People can then gauge your spending habits and what you're doing... [and] start sending you offers for different cards and other financial products which you might not actually want."
Male consumer, London, 26-35

A sufficiently appealing customer benefit can trigger unquestioning adoption

Where a clear customer benefit was identified within a use case, the research participants demonstrated a strong propensity for adoption. There was little evidence of their likely adoption being influenced by any potential concerns about data security. A strong, relevant utility appears to be the most important consideration. Similarly, where use cases are less appealing, the main reason given for rejection tended to be the lack of a relevant benefit, rather than any concerns around security.

Consumers tend to believe that considerable data sharing already happens in Financial Services, so the open API initiative appears to be an extension of it. If consumers like a proposition, it is likely they will readily give permission for data access, making the assumption that everything is secure and safe in the background. A sufficiently appealing customer benefit can trigger unquestioning adoption, suggesting a risk of taking ill-thought-through (or 'snap') decisions.

MINT VIDEO

The video shown to participants introduced Mint as a highly secure account aggregation tool which will automatically pull in data from a user's bank account, credit cards, mortgage etc. and allow them to see and manage all of these from one place. It also showed how users are able to create budgets to easily track their spending and the provision of personalised recommendations for how to save money.

www.ipsos-mori.com/mintvideo

Following the video, participants were presented with a description of the permissions required to make this possible:

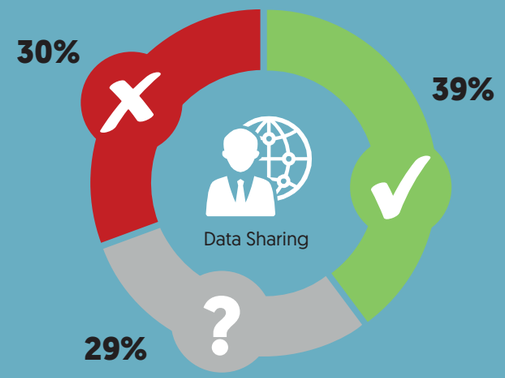
"You would be able to share details of your banking transactions with organisations of your choosing. With your permission, your bank would pass the information directly and securely to the organisation on your behalf. It would be up to you whether to give permission on a case by case basis. You would control which details are shared, and could remove permission at any time."

The possible use case was introduced first, before explaining the permission-based sharing that could underpin it, in order to provide context and avoid a possible negative knee-jerk reaction had the text been shown alone.

4 in 10 consumers respond positively to the concept of data sharing via open API in the context of a financial information aggregation product

The qualitative findings were supported by the quantitative survey. Consumers were played a video showing a specific use case (the money management tool "Mint") and then asked their reaction towards the concept of data sharing that could enable it ("open API"). Almost 4 out of 10 (39%) said they felt positive towards the open API idea, while only 3 out of 10 (30%) said they felt negative towards it.

Overall reaction to the concept of data sharing



Survey conducted online in October 2015
Q1. How do you feel about this idea on a scale of 1 to 5, where 1 = very positive and 5 = very negative? Base: All respondents, n=2027

USE CASE SCENARIOS EVALUATED IN SMALL BUSINESS GROUPS

1. Accounting software that is based on a deeper understanding of your business because you give it permission to look at your banking information directly (e.g. bank account data). The accounting software could also speak to your bank and instruct them (with your permission) to make a payment on behalf of your business.

2. Credit assessment for a lending product in a much faster and more accurate way because you give the lender permission to see your financial information directly. Multiple applications could be made at the same time online.

3. A financial product comparison service that is based on a deeper understanding of your business finances. You would give the tool permission to see your business's banking information directly, which would help them recommend a product for your needs.

SMEs tended to be more cautious in their responses to open API use cases

As with the consumers, the SMEs found some appealing elements in the use cases that were presented to them. The most appealing use case involved accounting software with functionality which would link it directly to a company's bank account. The main reasons for its appeal were the perceived improvements it offered in both efficiency of reconciliations and the ability to trigger payments directly.

"I run two businesses so what takes so long is I have to cross reference two bank accounts, so that [use case] is perfect because [it is] obviously integrating everything."
SME, London, higher turnover

"If it's doing some manual tasks automatically then that means it's going to improve efficiency, accuracy, but especially if it's [reducing] unnecessary [human] intervention."
SME, London, higher turnover

The other use cases were seen as less appealing. For instance, faster credit assessment was felt to be something that would be needed too infrequently for it to be worth allowing third party providers access to a company's financial data.

"It's not such a frequent thing... [accessing finance], I've just tried to get leasing for a vehicle and it's been a bit painful, but it's not the kind of thing that needs automating. I wouldn't do it very often."
SME, London, higher turnover

"I wouldn't feel comfortable with someone looking at my ledgers at any time that they choose, because you do your month end accounts and close off the period and make sure you pre-pay things or [do] accruals."
SME, London, higher turnover

"I wouldn't give anyone, not a third party any access to my business; I don't know who they are and what they are going to do with it and who they are going to pass it on to. So it's absolutely a big no for me."
SME, Manchester, lower turnover

Participants from SMEs tended to assess the use cases primarily in terms of their perceived utility and their likely impact on the business. Their concerns, where expressed, tended to relate to the control and confidentiality of business performance, solvency and trading data (rather than fraud or misuse of data). They gave only superficial consideration to potential data security implications.

Brand is a key consideration for consumers when evaluating risk – a brand they trust is seen as 'short-hand' for strong security

Many consumers consider the involvement of a known and trustworthy brand in an initiative, product or service sufficient assurance of security. There is an assumption that with household names such as PayPal, Apple, major retailers or high street banks, security issues are less likely to arise. If they do, consumers expect that they will be resolved swiftly and easily. The organisation's desire to protect its own reputation is felt to be a powerful motivation in such circumstances.

"They are all multimillion pound organisations so they must be doing something right. I think people are happy with banks because of the way they have been going for so many years."
Male consumer, London, 55+

"I am always happy with PayPal; I feel that they represent safe and secure."
Male consumer, London, 55+

"I just have bought into the whole Apple [thing]; I have found them to be very, very good. I've never had a problem with them."
Male consumer, London, 36-55

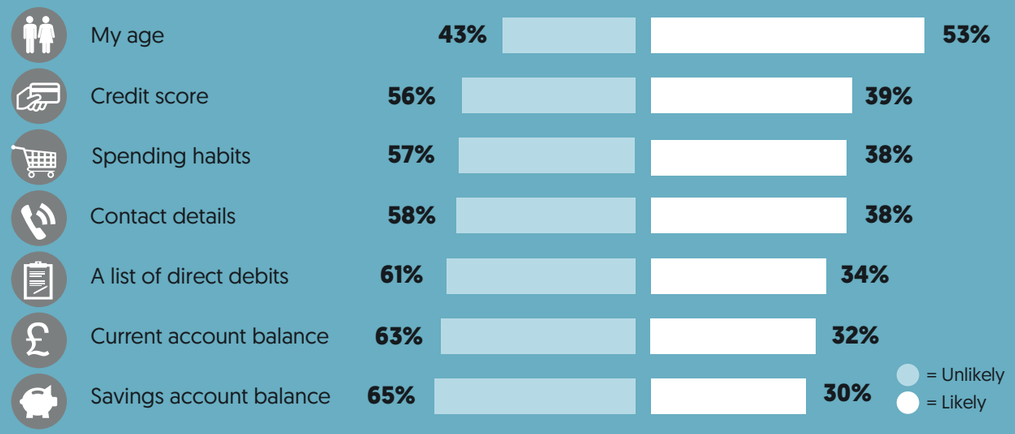
Consumers are generally not making informed decisions around data security considerations. Instead they are responding to how big or well-known the service provider is, and employing this as a proxy.

There is some caution about sharing personal data such as credit scores and account balances, but a significant number would be happy to do so

In the quantitative survey we asked consumers about their willingness to allow their bank to share different types of data with third parties. When considering the range of types of data which could be shared, consumers tended to be most willing to share information about their age, with over half (53%) likely to do so. For all other types of data covered, consumers were more likely to say they would not share them than say they would. Nonetheless, at least 3 in 10 say they would be likely to share information such as savings account and current account balances and details about direct debits.

This suggests that while there is still some caution, there is openness to the idea of giving third parties access to personal financial data in order to access services that are seen as desirable.

Likelihood of sharing banking data



Survey conducted online in October 2015

Q1b. If this initiative is introduced, how likely are you to give permission for the following types of banking data to be shared with third party organisations?

Please indicate your answer on a scale of 1 to 5, where 1 = very likely and 5 = very unlikely

Base: All respondents, n=2027

RESEARCH FINDINGS – SECURITY BREACHES

In order to understand how consumers might act if something were to go wrong as a result of their giving permission to a third party to access their financial data, participants in the quantitative survey were presented with one of three scenarios. Each scenario described the possible effects of an unauthorised or criminal use of their financial information. They were then asked several questions about their likely response.

SECURITY BREACH SCENARIOS PRESENTED

1. Marketing

You give permission for the provider of a tool/ service to access your financial information. You then begin to receive unsolicited phone-calls or emails because the organisation has shared it with others without your permission.

2. Money loss

You give permission for the provider of a tool/ service to access your financial information. That organisation is then hacked by someone who gets access to your information. Using this information, the hacker steals £500 from your account.

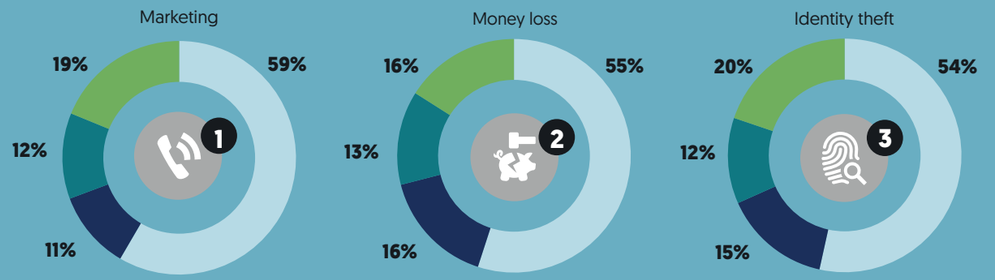
3. Identity theft

You give permission for the provider of a tool/ service to access your financial information. That organisation is then hacked by someone who gets access to your information. Using this information, the hacker steals your identity to get a loan and this damages your credit score.

When consumers apportion blame for possible security breaches the third party provider is given the greatest share but banks are also implicated

Consumers were given the opportunity to consider how they might apportion the blame for the scenario they had been asked to respond to. Across all three scenarios the majority of blame was felt to lie with the third party provider. However, the bank involved was also felt to share some responsibility. In the money loss and identity theft scenarios, there is a striking disconnect between where consumers feel blame lies and who they would turn to for resolution of the issue.

Who is to blame?



Survey conducted online in October 2015

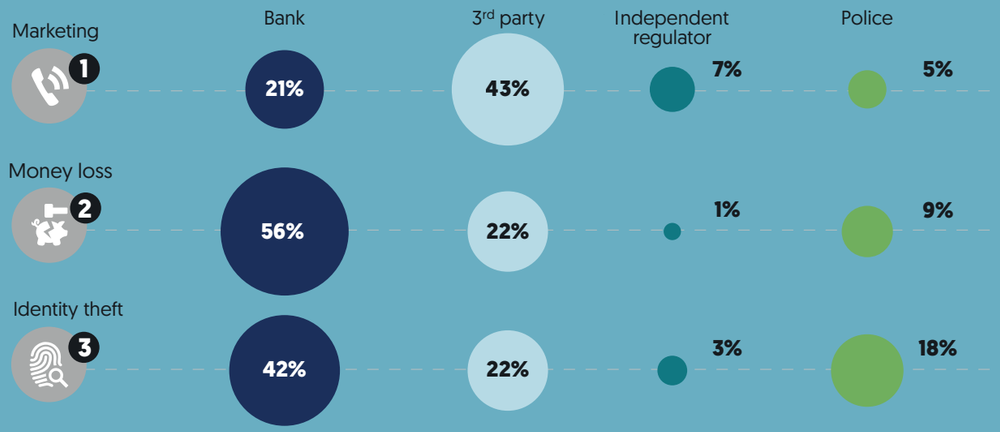
Q4. Who would you consider to be to blame for this issue, based on the information provided?

Base: All respondents, n=2027

Their bank would be many people's first point of contact for more serious breaches

Consumers were asked who they would contact in order to resolve the situation. In response to the marketing scenario, they said they would contact the third party first. In the other two scenarios, their first point of contact would be their bank.

Who would be contacted first?



There would also be a reputational impact for the parties involved. Almost half of consumers (47%) stated they would tell their friends and family about the issue, a quarter (25%) would contact the organisations involved through their social media channels and more than 1 in 5 (21%) would mention the issue on social media.

Survey conducted online in October 2015

Q2. In the scenario described above, who would you contact first to resolve the issue? Base: All respondents, n=2027

Banks are almost as likely to be expected to compensate consumers as third party providers

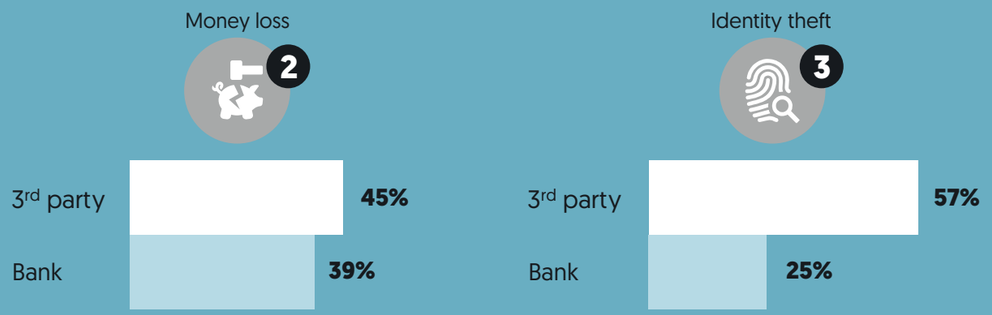
In both scenarios where compensation might reasonably be expected, it was the third party providers who were most often seen as the most appropriate source of such compensation. However, many consumers felt they would look to their bank to deliver such compensation. This was especially true in the scenario where money loss had occurred, where 45% would expect compensation from the third party, but 39% would expect it from their bank.

The research results suggest that, irrespective of who they believe is to blame, consumers think that the relevant bank should, or would, be involved when it comes to monetary compensation. This comes across even more clearly when we ask consumers who they would expect to compensate them if they do not obtain this through the first organisation they contact. 39% of consumers (for both scenarios) listed the bank as the second option for compensation.

Breaches are likely to have a negative impact on consumers' future behaviour

If they had experienced one of the scenarios, three-quarters of consumers say they would be less likely to give permission for their bank to share their information in future. Around half would be less likely to use mobile banking (51%) or trust their bank in general (48%).

Who is expected to compensate?



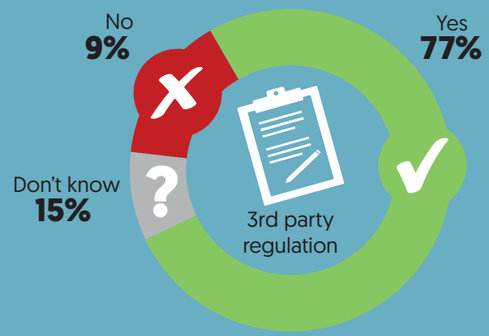
Survey conducted online in October 2015
Q6. In this scenario, who would you expect to compensate you/get your money back from?
Base: All respondents, n=2027

CONCLUSIONS

Based on this research a number of clear findings emerge, with significant implications for all the parties involved.

- Some use cases have considerable appeal among consumers and SMEs, particularly those offering aggregation and transactional functionality.
- Consumers could be at risk of taking ill-thought-through decisions about use case adoption, as their decisions are driven by the nature of the product or service they are being offered – i.e. if it is compelling, they will readily give permission for data access, assuming that everything is secure and safe in the background.
- Should problems arise with security, especially around money loss or identity theft, there is likely to be an expectation that the banks will play a significant role in resolution and compensation. There is also potential reputational risk for all parties involved (third party and banks).
- This suggests that consumer protection needs to form a key part of any developments in this area.
- Consumers endorse regulation (77% of participants felt that third parties should be regulated and over two-thirds of those (68%) expect the role to be taken on by those organisations who already regulate the banks).
- 'Tech savvy' consumers were both more likely than the rest of the population to look favourably on the concept of an open API and more likely to expect regulation to be in place - perhaps indicating that those who are more comfortable with digital innovation are more aware of the risks and so have higher regulatory expectations.

Should 3rd parties be regulated?



Survey conducted online in October 2015
Q8. If this initiative is introduced and you're able to give permission for your bank to share your financial information with third party service providers, do you expect that these service providers will be regulated?
Base: All respondents, n=2027

Ipsos MORI

FURTHER INFORMATION

PAUL STAMPER
Head of Financial Services

Paul.Stamper@ipsos.com
+44 (0)20 3059 4808

www.ipsos-mori.com
@IpsosMORI