

September 2014

---

# Data Sharing and Open Data for Banks

A report for HM Treasury and Cabinet Office

---



fingleton.  
associates

## Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Key message summaries	4
1.2	Organisations that we interviewed	8
1.3	Authors	8
<b>2</b>	<b>Access to data, and competition in UK banking</b>	<b>9</b>
2.1	Competition in UK Banking	11
2.2	The role of information asymmetries as a factor in poor market outcomes	11
2.3	The potential for better access to data to improve market outcomes	12
2.4	Current government interventions aimed at improving access to data	13
<b>3</b>	<b>An introduction to the technology concepts that could enable better data sharing in banking</b>	<b>14</b>
3.1	Technology concepts for better data sharing	16
3.2	APIs	16
3.3	OAuth	22
3.4	Open Data Standard	25
<b>4</b>	<b>The potential uses of bank APIs</b>	<b>28</b>
4.1	Demand for bank APIs from third parties	31
4.2	Ways in which external APIs can create value for banks	39
4.3	Demand for Open Data	44
<b>5</b>	<b>Implementing data sharing in a way that is consistent with data protection and privacy</b>	<b>47</b>
5.1	Use case	49
5.2	Case study - a recommended approach to implementation	52
5.3	Open data: sharing anonymised information with the public	61
5.4	Example: Crédit Agricole Store - Applications Mobiles	62
5.5	Example: Xero Add-ons	64
<b>6</b>	<b>Best practice technical standards for sharing bank data</b>	<b>66</b>
6.1	Use case definitions	69

6.2	Technical requirements	71
6.3	Web-based API best practices	72
6.4	Evaluation of existing data access technologies	75
6.5	Recommended approach to private data access	78
6.6	Recommended approach to open data publishing	79
<b>7</b>	<b>The cost to a bank of implementing data sharing</b>	<b>82</b>
7.1	The importance of non-tech costs	84
7.2	Factors that make APIs more costly than manual file downloads	84
7.3	The challenges of working with legacy banking IT systems	85
7.4	Skills and capabilities	86
7.5	Ballpark estimates on implementation costs	87
7.6	Implementation costs associated with publishing open data	88
<b>8</b>	<b>Summary of measures that would help deliver the benefits outlined in this report</b>	<b>90</b>

## 1 Introduction

The Open Data Institute was commissioned by HM Government and engaged Fingleton Associates to explore how competition and consumer outcomes in UK banking could be affected by banks giving customers the ability to share their transaction data with third parties using external Application Programming Interfaces (APIs<sup>1</sup>). As part of our work, we also reviewed how these outcomes would be improved if banks published non-personal data as open data<sup>2</sup>.

These two forms of data access comprise the core reference points throughout the document. In the main, when we refer to external APIs we mean read only access to some or all transaction history data and other account information. Occasional references to write access, such as the ability to initiate payments, are labelled as such. When we refer to open data, we generally describe the data set in question on each occasion.

We largely focus on the implementation of these data sharing concepts in two core banking markets: Personal Current Accounts (PCAs) and SME Lending. However, we have also tried to capture some of the benefits that would accrue in other adjacent markets.

### 1.1 Key message summaries

We summarise the key messages and policy recommendations from each of the chapters below.

#### **Chapter 2. Access to data, and competition in UK banking**

- 1) Greater access to data has the potential to help improve competition in UK banking.
- 2) Current policy interventions to promote access to data are steps in the right direction, and could be taken further by the application of more widely-used technologies and standards for data sharing.

#### **Chapter 3. An introduction to the technology concepts that could enable better data sharing in banking**

- 1) APIs allow different software applications to communicate with each other and exchange data directly, without the need for human input each time. They have become the de facto standard for sharing data, and have enabled organisations that hold large amounts of data to become platforms for third party innovation.
- 2) OAuth is a widely used standard that provides a simple and secure mechanism for users to authenticate themselves, and authorise how their data can be shared. It allows a user to initiate the sharing of their personal data between different organisations without sharing their login credentials.

---

<sup>1</sup> APIs - Application Programming Interfaces - are rules that allow pieces of software to interact with each other and exchange data. They are explained in detail in Chapter 3. See also [en.wikipedia.org/wiki/Application\\_programming\\_interface#Web\\_APIs](http://en.wikipedia.org/wiki/Application_programming_interface#Web_APIs)

<sup>2</sup> Open Data refers to data that can be used and redistributed by anyone for free, subject only to the requirement to attribute and share alike. It is also explained in Chapter 3. See also [http://en.wikipedia.org/wiki/Open\\_data](http://en.wikipedia.org/wiki/Open_data)

- 3) Open data provides a gold standard for publishing non-personal data in a way that maximises its potential value by creating the best possible environment for its re-use.
- 4) Banks outside the UK have started to make use of all three technology concepts. Banks in the UK are by and large yet to do so.

#### **Chapter 4. The potential uses of bank APIs**

- 1) The demand for data is strong across alternative lenders, accounting software platforms, comparison and advisory services, payment services and others. Many of these organisations already create considerable value from data.
- 2) These organisations currently access data using means such as manual downloads, screen scraping, manual entry and occasionally bilateral data feeds. There is widespread consensus that these methods are hard to use, expensive, and have limited capabilities. Consequently, the desire to see banks provide external APIs was almost universal.
- 3) The use cases described have the potential to encourage competition in the PCA market and SME lending.
- 4) They also impact on other adjacent markets in ways which could be beneficial to SME productivity and consumer welfare.
- 5) Banks themselves could also stand to benefit from creating external APIs. Encouraging third party integration and becoming a 'platform' is potentially a strategy to mitigate the threat of being 'unbundled'.
- 6) Many of the use cases described rely on being able to access not just individual account data, but also aggregated data (anonymised account data) and reference data (banks' respective charges, terms and conditions), ideally published as open data. This includes the core 'Midata' account switching use case, which would benefit from more standardised data on PCA terms and conditions in achieving its potential.
- 7) Applying an open API standard across the whole sector would create the optimal conditions for the re-use of data. However, some organisations predicted that it would take considerable effort and co-ordination to achieve.
- 8) Where API access to this kind of data has been made available, such as by accounting software providers and the Open Bank Project, it has resulted in successful ecosystems of third party applications. These could be replicated by banks.

#### **Chapter 5. Implementing data sharing in a way that is consistent with data protection and privacy**

- 1) Third party access to consumer data is perfectly compatible with both the Data Protection Act (DPA) and the principles of privacy by design so long as it is implemented carefully.
- 2) Both the Bank and any Third Party that the User authorizes to access their data are Data Controllers, and must comply with the DPA accordingly.

- 3) If a Bank is following a User's explicit instruction to share their data with a Third Party, then the Bank has no liability for what happens once the data has been shared. However, the Bank must be sufficiently confident that the the User has consented to the Third Party accessing their data, and that the User understands which of their data the Third Party will be able to access. Other risks to banks may arise if data is shared inappropriately.
- 4) The case study in this chapter provides a high level framework that can help banks implement an approach to data sharing that is compliant with the DPA and is appropriately sensitive to consumer privacy.
- 5) The key principles are:
  - a. The user is fully informed about what is happening to their data, and consent is specific, informed, freely-given and explicit.
  - b. The user has on-going visibility and control over terms of access to their data.
  - c. Third party access to the API should be governed by a vetting process.
  - d. Security standards are "appropriate" as guided by recent technological developments and the Financial Conduct Authority.
- 6) The approach described goes beyond the DPA in two key ways. Firstly, it treats all data as sensitive personal data. OAuth allows the extra responsibilities of working with sensitive data to be met with minimal extra burden.
- 7) Secondly, it suggests that Banks should administer access to APIs by Third Parties, but that a third party should set and enforce the rules governing access on the basis of security and privacy.
- 8) Open datasets which are properly anonymised are attractive to work with as they are exempt from the provisions of the DPA and do not require the provision of informed consent.

## **Chapter 6. Best practice technical standards for sharing bank data**

- 1) Established standards like OFX and FinTS demonstrate that there are no technical barriers to providing detailed access and control to bank data. However, they lack some of the features expected from modern web APIs, such as third party delegation capability.
- 2) More modern implementations of the concept, such as Crédit Agricole and the Open Bank Project provide a good starting point for designing an API to contemporary standards.
- 3) The API should have REST architecture and use JSON or CSV encoding for requests and responses, depending on the type of data.
- 4) To ensure maximum security the API should employ HTTPS connections with HSTS and Forward Secrecy. The industry standard open source cryptographic library OpenSSL should be used.
- 5) The OAuth 2.0 protocol should be used for authentication. Authorisation should be very fine-

grained so that each different type of data can be granted separately according to the specific needs of each Third Party application.

## **Chapter 7. The cost to a bank of implementing data sharing**

- 1) It may cost a bank more to decide what technology and standards to use, and to get the relevant legal clearances, than it does to build the tech itself. Guidance about standards and legal requirements could help reduce these costs.
- 2) Legacy IT systems are a complicating factor in implementing modern data sharing. However, experts who work with bank IT are confident that the challenges they pose can be managed.
- 3) Banks are building the skillsets for implementation and maintenance of high quality API ecosystems, although some have made more progress than others. However, a number of organisations provide ready-made API platforms which banks could deploy rather than building their own from scratch.
- 4) Non-bank experts that we spoke to said consistently that the cost of implementing data access is unlikely to surpass £1m for a bank. Banks were less confident about likely costs, but thought that the figure would be much higher.
- 5) Informed sources assert that it is possible for implementation to be completed from start to finish in less than 12 months. Longer processes may reflect the speed of banks' internal decision-making processes rather than the amount of time needed for technical implementation.
- 6) Once account and transaction data has been made available over an API, the additional cost of publishing aggregated and anonymised open data based on this source is likely to be very low. However, it could equally be created without an API also being made available by the banks.
- 7) It should be possible for banks to publish open reference data, such as PCA terms and conditions, at low cost.

## **Chapter 8. Summary of measures that would help deliver the benefits outlined in this report**

- 1) Banks agree on an open API standard for third party access.
- 2) Independent guidance provided on technology, security and data protection standards that banks can adopt to ensure data sharing meets all legal requirements.
- 3) Industry wide approach established to vet third party applications and publish a list of vetted applications as open data.
- 4) Standard data on PCA terms and conditions published by banks as open data.
- 5) Credit data made available as open data.

## **1.2 Organisations that we interviewed**

We spoke to 28 organisations in the course of researching this report. They include SME lenders, SME accounting software providers, consumer advice and comparison services, banks, payment providers, and various financial data experts. Our thanks is due to all of them for their kind support.

## **1.3 Authors**

The report was researched and created by John Gibson and Andy Reiss of Fingleton Associates, and James Smith, Ulrich Atz and Jeni Tennison of the Open Data Institute.



## 2 Access to data, and competition in UK banking

This chapter describes the potential role that data access could play in promoting competition in UK banking, and outlines some of the key technology concepts that could be employed to help deliver this outcome.

The chapter is structured as follows:

<b>2.1 Competition in UK Banking</b>	<b>11</b>
<b>2.2 The role of information asymmetries as a factor in poor market outcomes</b>	<b>11</b>
<b>2.3 The potential for better access to data to improve market outcomes</b>	<b>12</b>
<b>2.4 Current government interventions aimed at improving access to data</b>	<b>13</b>

### **Key messages**

- 1) Greater access to data has the potential to help improve competition in UK banking.
- 2) Current policy interventions to promote access to data are steps in the right direction, and could be taken further by the application of more widely-used technologies and standards for data sharing.

## 2.1 Competition in UK Banking

Recent investigations into UK banking have concluded that key markets are not working well for customers and SMEs.

- The Competition and Market Authority's (CMA's) market study into personal current accounts found that: the market remained relatively concentrated; new entry has had a limited impact on the largest incumbent providers; barriers to entry and expansion remain high; products and fee tariffs are complex and consumers are not easily able to compare between PCA providers; and switching, while easier, remains low.<sup>3</sup>
- Similarly, the joint study by the CMA and the FCA into 'Banking services for small and medium sized enterprises' found that: the market remained highly concentrated; new entry has been limited; product pricing appears complex and SMEs are not easily able to compare between providers; switching rates are low; and customer satisfaction is low. In addition, the CMA found that, for smaller SMEs, personal current accounts are a gateway to business current accounts, which in turn are a gateway to ancillary business banking products (for example, loans).<sup>4</sup>

## 2.2 The role of information asymmetries as a factor in poor market outcomes

A persistent theme in these reports is the role played by poor availability of meaningful information, both to consumers and to new or potential entrants, or competing providers. For example, the CMA/FCA study into banking services for SME's concludes that:

- SMEs struggle "to understand the cost and service quality provided by SME banking providers, and particularly to compare the offer that they may have with one available from other providers of SME banking services."<sup>5</sup>
- Because an "SME's main banking provider has ready access to significantly more information about that SME than any provider which does not offer that service to it," they are at a "significant advantage over competitors" when it comes to assessing creditworthiness, which results in an information asymmetry that "is likely to create barriers to the entry and expansion of smaller and newer providers."<sup>6</sup>

These findings form the latest instalment in a procession of reviews - Breedon in 2012,<sup>7</sup> Large in 2013,<sup>8</sup> the OFT in 2014<sup>9</sup> – all of which identify problems with information accessibility as a barrier to competition in SME banking and SME lending.

The CMA also identified similar problems in the market for personal current accounts. It found that it is "difficult to compare the costs of PCAs using information on providers' websites" because "many PCA providers have introduced different charging structures that are not easily comparable with those used by other PCA providers."<sup>10</sup>

---

<sup>3</sup> [assets.digital.cabinet-office.gov.uk/media/53c834c640f0b610aa000009/140717\\_-\\_PCA\\_Review\\_Full\\_Report.pdf](https://assets.digital.cabinet-office.gov.uk/media/53c834c640f0b610aa000009/140717_-_PCA_Review_Full_Report.pdf)

<sup>4</sup> [assets.digital.cabinet-office.gov.uk/media/53c8b0ace5274a106b00000b/140723\\_SME\\_report.pdf](https://assets.digital.cabinet-office.gov.uk/media/53c8b0ace5274a106b00000b/140723_SME_report.pdf)

<sup>5</sup> *ibid.* page 122

<sup>6</sup> *ibid.* page 97

<sup>7</sup> [bis.gov.uk/assets/biscore/enterprise/docs/b/12-668-boosting-finance-options-for-business.pdf](https://bis.gov.uk/assets/biscore/enterprise/docs/b/12-668-boosting-finance-options-for-business.pdf).

<sup>8</sup> [independentlendingreview.co.uk](https://independentlendingreview.co.uk)

<sup>9</sup> [webarchive.nationalarchives.gov.uk/20140402142426/www.offt.gov.uk/shared\\_offt/markets-work/sme-update.pdf](https://webarchive.nationalarchives.gov.uk/20140402142426/www.offt.gov.uk/shared_offt/markets-work/sme-update.pdf)

<sup>10</sup> [assets.digital.cabinet-office.gov.uk/media/53c834c640f0b610aa000009/140717\\_-\\_PCA\\_Review\\_Full\\_Report.pdf](https://assets.digital.cabinet-office.gov.uk/media/53c834c640f0b610aa000009/140717_-_PCA_Review_Full_Report.pdf)

## 2.3 The potential for better access to data to improve market outcomes

The negative impact of information blockages on the market is unsurprising. Standard economic theory, corroborated in practice across many real world examples, tells us that markets work well when customers are informed, there is a level playing field between competitors, and switching costs between providers and barriers to entry for new providers are low.

There are good reasons to believe, *a priori*, that increasing the extent to which information is able to flow between different participants in the banking market could help meet these conditions. The table below applies this logic to some examples from retail and SME banking markets. All of these examples are taken from Chapter 4, where they are described in more detail.

**Table 1: Conditions of a well functioning market**

Condition of a well functioning market	Example from the UK banking sector	Potential role for data access
Prices are transparent to consumers	Prices for current accounts are a highly opaque blend of charges and foregone interest. <sup>11</sup>	With access to account data, comparison services could tell a customer precisely how much they paid for their account in the last 12 months. With additional open data about terms and conditions at other banks, they could tell the consumer exactly which current account would have been cheapest for them based on historical usage.
Quality is transparent to consumers	Bank accounts have low levels of differentiation. ‘Innovation’ is largely limited to pricing structure (e.g., Santander’s 123 account) rather than other dimensions of quality. <sup>12</sup>	By allowing third party software access to data, a bank could act as a platform for third party innovation, in much the same way that Apple acts as a platform for developers through its Appstore. The additional functionality created by third party applications could then be used to differentiate quality to attract customers. Publication of data about account features or customer feedback can also be published as open data which can in turn increase transparency of quality.
Switching costs are low	Seven day switching has made the account switching process easier in principle, although absolute switching numbers remain low. <sup>13</sup>	More transparent pricing and account quality information, as above, would reduce the information costs of switching. Furthermore, if consumers were able to port their historical records with them when they switched accounts, this would remove a reason not to do so.
Barriers to entry are low	Banks are able to use an SME’s bank account history as an input to credit scoring, whereas alternative lenders have no access to this information.	If alternative lenders were able to access this data, they could use it to make more accurate decisions about creditworthiness, and the pricing of loans.

<sup>11</sup> Despite years of regulatory intervention, the OFT found that overdraft charges and foregone interest still accounted for two thirds of current account revenues in 2011. See [oft.gov.uk/shared\\_oft/reports/financial\\_products/OFT1005rev](http://oft.gov.uk/shared_oft/reports/financial_products/OFT1005rev)

<sup>12</sup> A well functioning market needs innovation that seeks to attract new customers. Where banks have rolled out consumer innovation in the recent past – Internet banking, mobile apps, improvements in security – this has largely been focused on reducing cost and growing revenues from existing customers. As Vickers’ Independent Commission on Banking reported, “A good deal of the innovation in the banking industry makes products and pricing structures more complex, hindering the ability of consumers to understand and compare the different products.” See: [publications.parliament.uk/pa/jt201314/jtselect/jtpebs/27/2704.htm](http://publications.parliament.uk/pa/jt201314/jtselect/jtpebs/27/2704.htm)

<sup>13</sup> Although the numbers switching have increased by about 15% since the introduction of the 7 day switching service, the numbers involved are still only 2-3% of current accounts. See, for example, [ft.com/cms/s/0/fe110e34-0d8d-11e4-815f-00144feabdc0.html#axzz3Aj4k6oSf](http://ft.com/cms/s/0/fe110e34-0d8d-11e4-815f-00144feabdc0.html#axzz3Aj4k6oSf)

## 2.4 Current government interventions aimed at improving access to data

The importance of information flows to this market is reflected in a number of recent Government interventions, which are designed to open up access to account and credit data to a wider range of market participants:

- At Budget 2014, HM Treasury announced an agreement with the largest UK banks that they would provide their customers with access to their transaction history data in a standard format, through the manual download of a CSV file as part of the Midata initiative. The stated objective is that the data could be used by comparison services to help customers understand which current account suits them best.<sup>14</sup> This is due to be implemented by March 2015.
- In June 2014, HM Treasury concluded a consultation which proposed to improve access to SME credit data by ensuring that this data is shared through Credit Reference Agencies (CRAs) with equal access for alternative lenders.<sup>15</sup> The objective of the reform is to diversify the supply of credit to SMEs. The data in question here is a) 'key indicators of current account performance' and b) data relating to the performance of credit facilities.
- In May 2014, the Bank of England published a discussion paper that considers options for further improving the availability of credit data in the UK.<sup>16</sup> The objectives are diverse; ranging from a more robust and diverse supply of credit to SMEs with lower barriers to potential entrants to better data for policymakers and regulators. The policy options under consideration include a comprehensive register of businesses, and a central credit register.

Collectively these measures constitute a significant step forward, and are to be welcomed. However, they could be developed further through the application of more widely-used technology approaches that have the potential to enable more sophisticated data sharing.

Chapter 3 introduces these concepts and describes how they could be applied to bank data.

---

<sup>14</sup> [gov.uk/government/news/government-to-make-it-easier-to-check-that-youve-got-the-right-bank-deal](http://gov.uk/government/news/government-to-make-it-easier-to-check-that-youve-got-the-right-bank-deal)

<sup>15</sup> [gov.uk/government/consultations/competition-in-banking-improving-access-to-sme-credit-data](http://gov.uk/government/consultations/competition-in-banking-improving-access-to-sme-credit-data)

<sup>16</sup> [bankofengland.co.uk/publications/Documents/news/2014/dp300514.pdf](http://bankofengland.co.uk/publications/Documents/news/2014/dp300514.pdf)

## **3 An introduction to the technology concepts that could enable better data sharing in banking**

This chapter outlines some of the key technology concepts that could be employed to help deliver better data sharing in banking.

The chapter is structured as follows:

<b>3.1 Technology concepts for better data sharing</b>	<b>16</b>
<b>3.2 APIs</b>	<b>16</b>
<b>3.3 OAuth</b>	<b>22</b>
<b>3.4 Open Data Standard</b>	<b>25</b>

### **Key messages**

- 1) APIs allow different software applications to communicate with each other and exchange data directly, without the need for human input each time. They have become the de facto standard for sharing data, and have enabled organisations that hold large amounts of data to become platforms for third party innovation.
- 2) OAuth is a widely used standard that provides a simple and secure mechanism for users to authenticate themselves, and authorise how their data can be shared. It allows a user to initiate the sharing of their personal data between different organisations without sharing their login credentials.
- 3) Open data provides a gold standard for publishing non-personal data in a way that maximises its potential value by creating the best possible environment for its re-use.
- 4) Banks outside the UK have started to make use of all three technology concepts. Banks in the UK are by and large yet to do so.

### 3.1 Technology concepts for better data sharing

The limitations described in the previous chapter are in large part a function of the approach to data sharing, and the technology concepts being applied.

However, there are a number of well established principles that underpin a well functioning data ecosystem. Technology and standards have been developed to instantiate these principles.

Application of the appropriate principles technology and standards to the bank data use case has the potential to overcome the limitations described above. Three are particularly relevant here, as shown in the table below.

**Table 2: Principles for data sharing**

Principle	Relevant technology and standards
For data sharing to be useful to users, it should be simple, low friction and scalable. <sup>1</sup>	<b>The API</b> is a technology concept that allows different software applications to communicate with each other and exchange data directly, without the need for human input each time.
Users should provide fully informed consent before their personal data is shared and should remain in control of how it is used.	<b>OAuth</b> is a widely used standard that provides a simple and secure mechanism for users to authenticate themselves, and authorize how their data can be shared.
To create optimal conditions for innovation, datasets that do not contain personal or commercially sensitive information should be made as accessible as possible.	The concept of <b>open data</b> sets out how data can be made available for anyone to use freely, for any purpose, providing a 'permission free' basis for 'serendipitous reuse'.

The remainder of this report will assess how the application of these more widely-used approaches sharing data around the web can be used to further the objective of making the UK banking market deliver better outcomes for consumers and SMEs.

The remainder of this chapter provides a brief introduction to each of the three concepts that the report will draw on, and how they relate to banking.

### 3.2 APIs

APIs (Application Programming Interfaces) are standards that allow software components to interact and exchange data, particularly over the web.

Put most simply, an API is a set of instructions that allows one piece of software to interact with another. For any given piece of software an API specifies:

- a mechanism for connecting with the software
- the data and functionality that is made available for this software, and
- what rules other pieces of software need to follow to interact with this data and functionality.

Before APIs became prevalent, pieces of software tended to work in isolation. Getting two pieces of software to work together (for example, pre-internet computer networks or early electronic mail services) involved building bespoke one-off connections between them that tended to be



rigidly defined around a single use case, and therefore fragile and slow.

As standardised APIs began to grow in popularity, they brought with them an era in which it became the norm for applications to begin to work together.

### **Internal APIs**

In many cases, APIs are used to facilitate interactions between applications held within a single organisation. APIs are often used to connect internal datasets and processes with each other, and to build layers of functionality upon them.

A very common use case for 'internal' APIs is the mobile phone application. Any organisation that has an 'official' application that draws on data held remotely will use an API to do so. Apps like Gmail, Twitter, Facebook, Paypal and those of many banks use APIs to draw data from their servers and display it on the user's phone when they want to read their email, tweet, update their status or check their balance. Although banks were perhaps a little late to bring out their own mobile applications, they now use internal APIs like most other organisations to provide this service.

### **External APIs**

However, internal APIs are only part of the story. Some of the more innovative uses of this technology are those in which organisations use APIs to allow external software to interact with their applications and data. APIs that are accessible to third parties are often referred to as 'public'.

APIs are an attractive method for an organisation to provide access to its applications. A well documented API means that without having intimate knowledge of a piece of software or any access to its code, a developer can build applications that interact with it. Furthermore, the API means that only the desired aspects of software functionality are exposed, with the rest of the application protected (for example, an API might allow 'read only' access to certain data fields without allowing them to be altered, and without revealing other adjacent data fields). In this respect, it is crucial to note that it is rare for public APIs to be truly open and unregulated - most organisations will create limits around what the API will access and who is able to connect to them.

The use of APIs to enable this kind of third party access has grown rapidly over the last decade. The ProgrammableWeb, a public directory of web APIs has grown the size of its records from just one in 2005 to a current count of 11,637. Most of this growth has come since 2010 when there were only 2,000.<sup>17</sup>

The growth in the use of public APIs reflects the fact that there are a number of ways in which organisations can benefit from allowing their software and data to interact with third parties. For some companies, their APIs are their core business model. Twillio, for instance, provides a service that allows partners to send and receive voice and SMS communications.<sup>18</sup> When a customer receives an SMS message telling them that their Uber driver has arrived, this is powered by the Twillio API.<sup>19</sup> Other companies use APIs to allow third party apps or websites to syndicate their content and functionality. Google maps, Accuweather updates, Amazon product advertising,

---

<sup>17</sup> [programmableweb.com/api-research](http://programmableweb.com/api-research)

<sup>18</sup> [twillio.com](http://twillio.com)

<sup>19</sup> [twillio.com/customers/stories/uber](http://twillio.com/customers/stories/uber)

Facebook 'likes' and 'shares' and youtube videos are all embedded in third party websites using their respective APIs. In general, as the array of API enabled devices and services grows, so too does the range of ways that they can be connected. You can even connect the lights in your living room to ESPN so that they flash when your football team scores, or to your calendar so that they blink on your birthday.<sup>20</sup>

### **The use of external APIs to create platforms for third party innovation**

The use case that is arguably most applicable to banks is that in which organisations use public APIs to allow external parties to add functionality to their core offer. The underlying logic is that a potentially large number of third parties can bring ideas and customers that extend way beyond the original organisation's scope. If this strategy is executed successfully, the original organisation can become a 'platform' for third party innovation.

This strategy has been used to great success by a large number of organisations. For example:

- Apple's App Store is considered the quintessence of a platform that has successfully leveraged third party innovation. Apple's APIs allow third party software in its app store to connect to hardware and software components on the iPhone, such as the camera, the GPS sensor, the photo library or the contacts list. There are now 1.2 million apps on the app store, which have been downloaded 75 billion times.<sup>21</sup>
- Salesforce.com's API ecosystem also operates on an immense scale. It comprises over 800,000 developers who have built more than 4 million applications that run on the force.com platform<sup>22</sup>. Salesforce.com states that API calls drive more than 60% of the total traffic to its site<sup>23</sup>, and generated more than half of its \$2.3bn revenue in 2012<sup>24</sup>.
- eBay has an 'app center'<sup>25</sup> that contains about 90 applications that use eBay's APIs to provide additional functionality for users. These range from inventory management tools<sup>26</sup> to automated 'thank you' emails<sup>27</sup>.

### **The use of external APIs by banks**

Although no UK bank has exposed APIs to become a platform for third party innovation, some other banks internationally are starting to experiment with this approach. The following table shows examples of banks and banking markets where APIs are currently used.

---

<sup>20</sup> [mashable.com/2013/08/17/iftt-best-recipes/](http://mashable.com/2013/08/17/iftt-best-recipes/)

<sup>21</sup> [techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/](http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/)

<sup>22</sup> [salesforce.com/platform/overview/?d=7013000000lan8](http://salesforce.com/platform/overview/?d=7013000000lan8)

<sup>23</sup> [venturebeat.com/2013/08/31/api-economy/](http://venturebeat.com/2013/08/31/api-economy/)

<sup>24</sup> [forbes.com/sites/ciocentral/2012/08/29/welcome-to-the-api-economy/](http://forbes.com/sites/ciocentral/2012/08/29/welcome-to-the-api-economy/)

<sup>25</sup> [applications.ebay.com/](http://applications.ebay.com/)

<sup>26</sup> [applications.ebay.com/selling?ViewEAppDetails&stab=1&mId=745&appType=1&appld=thank\\_you.3dsellers.com](http://applications.ebay.com/selling?ViewEAppDetails&stab=1&mId=745&appType=1&appld=thank_you.3dsellers.com)

<sup>27</sup> [applications.ebay.com/selling?ViewEAppDetails&stab=1&mId=745&appType=1&appld=thank\\_you.3dsellers.com](http://applications.ebay.com/selling?ViewEAppDetails&stab=1&mId=745&appType=1&appld=thank_you.3dsellers.com)

Table 3: Existing usage of APIs by banks

Bank	Country	Use of APIs
Crédit Agricole	France	Crédit Agricole launched its own app store, CA store, in 2012. <sup>28</sup> The logic, as described by Bernard Larrivière, head of innovation at Crédit Agricole, was that “Every [piece of] data the customer creates in his relationship with the bank, or any partner, is his own property so he should have access to it, but he should have access to it in apps that are useful to him.” <sup>29</sup> Apps on the CA store allow the customer to change the currency their account is displayed in, <sup>30</sup> to see the location of their transactions on a map, <sup>31</sup> to manage healthcare expenses, <sup>32</sup> and even turn saving into a game. <sup>33</sup>
AXA Banque	France	AXA Banque opened up an API to account data in 2012 <sup>34</sup> and then ran a competition for independent developers to use it to build applications. The prize winner was a money management and spend tracking dashboard. <sup>35</sup>
Capital One	US	Capital One has four public APIs. Although they have not yet implemented data access, third parties can authenticate customer identity and integrate with Capital One’s Digital Deals and Rewards programmes. <sup>36</sup> Capital One is keen to extent it’s API programme further.
BBVA	Spain	BBVA has built a strong developer community using Innovation Challenges based around reuse of aggregated (though not personal level) data. They are now in the process of building and rolling out APIs across different aspects of their business. <sup>37</sup>
Banco Sabadell	Spain	Banco Sabadell has launched an ‘Open Apps’ innovation programme <sup>38</sup> that provides limited access to some APIs for trusted developers. Perhaps curiously, one of the first integrations they sponsored was with Google Glass, enabling users to see their account balance or receive directions to an ATM. <sup>39</sup>
Fidor Bank	Germany	Fidor Bank is currently developing its API platform for developers. It is engaging independent developers throughout the process, in order to ensure that it builds the “best and developer friendliest APIs a bank can offer”. <sup>40</sup> It has a roadmap that will open a very wide range of functionality to third parties - starting with transfers, payments and account views before moving on to more complex transactions like KYC verification and new account creation. <sup>41</sup>
Bradesco	Brazil	Bradesco built a set of API’s to integrate with Facebook. The app allows customers to check their bank balance and make transactions from within Facebook. <sup>42</sup> Although this was a ‘closed’ partnership rather than an ‘open’ API strategy, it nevertheless illustrates the potential of integrating with third party applications.

<sup>28</sup> [creditagricolestore.fr/](http://creditagricolestore.fr/)

<sup>29</sup> [europeanpaymentscouncil.eu/index.cfm/newsletter/article/?articles\\_uuid=42210000-5056-B741-DB0CD1AA4E9F34EA](http://europeanpaymentscouncil.eu/index.cfm/newsletter/article/?articles_uuid=42210000-5056-B741-DB0CD1AA4E9F34EA)

<sup>30</sup> [creditagricolestore.fr/application-convertissor.html](http://creditagricolestore.fr/application-convertissor.html)

<sup>31</sup> [creditagricolestore.fr/application-j-etais-ou.html](http://creditagricolestore.fr/application-j-etais-ou.html)

<sup>32</sup> [creditagricolestore.fr/application-mon-budget-sante.html](http://creditagricolestore.fr/application-mon-budget-sante.html)

<sup>33</sup> [creditagricolestore.fr/application-ma-tirelire.html](http://creditagricolestore.fr/application-ma-tirelire.html)

<sup>34</sup> [developer.axabanque.fr/presentation](http://developer.axabanque.fr/presentation)

<sup>35</sup> [developer.axabanque.fr/le-grand-gagnant-2012](http://developer.axabanque.fr/le-grand-gagnant-2012)

<sup>36</sup> [developer.capitalonelabs.com/apis](http://developer.capitalonelabs.com/apis)

<sup>37</sup> [developer.bbva.com/](http://developer.bbva.com/)

<sup>38</sup> [bancsabadell.com/cs/Satellite/SabAtl/SabadellOpenApps/6000010169279/en/](http://bancsabadell.com/cs/Satellite/SabAtl/SabadellOpenApps/6000010169279/en/)

<sup>39</sup> [finextra.com/news/fullstory.aspx?newsitemid=25332](http://finextra.com/news/fullstory.aspx?newsitemid=25332)

<sup>40</sup> [developer.fidortecs.com/developer-partner-day-2014-munich/](http://developer.fidortecs.com/developer-partner-day-2014-munich/)

<sup>41</sup> [slideshare.net/Ficoba/here-you-will-soon-see-the-full-slides-of-the-presentation-fidor-api-for-developers](http://slideshare.net/Ficoba/here-you-will-soon-see-the-full-slides-of-the-presentation-fidor-api-for-developers)

<sup>42</sup> [industry.shortyawards.com/category/6th\\_annual/financial\\_services/dM/fbanking-bradesco](http://industry.shortyawards.com/category/6th_annual/financial_services/dM/fbanking-bradesco)

Bank	Country	Use of APIs
Garanti	Turkey	Turkey's second largest bank, Garanti, opens up its APIs to partners who want to integrate with them. <sup>43</sup> It has a large range of applications for customers, which mixes those built in-house with others designed by third parties.
<i>Banks not public yet</i>	Nigeria	Several large banks in Nigeria are currently deploying the Open Bank Project API, with rollout scheduled for Q4 2014. <sup>44</sup> This will provide customers with full API access to their data, and a readymade ecosystem of more than 100 applications. <sup>45</sup>
<i>FinTS - Multiple banks</i>	Germany	FinTS (Financial Transaction Services) is a publicly available open protocol managed by DK (die Deutsche Kreditwirtschaft, the German Bankers Association). It was conceived in 1995, as the HCB <sup>46</sup> Home Computer Banking Interface, as a standard to enable many small banks to grant "home banking" access to customers without the need for them to all invest in front-end internet banking interfaces. Over several versions security and functionality were enhanced. Most regular banking and some wealth management services are possible through third party "front ends", as well as the aggregation of multiple accounts from different institutions.
<i>OFX - Multiple banks</i>	US	Open Financial Exchange (OFX) <sup>47</sup> is a standard for bank data access that was created in 1997 by Microsoft, Intuit, and CheckFree to allow exchange of data between their software and their customers' banks. It is used by popular tools such as Microsoft Money, Quicken, and supported by over 5,500 banks and brokerages. It enables many features, such as access to transaction data, initiating payments and transfers, and recently multi-factor authentication. However, unlike more modern web APIs like Crédit Agricole or the Open Bank Project, it does not allow secure third-party delegation.
BBVA	Spain	BBVA has built a strong developer community using Innovation Challenges based around reuse of aggregated (though not personal level) data. They are now in the process of building and rolling out APIs across different aspects of their business. <sup>48</sup>
Banco Sabadell	Spain	Banco Sabadell has launched an 'Open Apps' innovation programme <sup>49</sup> that provides limited access to some APIs for trusted developers. Perhaps curiously, one of the first integrations they sponsored was with Google Glass, enabling users to see their account balance or receive directions to an ATM. <sup>50</sup>

### The use of external APIs in markets closely related to banking

In markets closely related to banking, public APIs are increasingly widely used.

For example, the vast majority of payments providers use APIs to allow third parties to implement their services. Paypal have been running a developer programme since 2009<sup>51</sup>. Mastercard<sup>52</sup> and

<sup>43</sup> [i-amonline.com/wp-content/uploads/Garanti-Contagious.pdf](http://i-amonline.com/wp-content/uploads/Garanti-Contagious.pdf)

<sup>44</sup> [eviscape.com/evis/tesobe-and-vanso-partner-to-bring-the-open-bank-pr-hhfgfxme/](http://eviscape.com/evis/tesobe-and-vanso-partner-to-bring-the-open-bank-pr-hhfgfxme/)

<sup>45</sup> [openbankproject.com/en/apps/](http://openbankproject.com/en/apps/)

<sup>46</sup> <http://www.hbci-zka.de/english/>

<sup>47</sup> OFX: <http://www.ofx.net/>

<sup>48</sup> [developer.bbva.com/](http://developer.bbva.com/)

<sup>49</sup> [bancabadell.com/cs/Satellite/SabAtI/SabadellOpenApps/6000010169279/en/](http://bancabadell.com/cs/Satellite/SabAtI/SabadellOpenApps/6000010169279/en/)

<sup>50</sup> [finextra.com/news/fullstory.aspx?newsitemid=25332](http://finextra.com/news/fullstory.aspx?newsitemid=25332)

<sup>51</sup> [developer.paypal.com/](http://developer.paypal.com/)

<sup>52</sup> [developer.mastercard.com/portal/dashboard.action](http://developer.mastercard.com/portal/dashboard.action)

VISA<sup>53</sup> also both have APIs and developer programmes, as do Amazon Payments<sup>54</sup> and Google wallet.<sup>55</sup> API integration is central to more recent entrants to the market, such as GoCardless<sup>56</sup> and Stripe<sup>57</sup> who have built products that are designed to be quick, easy and flexible for merchants to integrate with. Many of these APIs offer services beyond core payment processing. By integrating with Amazon or Paypal, a merchant can automatically pre-populate a customer's delivery address and run fraud checking. Google Wallet allows integration with loyalty and rewards programmes.

Small business accounting packages also make extensive use of APIs to let third parties integrate with them and expand the functionality they offer to their consumers. Intriguingly, they do this to provide access to very similar data to that which is held by banks. There are currently over 350 'add-ons' available on Xero's platform.<sup>58</sup> These range from cash flow forecasting and budgeting tools,<sup>59</sup> to point-of-sale devices for retailers that submit data directly from each sale to the company's accounts.<sup>60</sup> Kashflow also has a large variety of add-ons on its platform, which offer an equally impressive range of functionality<sup>61</sup>. Accounting software providers tell us that these add-ons are extremely popular with their SME customers. For more information see 4.2.3.

Providers of personal finance management software are using public APIs to extend their customer offer in precisely the same way. For example, Geezeo provides a white labelled finance management platform to retail financial services providers. It uses its API to encourage third parties to integrate with it to provide services such as budgeting, goals, cash flow calendar, net worth calculator and alerts.<sup>62</sup> Other providers of personal finance management software such as MoneyDesktop and Yodlee also make their APIs available.

Intriguingly, banks are among the big customers of these APIs. Moven has integrated with MoneyDesktop.<sup>63</sup> Regions Bank and Wescom Credit Union use Geezeo.<sup>64</sup> Banks who do not provide access to their own data and functionality are still choosing to integrate with other software providers who have.

In Chapter 4, we provide examples of some of the functionality that third parties would be able to build if they were able to access bank account data over an API.

### **Overview of the additional functionality that APIs offer relative to the manual download of static files containing bank account transaction data**

Currently, consumers and SMEs who want to access their bank account data in the UK typically have to manually download it as a static file. Accessing this data over an API has a number of distinct advantages over this approach<sup>65</sup>.

---

<sup>53</sup> [developer.visa.com/vpp/](https://developer.visa.com/vpp/)

<sup>54</sup> [payments.amazon.com/developer](https://payments.amazon.com/developer)

<sup>55</sup> [developers.google.com/wallet/](https://developers.google.com/wallet/)

<sup>56</sup> [developer.gocardless.com/#introduction](https://developer.gocardless.com/#introduction)

<sup>57</sup> [stripe.com/docs/api](https://stripe.com/docs/api)

<sup>58</sup> [xero.com/uk/add-ons/](https://xero.com/uk/add-ons/)

<sup>59</sup> [floatapp.com/xero](https://floatapp.com/xero)

<sup>60</sup> [vendhq.com/tour/add-ons](https://vendhq.com/tour/add-ons)

<sup>61</sup> [kashflow.com/add-ons/](https://kashflow.com/add-ons/)

<sup>62</sup> [developers.geezeo.com/](https://developers.geezeo.com/)

<sup>63</sup> [moneydesktop.com/culture/releases/2014/03/13/Moven\\_and\\_MoneyDesktop\\_announce\\_partnership/](https://moneydesktop.com/culture/releases/2014/03/13/Moven_and_MoneyDesktop_announce_partnership/)

<sup>64</sup> [developers.geezeo.com/](https://developers.geezeo.com/)

<sup>65</sup> At least in part as a result of the limitations described here, whilst transaction history downloads are already widely available for energy customers, they are rarely used by third parties.

**Table 4: Comparison – static file download vs API access**

	Static File Download	API Access
Effort required to set up data access	Downloading .csv files and then re-uploading them to a third party is a relatively high friction process.	Authorising an API connection between a bank and a third party only requires inputting a username and password (see discussion of OAuth below), and data can then flow to a third party without any further effort from the consumer.
Effort required to maintain data access	Because the file downloaded is static, the data inside it starts to age immediately. To keep it up to date involves the user repeating the download / upload process regularly.	APIs can be configured to automatically refresh the data at the required interval (up to and including real time)
Data integrity	Once a file has been downloaded there is no guarantee that it has not been tampered with, which makes it less suitable for some use cases (such as assessments of creditworthiness by potential lenders).	APIs allow third parties to access data directly from source.
Data security	Consumers’ home PCs are more likely to represent a security vulnerability than enterprise or cloud servers, and so storing downloaded data may involve greater risk.	APIs enable data to be shared with third parties without having to pass through the user’s machine first.
Ease of use for developers		Developers tend to prefer to work with APIs, and can build more dynamic services with them than they are able to with static files

### 3.3 OAuth

When data is shared between applications, access controls are required. It is essential that the person whom the data belongs to can authenticate their identity, and authorise the terms on which their data is shared.

For many years, the prevailing approach to this kind of data sharing was for a ‘client application’ (e.g., “The Data App”) to ask for a user’s login details to a ‘service provider’ (e.g., “The Bank”), and then to login to the user’s account on their behalf, and ‘scrape’<sup>66</sup> their data. We refer in other chapters to Yodlee, which is a major “screen scraper”, especially in the US.

This approach has a number of serious limitations:

- “The Data App” now has full access to the user’s account at “The Bank”. Depending on what the account is “The Data App” (or a rogue employee) could buy or sell things, send emails, transfer money, or change the password and lock the user out.
- Even if “The Data App” is wholly trustworthy, they now have an unencrypted (or decryptable) copy of the login details on their servers which could be hacked.
- Even if “The Data App” only needs access to a small subset of data points to provide its service,

<sup>66</sup> See [http://en.wikipedia.org/wiki/Data\\_scraping](http://en.wikipedia.org/wiki/Data_scraping) for a definition of data scraping.

it has access to the full range of data in the account.

- “The Bank” often cannot tell whether it is the user logging in, or “The Data App” on their behalf.
- By giving out their login details to “The Data App”, the user may now be in breach of terms and conditions associated with their account, which can strip them of certain consumer protections.
- Because the access is not officially authorised by “The Bank”, nor is it properly specified. Therefore, there is no guarantee that the data “The Data App” receives is accurate. Inaccuracies can occur when ‘scraping’ technologies are used to gather data, in particular when page layouts and formats are restyled by the bank.<sup>67</sup>

In response to these problems<sup>68</sup> many web companies started to look for ways to provide users with safer and more convenient ways to authenticate themselves and manage third party access to their data. After initially building their own protocols,<sup>69</sup> many large web services started to converge on a single standard; OAuth.<sup>70</sup> Now deployed by major network services like Google, LinkedIn, Facebook, and Twitter, OAuth has arguably become the *de facto* standard for authentication and authorization on the web.

Most simply put, OAuth is an open standard that allows users to authorize one application to interact with another on their behalf. Its widespread adoption reflects a number of important advantages that it brings:

- 1) **It is very user friendly.** If a user wants to provide “The Data App” with access to their data on “The Bank”, they are sent to “The Bank” where they simply login as normal, views the proposed terms of access for “The Data App”, and then clicks a button to authorize them. “The Data App” and “The Bank” then use the OAuth protocol to set up the data exchange between them.<sup>71</sup> The user does not need to manually upload or download data, and once the connection between “The Data App” and “The Bank” is established it can be left to run for a specified period of time.
- 2) **It does not involve sharing sensitive login details or passwords.** Once the user has told “The Bank” that they want their data shared with “The Data App”, tokens are exchanged between the two applications to enable the exchange. At no point in the process does “The Data App” get any access to the users login credentials or password. This dramatically reduces the risks to the user of “The Data App” being hacked, or containing rogue employees<sup>72</sup>. For this reason OAuth is attractive to developers who want to create login functionality but do not want to worry about storing passwords.
- 3) **Access to the user’s data is limited.** A chosen set of data and functionality is exposed to an API, but everything else is protected. See (Chapter 5\*\*) for an illustrative outline of the different components that a current account could be broken down into. Access to each could be

---

<sup>67</sup> This is because scrapers need to be updated every time even the slightest change is made to the way that the data is presented at source.

<sup>68</sup> Which were known as the ‘password anti-pattern’. See [designingsocialinterfaces.com/patterns/The\\_Password\\_Anti-Pattern](http://designingsocialinterfaces.com/patterns/The_Password_Anti-Pattern)

<sup>69</sup> For example, Google, Yahoo and Flickr all had their own Auth mechanisms, each of which has now been superseded by OAuth.

<sup>70</sup> [oauth.net/](http://oauth.net/)

<sup>71</sup> This process works through the exchange of a number of different tokens. For an accessible explanation of the detail, see Chapter 3.

<sup>72</sup> For an example of the benefits of OAuth in the scenario that a site is hacked, see [lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook](http://lifehacker.com/5918086/understanding-oauth-what-happens-when-you-log-into-a-site-with-google-twitter-or-facebook)

chosen independently depending on what data the Third Party requires. OAuth use the analogy of a 'valet key' to help explain the concept of limited access. "Many luxury cars today come with a valet key. It is a special key you give the parking attendant and unlike your regular key, will not allow the car to drive more than a mile or two. Some valet keys will not open the trunk, while others will block access to your onboard cell phone address book. Regardless of what restrictions the valet key imposes, the idea is very clever. You give someone limited access to your car with a special key, while using your regular key to unlock everything."<sup>73</sup>

- 4) **The user has fine-grained control over the data being shared.** The limits on what is exposed and what is protected can be very granular and very transparent. The exact terms of access are presented to the user at the point where they choose whether or not to authorize them. See the example below, where the dialogue box describes what bitly will and will not be able to do with the User's twitter account.

**Figure 1: An example OAuth authorisation page**



Source: Twitter

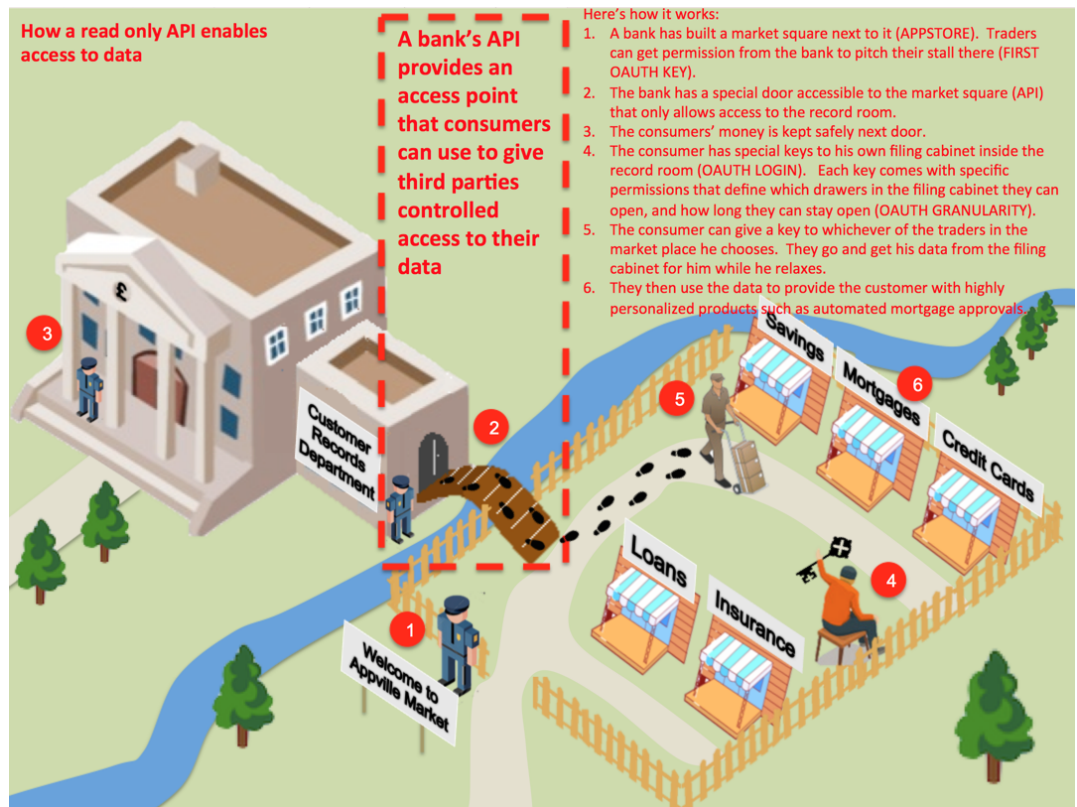
- 5) **The user remains in control throughout.** The user can revoke "The Data App's" access at any time, directly through "The Bank", as shown in the grey box at the bottom of the above example. In the event of an untrustworthy application or security breach in "The Data App", "The Bank" can also revoke "The Data App's" access to all data, without affecting the users access to "The Data App".

<sup>73</sup> [oauth.net/about/](https://oauth.net/about/)



6) **OAuth is an open protocol.** This means it can be reused by anyone without cost, which has helped spread adoption. Open standards are *de facto* more secure than proprietary standards, as their specifications will have been evaluated by many more security professionals than for proprietary standards. Also, many implementations of OAuth are open source and will have been inspected for bugs and vulnerabilities by very large numbers of developers.

**Figure 2: A visual representation of how APIs and OAuth interact to enable the sharing of bank data**



Source: Fingleton Associates

### 3.4 Open Data Standard

The Open Definition summarises open data as follows:

*“A piece of data or content is open if anyone is free to use, reuse, and redistribute it — subject only, at most, to the requirement to attribute and/or share-alike.”*

**Open Definition ([opendefinition.org](http://opendefinition.org))**

Open data is easily accessible, usually through the web, machine-readable, and has a clear open licence that states that anyone can use it for any purpose.

Evidence is beginning to emerge about the economic impact of open data:

- A McKinsey report from 2013 estimates the value of the open data marketplace at \$3-5 trillions per year.<sup>74</sup>
- A Lateral Economics study commissioned by the Omidyar Network estimates that open data policies by G20 nations could contribute 1.1 per cent to GDP growth.<sup>75</sup>
- Open data published by Transport for London has saved public transport users £15-58 million in time per year.<sup>76</sup>
- The Climate Corporation, a startup providing agricultural forecast modelling based on open weather data, was sold for \$1.1 billion in October 2013.<sup>77</sup>

A variety of open data relating to the UK banking sector is already available. For example:

- The Bank of England publishes monthly aggregate data about macroprudential indicators such as total levels of consumer credit or lending secured on dwellings in the economy.<sup>78</sup>
- The British Banker's Association (BBA) and Council for Mortgage lenders have published data about SME and personal lending by postcode.<sup>79</sup>
- the Financial Ombudsman publishes data on complaints about financial products, and the way that companies handle these complaints.<sup>80</sup>

Some financial services companies are also starting to publish their own open data. For example the peer to peer lending sector also published open data on lending flows to give a snapshot of the market in 2013.<sup>81</sup> Funding Circle publishes live, aggregate data on the performance of its loan book.<sup>82</sup>

Looking beyond the UK, Spanish bank BBVA has been at the forefront of efforts to explore the potential value of open data. In Dec 2013 and March 2014 it ran innovation challenges in which developers were able to access aggregated, anonymised data for 30 million transactions conducted 2012 and 2013, over an API.<sup>83</sup> A range of different applications were produced, including;

- QKLY, which analyses when different stores were most crowded, so that customers can avoid queues and businesses can manage demand more efficiently.<sup>84</sup>
- Chances, an application that advises businesses on where to open store locations based on how many customers a location gets, what type of customer they are, how much they spend,

---

<sup>74</sup> [http://www.mckinsey.com/insights/business\\_technology/open\\_data\\_unlocking\\_innovation\\_and\\_performance\\_with\\_liquid\\_information](http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information)

<sup>75</sup> [http://www.omidyar.com/sites/default/files/file\\_archive/insights/ON\\_Report\\_061114\\_FNL.pdf](http://www.omidyar.com/sites/default/files/file_archive/insights/ON_Report_061114_FNL.pdf)

<sup>76</sup> [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/198752/13-744-shakespeare-review-of-public-sector-information.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/198752/13-744-shakespeare-review-of-public-sector-information.pdf)

<sup>77</sup> [http://en.wikipedia.org/wiki/The\\_Climate\\_Corporation](http://en.wikipedia.org/wiki/The_Climate_Corporation)

<sup>78</sup> [bankofengland.co.uk/statistics/Pages/bankstats/2014/jun.aspx](http://bankofengland.co.uk/statistics/Pages/bankstats/2014/jun.aspx)

<sup>79</sup> [bba.org.uk/news/statistics/postcode-lending/](http://bba.org.uk/news/statistics/postcode-lending/)

<sup>80</sup> [financial-ombudsman.org.uk/publications/complaints-data.html](http://financial-ombudsman.org.uk/publications/complaints-data.html)

<sup>81</sup> [smtm.labs.theodi.org/](http://smtm.labs.theodi.org/)

<sup>82</sup> [www.fundingcircle.com/statistics](http://www.fundingcircle.com/statistics)

<sup>83</sup> [press.bbva.com/latest-contents/press-releases/n-a\\_\\_9882-22-c-106697\\_\\_.html](http://press.bbva.com/latest-contents/press-releases/n-a__9882-22-c-106697__.html)

<sup>84</sup> [prezi.com/sdpy6xzfgixe/qkly-bbva-challenge-urbanbeers-2013/](http://prezi.com/sdpy6xzfgixe/qkly-bbva-challenge-urbanbeers-2013/)

and when then spend it.<sup>85</sup>

- Urbeo, which analyses the social and economic impact that a large event such as a sporting contest has on a city.<sup>86</sup>

The economic case for publishing further banking data as open data was made by McKinsey, whose research from 2013 estimated that making consumer finance data more accessible could generate \$210 - \$280bn of value globally. Although much of their analysis involves the use of wider sources of data by banks, they also argue that data on fee structures, or the features of mortgages, credit cards and pensions could be valuable in improving consumer choice.<sup>87</sup>

In Chapter 4, we provide examples of some of the additional datasets that could be provided as open data, and the uses that a range of organisations would put this data to.

---

<sup>85</sup> [centrodeinnovacionbbva.com/en/news/michele-trevisiol-alejandra-herandez-and-oscar-marin-winners-innova-challenge-big-data](http://centrodeinnovacionbbva.com/en/news/michele-trevisiol-alejandra-herandez-and-oscar-marin-winners-innova-challenge-big-data)

<sup>86</sup> *ibid*

<sup>87</sup> [mckinsey.com/insights/business\\_technology/open\\_data\\_unlocking\\_innovation\\_and\\_performance\\_with\\_liquid\\_information](http://mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information)

## 4 The potential uses of bank APIs

This chapter assesses the nature and level demand for bank APIs and open data amongst 25 potential users of data that we interviewed.

The chapter is structured as follows:

<b>4.1 Demand for bank APIs from third parties</b>	<b>31</b>
4.1.1 Consumer advice and comparison services	31
4.1.2 Alternative Lenders	33
4.1.3 Accounting Software	36
<b>4.2 Ways in which external APIs can create value for banks</b>	<b>39</b>
4.2.1 Current approach to data access	40
4.2.2 Quick wins for banks from exposing APIs	40
4.2.3 The strategic value of banks being a platform for third party innovation	41
<b>4.3 Demand for Open Data</b>	<b>44</b>
4.3.1 Lending: Refining risk models, lowering barriers to entry, identifying underserved segments of the market	44
4.3.2 Switching services: providing a 360° view on financial products	44
4.3.3 Money advice: Building predictive debt advice tools.	45

## Key messages

- 1) The demand for data is strong across alternative lenders, accounting software platforms, comparison and advisory services, payment services and others. Many of these organisations already create considerable value from data.
- 2) These organisations currently access data using means such as manual downloads, screen scraping, manual entry and occasionally bilateral data feeds. There is widespread consensus that these methods are hard to use, expensive, and have limited capabilities. Consequently, the desire to see banks provide external APIs was almost universal.
- 3) The use cases described have the potential to encourage competition in the PCA market and SME lending.
- 4) They also impact on other adjacent markets in ways which could be beneficial to SME productivity and consumer welfare.
- 5) Banks themselves could also stand to benefit from creating external APIs. Encouraging third party integration and becoming a 'platform' is potentially a strategy to mitigate the threat of being 'unbundled'.
- 6) Many of the use cases described rely on being able to access not just individual account data, but also aggregated data (anonymised account data) and reference data (banks' respective charges, terms and conditions), ideally published as open data. This includes the core 'Midata' account switching use case, which would benefit from more standardised data on PCA terms and conditions in achieving its potential.
- 7) Applying an open API standard across the whole sector would create the optimal conditions for the re-use of data. However, some organisations predicted that it would take considerable effort and co-ordination to achieve. .
- 8) Where API access to this kind of data has been made available, such as by accounting software providers and the Open Bank Project, it has resulted in successful ecosystems of third party applications. These could be replicated by banks.

**Table 5: Overview of the opportunities created for third parties by access to external bank APIs and the publication of open data**

Third party users	Opportunities created by bank APIs and the publication of open data
Consumer advice and comparison services	<ul style="list-style-type: none"> <li>a) Higher engagement with existing services</li> <li>b) Next generation comparison services</li> <li>c) Predictive and real-time advisory tools</li> <li>d) Mass market financial planning</li> </ul>
SME Lenders	<ul style="list-style-type: none"> <li>a) Increased speed and accuracy of credit assessment</li> <li>b) Reduced cost and friction of credit assessment</li> <li>c) Identity verification and fraud prevention</li> <li>d) Adaptive repayment services</li> <li>e) New financial management tools</li> </ul>
Accounting Software	<ul style="list-style-type: none"> <li>a) Productivity enhancing tools for SMEs</li> <li>b) Ability to offer a fully automated service to all SMEs</li> <li>c) Lower cost sign up</li> <li>d) New services</li> </ul>
Government and Regulators	<ul style="list-style-type: none"> <li>a) Smarter regulation.</li> <li>b) One click tax payment.</li> <li>c) Fraud prevention for government payments</li> </ul>

**Table 6: Overview of the opportunities created for banks by access to external bank APIs and the publication of open data**

Banks	Opportunities created by bank APIs and the publication of open data
Quick wins from external APIs	<ul style="list-style-type: none"> <li>a) Enhanced security</li> <li>b) Account history porting</li> <li>c) Digital sign up and identity verification</li> </ul>
Strategic opportunities from acting as a platform for third party innovation	<ul style="list-style-type: none"> <li>a) A varied suite of digital products</li> <li>b) A faster product development cycle</li> <li>c) A strategy to mitigate the impact of unbundling</li> <li>d) An opportunity to get ahead of PSD2</li> </ul>

## 4.1 Demand for bank APIs from third parties

In researching this chapter, we spoke to a range of organisations (see Introduction for list). For each of these groups, this chapter covers: their current approach to data access, what bank APIs would allow them to do differently and what aggregated or open data they would make use of.

### 4.1.1 Consumer advice and comparison services

High quality advice and comparison services have an important role to play in helping to foster competition in the PCA market. They can also enhance consumer welfare in adjacent market. Delegated access to a consumer's bank data has the potential to expand their ability to perform these functions, perhaps considerably.

#### Current approach to data access

**Price comparison websites** for financial products currently rely on personal information that users input directly. Because of the limitations of this, they rely to a great extent on users knowing what they “spend” on their bank account, which very few do. The advice given is therefore fairly generic, categorising customers into fairly broad categories such as - for Current Accounts - ‘mostly in credit’, ‘frequent overdraft user’ and making recommendations within equally broad categories of account, such as ‘best accounts with cashback’ or ‘accounts with good customer service.’

**Personal Financial Management (PFM)** tools require a range of personal financial information in order to provide customers with analysis of their spending or saving patterns. They have two main sources:

- **CSV file uploads** are a widely-available source of this information, but tend to be fiddly to work with.
- **Screen scraping** technology is used by some providers to provide more automated access to data<sup>88</sup>. However, as outlined at 3.1.2, there are several drawbacks to this method.
  - Firstly, passing security credentials to a screen scraping provider may breach bank terms and conditions. Only Lloyds currently expressly permits the use of third party scrapers. Other banks’ terms and conditions are either ambiguous or forbidding, which causes uncertainty for customers.
  - Secondly, the data can be unreliable. When a bank changes its screen design, scraped links often “break” while the new design is bedded in – perhaps for a matter of days.
  - Thirdly, token-based account access such as HSBC make access by screen scrapers impossible.
  - Fourthly, for some banks, the credentials handed over to a scraper allow full “read and

<sup>88</sup> Yodlee is the market-leading provider of financial screen scraping technology in the world, and are the dominant provider of these services to companies in the UK. They also provide a range of other value added financial data services. In the US about half of the data that they get from banks comes from direct integrations with the bank. However, no bank in the UK has yet allowed them to integrate. Although all of the drawbacks of screen scraping apply to Yodlee in principle, it should be mentioned that Yodlee’s security record is impeccable across billions of transactions globally.

write”, rather than just “read”. This would enable a third party with malicious intentions to not only read all the data, but to also initiate payments.

These limitations mean that customers are often reticent when it comes to passing over credentials to a third party. One provider told us that roughly half of all customers signing up drop out of the process when asked to hand over bank login details to a scraper.

- **Advisory Services** endeavour to provide personalised advice to their clients about issues ranging from wealth management to budgeting. In general they ask users to input data manually. This can be burdensome for users, and once again, this is the point at which a large number of potential users drops out. For example, the Money Advice Service’s (MAS’s) Budget Planner has a total of 143 fields to fill in.<sup>89</sup> MAS explained that a lot of their clients have regular access to smartphones, but not to desktop computers, making manual downloads impossible.

## What would APIs enable?

- 1) **Higher engagement with existing services.** Consumers are put off by the labour intensity of manually inputting information or manually uploading and downloading files. The use of screen scrapers makes things easier, but also puts off consumers because of the need to hand over sensitive login credentials. The use of APIs and OAuth to facilitate access to data provides the best of both worlds - a low friction process with high security authentication. It should result in more consumer engagement, particularly for the more data-intensive and non-automated services such as MAS’ budget planner.

In addition to broadening engagement with existing services, APIs create the possibility of a number of potentially useful, but currently out-of-reach applications.

- 2) **Next generation comparison services.** Comparison services would be able to apply the highly personalised, analytics driven approach of companies like BillMonitor to financial services. Billmonitor uses customers’ usage data and smart algorithms to show exactly which of the 1.91m phone tariff combinations on the market are best suited to their needs. It does this by interrogating the exact combination of minutes, data, texts, international calls etc. they have used over the past 6 months.<sup>90</sup>

This kind of approach has not yet been applied to retail banking, but would become possible with greater data access. Personal financial products are perfectly suited to next-generation comparison, and sophisticated intermediaries could help to empower consumers, driving greater switching levels. Consumers would benefit from greater insight into the costs and charges associated with their bank accounts, such as any monthly fees, forgone interest, and overdraft charges. They could also tell consumers which products are best suited to their needs, based on exactly how they use their accounts.

This is what the Midata initiative is seeking to achieve. Midata has the scope to help boost switching levels and therefore competition in the PCA market. Providing APIs as well as CSV

---

<sup>89</sup> 31 fields for inputting income, including 12 different benefits and tax credit fields, and 4 just for pensions. For outgoings, there are 30 fields for household bills, 24 for living costs, 27 for insurance and banking, 23 for friends and family, 18 for travel (car etc.), and 21 for leisure.

<sup>90</sup> To illustrate how powerful this kind of analysis can be in complex markets, billmonitor’s data show that 76% of people are on the “wrong” tariff, and spend an average of £194.71 per year more than if they were on the right tariff.



downloads could make tools and services that use this data both easier to use and, through the use of OAuth, more secure.

- 3) **Predictive and real-time advisory tools.** If advisory services were able to run an on-going connection to someone's bank account over an API, it is possible that they might be able to spot some of the early warning signals that indicate a risk of problem debt. Such a service could also be operated by a bank. For more detail on this see the discussion of open data below.

Similarly, if the API was live and enabled push notifications then services that offer more day to day advice could be enabled. This could be simple warnings when the balance goes below a certain threshold, or more sophisticated services. A good illustration comes from Moneyworks in the US<sup>91</sup>. While not yet launched, they plan to incorporate live bank account data with a wide variety of other data sources, such as positional (GPS or iBeacon) data. For example, if it knows that a user's bank account is running low, and it tracks the user going into Starbucks, it might send a message advising to forego that white chocolate mocha latte.

- 4) **Mass market financial planning.** Gaining access to trusted advice on financial planning can be challenging for many but the most wealthy. Prior to the Retail Distribution Review (RDR), high charges were extracted by the IFA industry, often using opaque commissions. But post RDR, now that the charges are more transparent, some may consider the cost of advice to be excessive, and will not pay for it. This points to a possible advice vacuum, and a number of businesses with intelligent tools believe that they can use automation to fill that vacuum. Several providers suggested that data driven planning tools with a complete picture of a user's finances, in terms of assets, liabilities, income and outgoings, can provide high quality advice. They also have the potential to bring down the cost of advice, and, so, make it accessible to a wider group of people.

### What else should we know?

The use cases described in this section would benefit from access to a range of financial data that goes beyond the current account. Advisory services would require access to credit cards and loans to provide meaningful feedback. Financial management tools would also need pensions, savings and potentially other assets too (though some of these could relatively easily be added manually).

Critically, next generation comparison tools, the core Midata use case, will benefit from aggregated data (anonymised account data) and reference data (banks' respective charges, terms and conditions), which should ideally be published as open data. See 4.3.2 below for details on this.

## 4.1.2 Alternative Lenders

### Current approach to data access

Data is a vital ingredient of lending decisions for all the lenders we spoke to. It is used to confirm a potential borrower's income, details of business costs, other cash outflows, and any other financial liabilities. No alternative lenders had direct APIs from banks, but instead accessed data

---

<sup>91</sup> <https://www.getmoneyworks.com>

about SMEs in a number of alternative ways:

- **Credit Reference Agencies** are widely-used credit data sources, but account-level information is only accessible on the basis of reciprocity, and so not to alternative lenders. Rather they receive a score based on proprietary factors and some truncated data (eg. overdraft: yes or no). Lenders recognised that the requirement to share data through CRAs would improve this channel but, had reservations about this intervention as outlined in 2.5 above.
- **Screen scraping.** As a result of the concerns about screen scraping described at 4.1.1 above, none of the lenders we spoke to currently deploy this technology, though several had considered or even trialled it.
- **Manual file handling.** Lenders do use PDF downloads, either emailed or printed, which they go through manually. Lenders stressed that data files uploaded by consumers could be easily manipulated - particularly if they are in an easily editable format, such as CSVs). Receiving machine readable data directly from banks is preferable for lenders.
- **Accounting software APIs.** Unlike banks, accounting software packages do issue APIs which lenders can use to quickly access some SME financial data. Several lenders make use of this data, and consider it an excellent template for direct access to bank accounts.

The point at which the lender asks for this data tends to be the point at which most “loss of business” occurs. Although some part of this drop out will be SMEs who don’t want to share their data, it is likely that the majority is caused by the levels of friction involved with most ways of providing the data at present.

### What would APIs enable?

Lenders were unanimously positive about the impact that API access to bank account data would have on their ability to make better lending decisions, to expand their lending and to compete with banks. Some went as far as to describe it as potentially transformative to SME lending.

As one interviewee expressed it, the banks’ control of the data gives them market power and limits competition. Success as a lender should be dictated by the ability to effectively price risk, not the ability to exert control over the most useful data.

All lenders said that they would build the functionality to use APIs quickly. Some lenders, such as MarketInvoice, FundingOptions<sup>92</sup> and Kabbage, have already integrated with the APIs provided by accounting software packages.<sup>93</sup>

A number of specific benefits were described:

- 1) **Increased speed and accuracy of credit assessment.** The core rationale for utilising APIs would be to improve the accuracy of credit assessment. As described above, most lenders already draw on whatever data they can access to do this. Universal, standardised access to bank account data would expand their abilities considerably. For example, it would allow proper checking of repayment affordability, something which cannot be done by alternative lenders

---

<sup>92</sup> <http://www.fundingoptions.com/blog/xero-and-freeagent-integrations-announced/>

<sup>93</sup> <http://marketinvoice.com/2014/07/28/partners-with-xero-to-offer-instant-funding-to-uk-businesses/>

today in the absence of consistent data on outgoings. It would also allow lenders to run sophisticated resilience tests, such as checking whether firms are reliant on large customers (who could be vetted separately if necessary).

As well as more accurate decisions, API access would also allow quicker decisions. Where lenders such as MarketInvoice have integrated with the APIs offered by accounting packages, this allows them to make a decision within 20 minutes of receiving an application.<sup>94</sup>

More than one lender suggested that API access could be asymmetrically beneficial for alternative lenders and other new entrants, as they believe they have better data analytics and risk modelling capabilities than incumbent banks.

- 2) **Reduced cost and friction of credit assessment.** Direct data access would also reduce the cost of credit assessment, for both parties in the transaction. Lenders currently spend a great deal of time asking for and processing information provided in inconvenient forms (such as scanned and emailed copies of banks statements). Borrowers spend a great deal of time providing them, and the frustration of doing so results in many dropping out of the process. With APIs implemented using OAuth authentication, all of this could be replaced with a few clicks of a mouse, saving both parties time, keeping more SMEs in the lending process, and resulting in lower lending costs. Indeed, this is already happening - where lenders have integrated with the APIs exposed by accounting packages, SMEs are able to make loan applications from within their accounting software in three clicks.<sup>95</sup>
- 3) **Identity verification and fraud prevention.** OAuth authentication could be used to provide automated and robust validation of account ownership. This would be a valuable anti-fraud measure. If configured to do so, the OAuth protocol could also be used to pre-populate some of the borrowers information (name, address etc), further reducing friction from the process.
- 4) **Adaptive repayment services.** If APIs enabled third parties to initiate payments as well as read account data, lenders could build innovative new product features around that. For example, a lender could analyse an SME's account balances, observe that they typically have more than, say, £10k in their account for 23 weeks of the year, and then price and offer an automatic repayment schedule that only triggers when the account is greater than this threshold and never takes it below £8k.
- 5) **New financial management tools.** If they were able to access data over an API, some lenders would also be interested in expanding their offer to include financial tools for customers, which would enable better understanding of cash flows, forecasting, advice on savings, and spending comparisons.

All lenders that we interviewed were sceptical about the value of manual downloads, in part because of how difficult they are for their customers to work with and in part because the provenance of the information they contain cannot be guaranteed once they have been downloaded. One lender suggested a workaround for this latter problem - building a system to effectively screen scrape the file directly from the SMEs online bank account - but since it would require the SME providing them with their login credentials they said they would be very reluctant to do this.

---

<sup>94</sup> <http://marketinvoice.com/2014/07/28/partners-with-xero-to-offer-instant-funding-to-uk-businesses/>

<sup>95</sup> <http://marketinvoice.com/2014/07/28/partners-with-xero-to-offer-instant-funding-to-uk-businesses/>

### What else should we know?

Some additional observations about data access:

- It is important that customers give explicit consent to data sharing and maintain control of their data using OAuth. Lenders thought that a large proportion of borrowers would understand why they were sharing their data, and would be happy to do so if it increased their chances of getting credit. However, more than one lender also suggested that something akin to a Kitemark, which certifies the data sharing practices, could be beneficial to secure trust.
- In an ideal world, historic bank account data would cover a whole economic cycle. However, lenders recognised that this was unlikely in the first instance and that SMEs would probably have to start building up their data history. If a minimum data standard was required, 3-5 years of historic data would be an acceptable baseline.
- All lenders pointed to the importance of consistent standards. This would allow them to build both technology and models that could apply to all banks and all firms. Where all banks have different standards, effort is wasted maintaining multiple different connections and building models that work with different sets of data. That said, one lender did point out that the alternative lenders themselves may be quicker to move than banks and so if they had to adapt to several protocols rather than wait for banks to reach an agreement on standards then they would.

#### 4.1.3 Accounting Software

##### Current approach to data access

Bank account data is used in accounting software packages as a means of reconciling paid customer invoice entries and outgoing payments or payroll with actual cash movements on the bank account, as well as current cash balances.

**Direct feeds** are the preferred source of data for providers. While UK banks do not offer APIs to third parties, three of the “big four” banks do have arrangements to provide data feeds to one or more accounting packages. The current relationships between banks and providers that exist are below.

**Table 7: Existing bank data feeds to accounting software**

Bank	"Tied" Accounting Package
HSBC	Xero, (Bankstream <sup>96</sup> )
Barclays	Freeagent, Sage, Crunch <sup>97</sup>
RBS (inc. NatWest)	(Bankstream)
Lloyds	No feeds

These feeds mimic some of the advantages of APIs, in that they allow the SME to delegate read access to their bank data, and once set up involve no maintenance burden for the SME.

However, these feeds they are not without their limitations. Firstly, the nature of these closed relationships mean that data access is patchy and require companies to strike bilateral commercial arrangements with banks. Not all banks are willing, and some want exclusivity. As a result, no accounting software provider is able to offer direct feeds to all of its customers. For example, Xero can only offer SMEs who bank with HSBC a data feed. This is a significant contrast to the market in New Zealand where Xero can utilise feeds from 18 banks, and 17 in Australia.

Secondly, in most cases the way that feeds are set up involves an arcane paper based process. The account holder must ask for a paper mandate form from the bank, complete and return it and then wait for days, maybe weeks, for the feed to be established. This is costly and time consuming to administer (certainly when compared to the automated and instantaneous authorisation provided by OAuth).

Where accounting software providers are unable to access direct feeds, they are left with three options:

- **Manual downloads.** By and large, providers prefer not to use this channel as their customers find it laborious and repetitive. One provider said that the burden of downloading and uploading CSV files is the single largest reason why they lose customers.
- **Print, scan and upload.** Bankstream describes this as a fairly common practice. Because their immediate users are accounting firms, rather than small businesses, this is done in batches with little resistance but it is usually impractical for small businesses to perform this themselves for direct-to-client software. Where accountants do it for their clients, the SME needs to share their account login credentials with their accountants; poor practice from a security perspective.
- **Screen scraping.** As with personal finance management tools above, some accounting software providers prefer to integrate with screen scraping services such as Yodlee to provide their customers with a more automated and less labour intensive means of accessing data. Again, the issue of potential customers dropping out of the signup process when asked to hand over

<sup>96</sup> Bankstream is not an accounting software package for business, but provides data from bank accounts directly to accountants on behalf of their clients.

<sup>97</sup> Crunch is an online accountant, incorporating software

login details was raised repeatedly. Nevertheless, one provider who is currently integrating with a screen scraping provider told us they expect that once they do, 50% of their SMEs will switch to it from manual downloads and as a consequence their customer churn will fall by 50%.

**What would APIs enable?**

Accounting software providers were very clear that having standardised API access to bank data would make a positive difference to their industry. And because they are designed to help make life easier for other SMEs, there is good reason to believe that better data access for them will have positive externalities across multiple markets.

Four key points stood out:

- 1) **Productivity enhancing tools for SMEs.** Modern accounting tools provide a wide range of functionality that is productivity enhancing for SMEs. Providers like Xero and Kashflow have done this by exposing APIs to their own data and functionality, which has provided the basis of a rich ecosystems of add-ons, akin to Apple’s App Store or Google Play.

The tables below provide examples of add-ons available in Xero and Kashflow.

**Table 8: Xero add-ons**

Xero Add-ons	Description
WorkflowMax	Generate quotes, time-sheets, job management (bought by Xero)
Receipt Bank	Digitises receipts
Vend	Instant reconciliation from in-store point-of-sale device into company accounts
Debtor Daddy	Allow set-and-forget limits, and automatic late payment notices for debtor management
ezyVet	Veterinary practice management, capturing entire end-to-end processes, from appointments to billing and payment reminders

Source: Xero

**Table 9: Kashflow add-ons**

Kashflow Add-ons	Description
MailChimp	Email marketing campaign management
Paypal	Card and payments processor
GoCardless	Payments processor
Unleashed	Accurate inventory management
ShipWire	Shipping management for e-commerce companies

Source: Kashflow

The range and quality of the applications that have been integrated with this data provides a strong validation of the hypothesis that the data currently held by banks would attract developers and provide fertile ground for innovation.<sup>98</sup>

Accounting providers had no doubt that they would be able to expand the range of service and capabilities provided for their SME customers if they were able to have third party access to bank data over APIs.

- 2) **Ability to offer a fully automated service to all SMEs.** For the reasons described above, direct bank feeds are increasingly central to the ability to offer a smooth, user friendly and reliable service to their clients. No other form of data access can match them. But at present access to feeds is dependent on closed bilateral relationships, and so is highly balkanised. API access across the industry would allow providers to offer a fully automated service to all their customers. For this reason, providers were confident that APIs would increase take up of their services, perhaps dramatically so. This would be particularly advantageous for new entrants, who at present need to forge bilateral commercial deals with banks to before they are able to provide any kind of automated service.
- 3) **Lower cost sign up.** Giving customers the ability to sign up for the service with OAuth authentication would also be a significant leap forward. At present, banks make SMEs and providers go through a paper based sign up process which is expensive to administer, and time consuming, taking days to complete.
- 4) **New services.** If APIs enabled 'write' as well as 'read' access then, like alternative lenders above, accounting software providers would use this to expand their product range. For example, in Australia and New Zealand, where 'write' access already exists, there are tools integrated with accounting software that allow an SME to initiate the payment and instant reconciliation of an invoice from within their accounting software.

## 4.2 Ways in which external APIs can create value for banks

Third party access has the potential to benefit banks just as much if not more than any of the

<sup>98</sup> Indeed, one provider pointed out that the ecosystem of 3<sup>rd</sup> party merchant providers that has amassed around the accounting software providers could just as easily have focused on banks, had they moved quickly enough.

other types of users described in this chapter.

There is no reason why banks couldn't build any of the third party services listed elsewhere in this chapter themselves. However, in this analysis we focus on the potential value to banks of using external APIs to integrate with others and encourage third party innovation.

#### 4.2.1 Current approach to data access

It goes without saying that banks already hold data on their existing customers. They use this for credit assessments, often in combination with external credit reference data.

Beyond this banks do not make much use of additional account data. Whilst some, particularly in the US, use scraping technologies to allow consumers to aggregate accounts held elsewhere, we were told that UK banks in general feel that customers would be sceptical of their motives for doing this.

Otherwise, Lloyds bank is the only one of the big four that has tried to use the data it holds about customers to provide them with services. "Money Manager" combines Lloyds current, savings and credit card account data, and categorises transactions into e.g. groceries, entertainment, public transport.<sup>99</sup>

#### 4.2.2 Quick wins for banks from exposing APIs

External APIs offer a number of valuable applications for a bank. Some are practical and immediate. For example:

- a) **Enhanced security.** As described above, growing numbers of consumers and businesses are using screen scraping technology to access their transaction data. 3.1.2 describes the security vulnerabilities that this risks creating as a result of the account holder handing their details to a third party. The account holder does it because they want to access the data, and this is the only way of doing it. By allowing them to use OAuth to delegate third party access, banks would be able to give consumers a safe way to do what they are already doing, and so kill this risk entirely.
- b) **Account history porting.** Banks could also act as 'third parties themselves and offer a service to customers that brings all their transaction history with them from their old bank when they switch bank account. This would stop the customer from losing all of their records, something which currently acts as an obstacle to switching.
- c) **Digital sign up and identity verification.** Much like other users described above, Banks are looking for ways to reduce the friction of signing up new customers. An API with OAuth would allow them to pre-populate much of the information that a consumer is asked for when opening a new bank account or switching bank accounts. If the API was allowed to integrate into the 7 day switching service, much of this process could be automated, further reducing friction for the consumer.

---

<sup>99</sup> Outside of the UK, US banks have been quicker to integrate with third party providers of financial management tools, which they white label for their customers. See 3.1.1.



More generally, banks are in a strong position to “verify attributes” on behalf of others<sup>100</sup>, or to become a trusted identity provider. They could sell this service.

### 4.2.3 The strategic value of banks being a platform for third party innovation

As well as immediate benefits, there may be strategic value to banks in attempting to act as a platform for third party innovation.<sup>101</sup>

a) **A varied suite of digital products.** Although all major banks now have online and mobile banking, it is perhaps fair to say that they are not at the vanguard of digital innovation. As a variety of service delivery digitises, this can no longer be dismissed as an early adopter niche. According to Ofcom<sup>102</sup>, 61% of the UK population has a smartphone, including 88% of 16-24 year olds. ONS statistics show that 76% of adults now use the internet daily, a near doubling since 2006<sup>103</sup>. Digitally native banks such as Moven and Simple in the US have made promising starts. Atom Bank<sup>104</sup> is due to launch next year in the UK.

Third party innovation is a quick and cheap way to build the kind of digital product suite that consumers increasingly expect. For example, the table below shows selected apps that have been developed for the Open Bank Project platform. The apps exist, but do not yet connect to any live bank data through the OBP platform (though they may well connect to live customers elsewhere). The sheer number, while only a selection of the 100 or so apps available, is intended to show the range of use cases that are possible. They also once again demonstrate the appetite for developers to work with this kind of data.

This variety of product offering is good not just for banks but for competition in the banking market. The lack of meaningful product differentiation currently acts as a drag on consumers’ appetites to switch. The use of third parties to add new features and functionalities to bank accounts gives consumers a new set of reasons to choose one bank over another.

---

<sup>100</sup> <https://www.ctrl-shift.co.uk/news/2014/07/18/how-personal-information-management-services-can-help-banks-meet-consumer-needs/>

<sup>101</sup> Chapter 3 outlines his concept, describing the way in which different companies use external APIs to become platforms for innovation, and how organisations such as Crédit Agricole and the Open Bank Project are applying this concept to banking.

<sup>102</sup> Ofcom, The Communications Market Report 2014 - 7 August, 2014; see <http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr14/uk/>

<sup>103</sup> According to ONS: see [http://www.ons.gov.uk/ons/dcp171778\\_373584.pdf](http://www.ons.gov.uk/ons/dcp171778_373584.pdf)

<sup>104</sup> <http://atombank.co.uk/>

**Table 10: Apps developed for the Open Bank Project**

App	Description
Paygel	A service that provides easier, faster and safer ecommerce checkout. It enables users to shop on TV, a laptop or tablet, and then links the purchase to a smartphone payment application using, for example, a QR code <sup>105</sup>
Kids View	A PFM for children. Providing kids with categorised money trail of transaction history
Selfie Bank	Secure payments using your face - without exchanging bank information, just using a selfie
Mortgage Masher	A dashboard showing you how to pay off your mortgage faster and smarter
Jamjars	Banking for the unbanked - an application that manages income allocation and budgeting for people with low incomes
Bank data aggregator	Share aggregates of transaction data with firms and friends
Spendapenny	A digital way of dropping pennies to charity
TimeBalance	See your account balance next to your MacOS clock
DonationBundle	Lets users decide how much they want to donate every month and to which causes.
Fritz	An app that lets family members approve online purchases or payments on behalf of other members, for example parents approving their children's expenses
Goal	Analyses spending habits, to help you reach your goals in life
CrowdFundMatcher	CrowdFunding comparison site with bank co-funding options
Perfect Shopper	Helps small shops send targeted personal offers to consumers, based upon their previous purchases, personal preferences, location and their latest social media posts
Money Score	Manage expenses related to other people and split bills
PayDutch	Debt overview amongst friends
AlamPay	A micro-financing service that provides online payment and POS transactions, focusing on developing countries
Denary	Allows anyone to receive money through multiple payment methods in a matter of seconds
Regulatory Detective	Identifies suspicious transactions

Source: Open Bank Project

<sup>105</sup> Paygel demonstration on Youtube: <https://www.youtube.com/watch?v=u6u8zaAUNFw>

- b) **A faster product development cycle.** Third party innovation may offer a quicker route for banks to develop new products than in-house builds. It is no secret that banks are risk averse, slow moving and often dominated by compliance and security concerns. One bank we spoke to had a new product sign off process that comprised 127 internal gateways. By comparison, an API ecosystem can result in new products being developed at rapid pace. Crédit Agricole's app store allowed them to bring products to market in just a few weeks rather than just a few years.
- c) **A strategy to mitigate the impact of unbundling.** Many commentators argue that digital technologies open up the components of retail banking to competition from outside. Banks' services are slowly being unbundled by the rise of highly specialised "fintech" companies such as Funding Circle, Wonga and Transferwise, who may turn out to be good at one thing for banks to compete against<sup>106</sup>.

History suggests that firms facing such competition cannot survive by operating in walled gardens. Early internet providers like AOL tried and failed to do this, as did early mobile application services

A third party innovation strategy allows a bank to find ways to engage with these innovators and find ways to create mutual value. If a customer is going to use Transferwise, it is better for a bank that they do so as a plug-in to the bank's own portal, rather than behind the bank's back. While this may appear to be "cannibalisation" of banks' revenues, similar scenarios have played out in numerous disrupted industries in the past. In *The Innovator's Dilemma*<sup>107</sup>, Clayton Christensen highlights IBM's "dilemma" over mainframe computers, on which earned 60% gross margins, with the advent of mini-computers, which had 45% margins. IBM's management recognised the need to reinvent itself, and so they survived. Eight of the other nine mainframe makers disappeared. IBM again reinvented itself when mini-computers (PCs) commoditised, and became a highly successful services company. Yet again, they are focussing on cloud and "big data", both of which are fundamentally changing their recent core business model.

Some banks may consider that the market will inexorably change, with unbundling caused by a combination of easier switching, better customer information (via APIs), and more open access (e.g. payments). Those that consider the gateway product status of the Personal Current Account to be under threat may be considering the "IBM-style" approach.

- d) **An opportunity to get ahead of PSD 2.** Payment Services Directive II (PSD 2) may impose similar requirements on banks as some of the recommendations on APIs considered here. The European Commission is consulting on PSD 2. As it currently reads, banks would have to allow third parties, via an interface (an API), to initiate payments from bank accounts. That access must be given on the same basis as if to account owner, i.e., if the owner can initiate a payment at zero cost, then so must a third party, obviously with appropriate consents. Telecom companies, among others, are keen to develop this ability.

This has potentially profound consequences for banks, as it may reduce their ability to use

---

<sup>106</sup> London's 'fintech' start-ups aim high - Financial Times, April 13, 2014  
<http://www.ft.com/cms/s/0/112c6932-bf37-11e3-a4af-00144feabdc0.html?siteedition=uk#axzz3BbTS0Fjf>

<sup>107</sup> *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Clayton M. Christensen, 1997

current account relationships as gateway products for the sale of other products and services. This could encourage UK banks to consider strategies for addressing these changes at an early stage. It may challenge the behaviour whereby bank account customers often, by default, buy and use other financial services such as loans, mortgages, savings, foreign exchange and even online access from their core account providers. It could facilitate easier access for customers to competitors who might have keener price points and more innovative or user-friendly functionality. It may also incentivise existing banks to develop and match these innovative features.

### 4.3 Demand for Open Data

It is often the case that the value of detailed data about an individual is significantly increased if it can be compared to data about a comparable reference population. For instance, knowing that an individual is 195cm in height and weighs 100kg may be useful in isolation for some specific purposes, but the person can only be judged as 'tall' and 'heavy' if these data points are placed on a distribution curve that shows how the individual compares to peers.

Accordingly, as well as asking potential users of data about how they would use an individual's bank account data, we also enquired about what kind of reference information would prove valuable if made available - ideally as open data. [Four] compelling use cases emerged:

#### 4.3.1 Lending: Refining risk models, lowering barriers to entry, identifying underserved segments of the market

- Both SME and individual lenders use aggregate data from sources such as Companies House and Credit Reference Agencies to understand how loan defaults spread across a population of borrowers. They make the point that good aggregate data that contextualises a potential borrower implies that only a small amount of customer specific data is needed to make a very customer-specific decision.
- As such, if additional aggregated data about current account performance, loan performance and overall defaults was published lenders would plug these into existing risk models to help refine them further.
- Lenders pointed out that the biggest impact of improved data access would be on market entry. Incumbents have all built up their own datasets over time, which provide the basis of their modelling. But new entrants do not have similar historical data that they can use to calibrate their risk models, and so market entry is difficult. As such, the publication of open data on loan performance and defaults would likely significantly reduce barriers to entry to this market.
- By comparing lending patterns with overall SME population statistics with lending patterns, alternative lenders could analyse whether different segments of the market are underserved by traditional lenders. The data that would need to be published to enable this analysis would be lending data by firm type, by sector or by region.<sup>108</sup> Alternative lenders would then be able to target underserved segments accordingly.

#### 4.3.2 Switching services: providing a 360° view on financial products

---

<sup>108</sup> Some regional data is already published by the BBA

- Providers of switching services and consumer advice that we interviewed saw open data as a way to give consumers as complete a picture as possible about the service offering provided by banks. As such, they would make use of open data about
  - 1) branch locations,
  - 2) ATM locations,
  - 3) branch opening hours,
  - 4) standardised branch ratings/customer reviews.
  - 5) standardised measures of terms and conditions including
    - a. overdraft rate, including EAR percentage, charges in £s (daily, per item etc.)
    - b. interest rates on balances, AER percentage
    - c. cashback details (yes or no, rates, applicability)
    - d. monthly fees, where applicable
    - e. account access (online only, branch only, both)

These indicators could be combined with existing open data about complaints and customer service performance.<sup>109</sup>

It is important to note that the core Midata next generation comparison services described above would greatly benefit from access to standardised measures of terms and conditions (as per bullet (5) above) in order to judge which bank account is most appropriate for an individual user.<sup>110</sup>

- Open data that provided information on which types of consumers are switching, and which accounts they are choosing would also allow recommendations to be made to customers on the basis of what their peers - 'people like you' - chose.

### 4.3.3 Money advice: Building predictive debt advice tools.

- Data analysis may be able to help identify early warning indicators of impending debt problems for individuals. This could be tested by taking a large sample of individuals who took advice for debt problems, and interrogating their bank account and credit data for the 12 or 24 months before they got into trouble. They would then need to be compared to a matched cohort who didn't fall into debt. Such analysis would require data that was sufficiently granular that it would contain personally identifiable information. As such, rather than working with an anonymised dataset, the data would probably need to be sourced from volunteers, and access

---

<sup>109</sup> See <http://www.fca.org.uk/static/documents/aggregate-complaints-data-2013-h2.xlsx>

<sup>110</sup> It should be noted that some organisations already provide this data commercially. Nevertheless, an Open Data standard would allow for more consistent and robust data.

to it controlled.<sup>111</sup> However, the results of the analysis could be published as open data, so that they could be freely used by charities and financial services providers to power predictive money advice tools.

---

<sup>111</sup> Access to the data could be modeled on the approach taken by the DfE towards access to the National Pupil Database, or by the Ministry of Justice for access their Justice Datalab.

## 5 Implementing data sharing in a way that is consistent with data protection and privacy

The processing of personal data in the UK is governed by the Data Protection Act 1998 (DPA). The Information Commissioner’s Code of Practice on Data Sharing highlights that the sharing of personal data can be achieved in compliance with the DPA provided that certain processes are in place to ensure “*that is fair, transparent and in line with the rights and expectations of the people whose information [is being shared].*”<sup>112</sup> Therefore both the spirit and the letter of the DPA are entirely compatible with the provision of third party access to bank account data, so long as data access is implemented appropriately.

This chapter uses the example of a specific use case to set out how third party access to personal data can be facilitated in a way that is sensitive to consumer privacy, and consistent with the DPA. This has been developed in consultation with the Information Commissioner’s Office (ICO).

For the avoidance of doubt, the approach described here is high level and does not guarantee compliance. Too much of the devil lies in the details of specific implementations. Rather it provides principles and guidance which, if executed appropriately and in good faith, can provide the basis of a compliant approach.

This chapter also sets out the legal parameters for sharing anonymised data with the public as open data. It is structured as follows:

<b>5.1 Use case</b>	<b>49</b>
5.1.1 How the DPA applies to the Bank in this use case	50
5.1.2 Areas in which we recommend going beyond the requirements of the DPA	51
<b>5.2 Case study - a recommended approach to implementation</b>	<b>52</b>
5.2.1 Design principles	52
<b>5.3 Open data: sharing anonymised information with the public</b>	<b>61</b>
<b>5.4 Example: Crédit Agricole Store - Applications Mobiles</b>	<b>62</b>
<b>5.5 Example: Xero Add-ons</b>	<b>64</b>

<sup>112</sup>

[http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/data\\_sharing\\_code\\_of\\_practice.ashx](http://ico.org.uk/for_organisations/data_protection/topic_guides/~media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx)

## Key messages

- 1) Third party access to consumer data is perfectly compatible with both the Data Protection Act (DPA) and the principles of privacy by design so long as it is implemented carefully.
- 2) Both the Bank and any Third Party that the User authorizes to access their data are Data Controllers, and must comply with the DPA accordingly.
- 3) If a Bank is following a User's explicit instruction to share their data with a Third Party, then the Bank has no liability for what happens once the data has been shared. However, the Bank must be sufficiently confident that the the User has consented to the Third Party accessing their data, and that the User understands which of their data the Third Party will be able to access. Other risks to banks may arise if data is shared inappropriately.
- 4) The case study in this chapter provides a high level framework that can help banks implement an approach to data sharing that is compliant with the DPA and is appropriately sensitive to consumer privacy.
- 5) The key principles are:
  - a. The user is fully informed about what is happening to their data, and consent is specific, informed, freely-given and explicit.
  - b. The user has on-going visibility and control over terms of access to their data.
  - c. Third party access to the API should be governed by a vetting process.
  - d. Security standards are "appropriate" as guided by recent technological developments and the Financial Conduct Authority.
- 6) The approach described goes beyond the DPA in two key ways. Firstly, it treats all data as sensitive personal data. OAuth allows the extra responsibilities of working with sensitive data to be met with minimal extra burden.
- 7) Secondly, it suggests that Banks should administer access to APIs by Third Parties, but that a third party should set and enforce the rules governing access on the basis of security and privacy.
- 8) Open datasets which are properly anonymised are attractive to work with as they are exempt from the provisions of the DPA and do not require the provision of informed consent.



## 5.1 Use case

This chapter is set up around the following use case:

- The User wants to apply for a mortgage with a Third Party to which they have no previous relationship.
- In order to ensure that the User meets the required lending criteria, the Third Party requests the user to share six months of account history.
- The User consents to this data sharing and authorizes the Third Party to access this data directly from their Bank over an API using OAuth
- The data fields requested by the Third Party for the specified service are as follows:

**Table 11: Data fields requested by third party mortgage provider**

Date	Transaction type	Merchant/ description	Debit/ Credit	Balance
2014-07-04	VIS	Boots	£5.00	£260.00
2014-07-03	ATM	Fitness First	-£50.00	£255.00
...	...	...	...	...

Source: ODI

**Table 12: How the use case compares to other ways in which account data could be shared**

	Description
Bank to customer	In this scenario, customer data goes directly from the bank to the customer (e.g. “Download My Data”), and the customer could subsequently choose to forward his or her data to a third party. The third party must establish relationship with the customer independent of the utility, and there is no contractual relationship between the bank and the third party.
Bank to third party	<b>Customer authorization:</b> In this scenario, customer data is transferred from the bank to a third party with the customer’s authorization (e.g. “Connect My Data”). The third party must establish a relationship with the bank and the consumer, and there is no contractual relationship between the bank and the third party. <b>Primary purpose:</b> In this scenario, customer data is transferred from the bank to a third party without the customer’s consent for a “primary purpose” (eg. to pay a bill). In this case, the third party must establish relationship with the bank. There is a contractual relationship between the bank and the third party.
Third party to third party	In this scenario, a third party, such as the payment processor Visa, may enable data sharing, for example as part of the credit card contract. The consumer could subsequently choose to forward his or her data to a third party. The third party must establish relationship with the customer independent of the bank, and there is no contractual relationship between the bank and the third party.

Source: Adapted from *Privacy by Design*<sup>113</sup>

We reviewed the scenarios on various aspects and present a summary in the following table. The preferred and recommended approach is highlighted in green.

**Table 13: How should data flow?**

Data flow	Low effort for customers	Bank contract with third party	Informed consent	Flexibility/transparency
Bank to customer				x
Bank to third party, customer authorisation	x		x	x
Bank to third party, primary purpose	x	x		
Third party to third party	x			
Bank to customer				x

Source: ODI

### 5.1.1 How the DPA applies to the Bank<sup>114</sup> in this use case

- The status of each party under the DPA is assumed to be:
  - The Bank is a Data Controller
  - The User is the Data Subject
  - The Third Party is also a Data Controller<sup>115</sup>
- The obligations on the Bank as a Data Controller in this use case are<sup>116,117</sup>:
  - to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data while it is in their possession.

<sup>113</sup> [http://www.ipc.on.ca/site\\_documents/PbDBook-From-Rhetoric-to-Reality-ch12.pdf](http://www.ipc.on.ca/site_documents/PbDBook-From-Rhetoric-to-Reality-ch12.pdf)

<sup>114</sup> We focus here on the obligations on the bank, but it should also be emphasised that Third Parties who access data are also subject to the full range of responsibilities of Data Controllers under the DPA. For guidance on the responsibilities of a Data Controller see <http://www.justice.gov.uk/downloads/information-access-rights/data-sharing/annex-g-guidance-data-controllers.pdf> and [http://ico.org.uk/for\\_organisations/guidance\\_index/~media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/data-controllers-and-data-processors-dp-guidance.pdf](http://ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Detailed_specialist_guides/data-controllers-and-data-processors-dp-guidance.pdf)

<sup>115</sup> Because the Third Party provides services that are not under the control of another party, they are a Data Controller in their own right. There is no Data Processor in this relationship.

<sup>116</sup> In addition to the responsibilities in this list, the Bank would also be obliged to respond to subject access requests by the data subject. However, we do not cover this here since it is a distinct concept from the data sharing use case described in this chapter. That said, it is worth noting that the kind of data access we describe here could provide an means for the data subject to access more of their personal data in a usable format without having to resort to a subject access request and incurring the prescribed fee

<sup>117</sup> In addition to the responsibilities in this list, the Bank would also be obliged to respond to subject access requests by the data subject. However, we do not cover this here since it is a distinct concept from the data sharing use case described in this chapter. That said, it is worth noting that the kind of data access we describe here could provide an means for the data subject to access more of their personal data in a usable format without having to resort to a subject access request and incurring the prescribed fee

- to ensure that they are sufficiently confident of the identity of the User prior to providing access to the data.
- to ensure that they are sufficiently confident that the User has consented to the Third Party accessing their data, and that the User understands which of their data the Third Party will be able to access.
- to ensure that the data is provided to the Third Party in a safe and secure manner.
- to ensure that the data shared is accurate, adequate, relevant and not excessive for the intended purpose.<sup>118</sup>
- If the Bank is acting on the explicit instruction of the User to pass their Data on to the Third Party, then, subject to the terms above being fulfilled, the Bank does not have liability for the data once it is in the hands of the Third Party.

### 5.1.2 Areas in which we recommend going beyond the requirements of the DPA

The case study we set out below goes beyond the requirements of the DPA in two key respects

- Firstly, since the Third Parties in question are all Data Controllers, the bank could in principle offer a public API that allowed the consumer to grant access to their data to whomever they wish.
  - However, given the sensitivity of the data in question we recommend that it is more appropriate for banks to operate a ‘controlled API’, in which Third Parties are vetted according to rules set by an independent body. The BSI (British Standards Institution) runs an equivalent “Kitemark” scheme for secure digital transactions for websites and apps<sup>119</sup>. As well as rules setting and enforcement, an appeals process would be an important mechanism to prevent banks from applying rules over-zealously. This is not required by the DPA, but it would constitute good practice in this case. There is more detail on how his vetting should operate in the case study below.
  - Banks would need to be clear with customers that they perform this vetting as a reasonable precaution to reduce the risks of data sharing, but that they cannot guarantee the integrity of any of the Third Parties. They would need to make it clear that Users should still make their own judgements about which Third Parties they share their data with.<sup>120</sup> And Banks should make it clear to Users that they cannot accept liability for any problems that arise once a User has requested that their data be shared with a Third Party.
  - There is an important policy question over whether to a) limit access only to vetted applications, or b) allow customers to enable anyone to access their accounts via APIs.

---

<sup>118</sup> This may create a legal obligation to vet third parties.

<sup>119</sup> BSI Group Kitemark for Secure Digital Transactions <http://www.bsigroup.com/en-GB/our-services/product-certification/industry-sector-schemes/bsi-kitemark-for-secure-digital-transactions/>

<sup>120</sup> Xero provides such a warning to Users of its Third Party addons. See Annexe B.

Open access is probably best suited to “read-only” access. This would include customers’ individual use for self-developed applications, as well as a testing of as-yet-unvetted applications. Where access to unvetted applications is permitted, consumers would need to be provided with careful warnings to proceed with cautions. Apps which are vetted could receive some form of Kitemark to help users make safe choices.

However, where "write" access, such as the ability to initiate payments, is involved, it may be appropriate to restrict access to vetted applications only.

In a scenario where access is restricted in any way, banks would need to provide suitable sand-boxed testing environments to enable the development of new applications.

- Secondly, the DPA does not include financial data in its definition of sensitive personal data. However, it is possible that sensitive personal data could be inferred from bank data (for example, payments for medical services or trade union membership could reveal health conditions or political affiliations). More generally, the misuse of financial data can lead to significant damage or distress to data subjects. Therefore, we recommend that the additional conditions of processing sensitive personal data are applied to all bank data as a matter of course. In practice, this means that the user’s consent must be explicit as well as specific, informed and freely given. There is more detail on how OAuth can be used to make sure that the required quality of consent is obtained in the use case below.

## 5.2 Case study - a recommended approach to implementation

The remainder of this chapter recommends, using a case study, how data sharing should be implemented for bank data. It is intended to be consistent with the DPA. In two key respects, outlined above, the recommended approach goes above and beyond the law.

### 5.2.1 Design principles

Data sharing should have **security** and **data protection** at its core. Therefore the system shall be set up according to four design principles.

- a) The user is fully informed about what is happening to their data, and consent is informed, specific, freely given and explicit.
- b) The user has on-going visibility and control over the terms of access to their data.
- c) Third party access to the API should be governed by a vetting process.
- d) Security standards are “appropriate” as guided by recent technological developments and the Financial Conduct Authority (FCA).

The remainder of this case study works through these principles.

#### **A. The user is fully informed about what is happening to their data, and consent is informed freely given and explicit**

- 1) The process for gaining a user’s consent to share data has a **two-tier opt-in**:

- a. First the user must opt-in to sharing their bank account data with third parties in general, using an **up-front consent form**, ideally digital, and akin to registering for online banking. This stage ensures that users are aware of the possibility, the risks and the process of providing third parties with access to their data.
- b. Second, each time they grant a specific third party with access to their data the user must opt-in again, using a **one-off consent form**. This app-specific form:
  - i. describes the specific reason for sharing the data and how it will be used
  - ii. describes the data that will be shared<sup>121</sup>
  - iii. describes related data that will not be shared
  - iv. describes who has access to the data
  - v. describes how long access will be granted for
  - vi. informs the user that they have the right to revoke access at any time
  - vii. includes a link that shows the user how to revoke access to the data
  - viii. warns the consumer that they should only share with companies they trust, and that the bank cannot accept liability for any problems that arise once the data has been shared.
  - ix. indicates whether the app has been vetted or not (in the event that regulation has allowed unvetted apps), providing a clear warning if the app has not been vetted.

At the point of sharing data, the user is asked to agree to these terms by clicking a button.<sup>122</sup>

- 2) This process should be delivered using the OAuth 2 protocol, which provides an open, secure and very widely used mechanism for enabling this degree of granular informed consent. See Chapter one for more detail on OAuth and an example of twitter's process for establishing informed consent for data sharing, using OAuth2.
- 3) For the mortgage application use case described above the informed consent process should state the following. Where OAuth is implemented in this way, the Bank can reasonably accept that the User consents to the Third Party accessing their data, and understands what data will be shared.

---

<sup>121</sup> In some cases it will be possible for this to incorporate granularity of permissions, so that if a data subject does not wish to share all of the data set they can deny access to certain data types but still proceed to use the service based on the data they are happy with. See discussion of OAuth granularity below.

<sup>122</sup> A log of which is recorded by the bank.

**Table 14: Mortgage application authorising access to bank account**

Authorise **Bank 1 Mortgages** to access your **Bank 2 Current Account** [reference no.]?

**Bank 1 Mortgages** has requested access to your Bank 2 Current Account [reference no.] data for the purpose of reviewing your **mortgage application** from the **1st July 2014**.

This application **will be able to**:

- Verify that you are the account holder
- Read your bank statements from 1st Jan 2014 to 31st Jun 2014. This includes all your transactions details (date, merchant, amount) made in that period.
- Process the data for the above purpose

This application will not be able to:

- Send or take any money to/from your account
- Access any data *before* the 1st Jan 2014
- Access any data that is not related to your account [ref. no.]
- Store the data beyond the above purpose
- Share the data with other third parties
- See any of your online banking login details

This is a **one-time** request. Without any further action, **Bank 1 Mortgages** will have no further access to your data.

You can revoke access to any application at any time from the application tab [\[link\]](#) in your Bank 2 Current Account Settings page.

All third parties and applications have gone through our vetting process. However, you should only share data with organisations you trust. We can not guarantee what happens to your data once you choose to share it. We accept no liability for any problems that arise once it has been shared. If you have any questions or concerns, please contact us here [\[link\]](#).

Be alert to phishing: We will never send you an email, text or a website link asking you to allow access to your data. [Click here to learn more about phishing.](#)

Source: ODI

**B. The user has on-going visibility and control over the terms of access to their data**

- 1) The bank should maintain a single, convenient point of access for users (e.g. on their online banking website, or through their mobile app) that allows them to review and manage access to their data.
- 2) The point of access should include a log, which records each instance that a user’s data is accessed over the API. This gives the user detailed information on
  - a. what data the app can access,
  - b. what data the app cannot access,

c. and when it last made a data request.

- 3) The user should also be able to use this point of access to revoke third party access to their data at any time. OAuth 2 allows that this can be done through the click of a button. The terms and conditions associated with access to the API should specify that third parties may only store local copies of data where it is necessary, and must undertake to delete all personal data they hold about the data subject at the point where access to the API is revoked.<sup>123</sup>
- 4) Every instance of third party access to account data should be time bound by default. The user has to **renew** the application's access rights after a predefined period of time.

### C. Third party access to the API should be governed by a vetting process.

As described above, we recommend that open access (with suitable warnings depending on vetting status) be applied to read-only (informational) APIs, while for APIs that have the ability to initiate payments, it may be appropriate to restrict access to third parties which have been successfully vetted. The vetting process creates additional costs for both banks and third parties, but we believe it to be a reasonable precaution to take when dealing with financial data. It will also provide additional guarantees that Banks and third parties are not sharing data which could be considered excessive.

- 1) The **objectives** for vetting third parties are below. The vetting process is designed to provide a balance among these priorities.
  - a. Give users trust and confidence in sharing data with third parties.
  - b. Ensure that banks provide a secure environment for the use of third party applications, that manages their liability when working with third parties.
  - c. Set out a standard that minimises the barriers to entry to the app marketplace by providing simple and consistent processes and optimises innovation.
- 2) It should be made clear to Users that the vetting process is design to help reduce risk, but that data sharing still takes place at the User's risk.<sup>124</sup> The Bank cannot accept liability for what happens to the data once it has been passed to another data controller, and User should be vigilant and only share with Third Parties they trust.

### D. Who undertakes the vetting?

- 1) Every submitted app undergoes a review process by an authority that is appointed to take responsibility for **auditing and Kitemarking** third parties and apps. The precise form of the authority is to be determined, but we recommend that rather than each bank running its own processes, **there should be a single set of standards applied across the industry.**
- 2) The advantages of using a single standard across the industry are:

---

<sup>123</sup> This could be implemented by an alert being sent to the third party to halt further processing of any personal data they already have relating to the data subject.

<sup>124</sup> Xero provides such a warning to Users of its Third Party add-ons. See Annexe B.

- a. It would reduce the cost of third parties accessing the market, by allowing them to provide their service to all bank customers after going through a single vetting process.
- b. It would mitigate the risk of exclusive relationships and balkanisation of access to data
- c. Banks would also be able to share the costs of running the vetting process.

3) Two models could be used to operate a vetting process with a single standard:

- a. The banks may adopt a system similar to the **Direct Debit Service User Number (SUN)**. In order to create direct debits, companies need a SUN. The SUN is issued by one bank to the company, who give the bank a bond to mitigate the risk that the bank takes by issuing.<sup>125</sup> All banks will accept the SUN as issued by another bank to that company, so the company does not need to get verified by every bank. A SUN is traceable to the issuing bank, so the banks have a web of trust across each other for the various SUNs in use.

The advantages of such a model to use for the issuing of credentials are

- i. There is no need for a “central authority” to issue credentials
  - ii. Credentials are not unique to particular banks
  - iii. Risk can be mitigated by the use of the bond issue if deemed necessary (perhaps, in our case, it could be reserved for ‘write’ access, such as the ability to initiate payments)
  - iv. Everything is traceable in the same way that OAuth tokens would be
  - v. Banks are familiar with the model
- b. Alternatively, a **single body** could be given responsibility for pre-vetting third party applications and granting them with API keys that allow them to interact with all banks. This could be an individual bank, a body like the BBA representing the banking sector, an independent body set up specifically, BSI (as mentioned earlier), or a regulator like the FCA.

## E. How does the vetting process work?

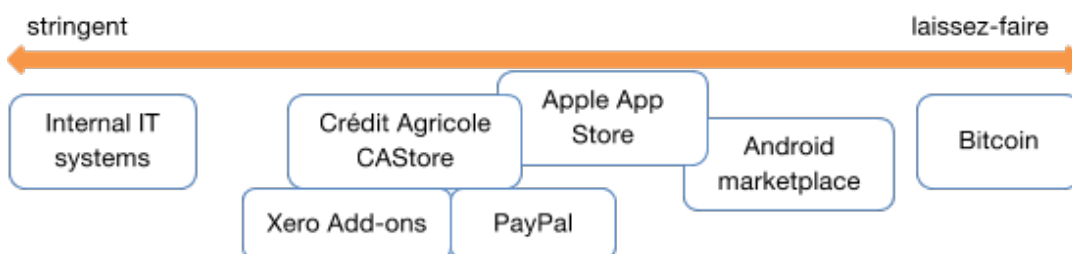
- 1) The whole vetting process may occur somewhere on the scale from very stringent requirements to a laissez-faire approach. Our recommendation is similar to the existing models by Crédit Agricole and Xero who focus on securing apps and have relatively simple processes that allow third party developers to contribute.

---

<sup>125</sup> In the case of DDs, the bond varies based on expected amount of transactions. For a read only data access, the bond may not be necessary.



Figure 3: Vetting stringency scale



Source: ODI / Fingleton Associates

Table 15: Examples of vetting process already in place in various app marketplaces

App marketplace	Example process
Crédit Agricole (French bank)	<ul style="list-style-type: none"> <li>• Direct involvement with third-party developers (mostly small enterprises) to join the venture on a co-operative basis.</li> <li>• On-going review at least every two weeks to confirm apps have no malicious code.</li> </ul>
Apple	<ul style="list-style-type: none"> <li>• Registration on developer platform with proprietary Software Developer Kit</li> <li>• 2-3 week review process for testing the app in a sandbox environment</li> <li>• Review applies for each new version of the app</li> </ul>
Xero (accounting software)	<ul style="list-style-type: none"> <li>• Internal demo</li> <li>• Pilot test with Xero customers for third party partner applications</li> <li>• Mandates sufficient end user documentation</li> </ul>
PayPal (payment solutions)	<ul style="list-style-type: none"> <li>• Registration as a PayPal Developer</li> <li>• Use of the OAuth protocol for API calls</li> <li>• Lengthy legal contracts outlining data sharing processes</li> </ul>

Source: ODI / Fingleton Associates / external sources

2) Below is a high-level recommendation of what a comprehensive audit involves. The review process *may* follow these three **dimensions**, but it is up to the institutions to align it with their current practices.

- a. **A review of the code.** For example, every app in the Apple ecosystem undergoes a review process that takes several weeks. This can happen in a sandbox environment or it can involve a few pilot testers, e.g. Xero provides a few pilot customers for testing third party partner applications. The purpose of this review is to ensure that the application does not introduce any security vulnerabilities into the system, and does not contain dubious actions such as extracting all of a user’s data.
- b. **A review of the business practices.** For example, this may include any accreditations that a business may have acquired. Other processes may be based on standard vetting practices for working with third parties. The FCA’s guidelines for managing third party IT suppliers are more stringent than is required for his use case (as they relate to suppliers who are able to access core IT systems) but are illustrative of the kinds of checks that could be applied. See below:

**Figure 4: Managing third-party suppliers**

<p>Examples of good practice:</p> <ul style="list-style-type: none"> <li>• Conducting due diligence of data security standards at third-party suppliers before contracts are agreed.</li> <li>• Regular reviews of third-party suppliers' data security systems and controls, with the frequency of review dependent on data security risks identified.</li> <li>• Ensuring third-party suppliers' vetting standards are adequate by testing the checks performed on a sample of staff with access to customer data.</li> <li>• Only allowing third-party IT suppliers access to customer databases for specific tasks on a case-by-case basis.</li> <li>• Third-party suppliers being subject to procedures for reporting data security breaches within an agreed timeframe.</li> <li>• The use of secure internet links to transfer data to third parties.</li> </ul>	<p>Examples of poor practice:</p> <ul style="list-style-type: none"> <li>• Allowing third-party suppliers to access customer data when no due diligence of data security arrangements has been performed.</li> <li>• Firms not knowing exactly which third-party staff have access to their customer data.</li> <li>• Firms not knowing how third-party suppliers' staff have been vetted.</li> <li>• Allowing third-party staff unsupervised access to areas where customer data is held when they have not been vetted to the same standards as employees.</li> <li>• Allowing IT suppliers unrestricted or unmonitored access to customer data.</li> <li>• A lack of awareness of when/how third-party suppliers can access customer data and failure to monitor such access.</li> <li>• Unencrypted customer data being sent to third parties using unregistered post.</li> </ul>
---	---

Source: FCA, April 2013. Financial crime: a guide for firms. Part 2: Financial crime thematic reviews

3) **A review of the service.** A crucial element of the service review is the question whether an app makes **proportionate** data requests given its scope, applying the principle of maximum parsimony. To do this the vetting process can apply the granularity of data access made possible by OAuth, to ensure that Third Parties only get access to the data they need to discharge the service they are offering to the User.

## Variants of data requests

Access to customer data may happen on a spectrum of less sensitive to highly sensitive data requests. The following table lists a few examples we have considered to emphasise the different requirements of granting such access. The advantage of OAuth 2 lies in its granular permission specifications, hence, it can accommodate different types of requests.

Example	Process
Query-based	Does this person have an account with the bank?
Limited history	Has the lender ever be in overdraft more than £1000?
Full access to information, no modifications	12 months worth of account data
Full access to information, and modifications	Initiate payment of a utility bill

Source: ODI

- 4) The review process is **on-going**: for example, the apps available in the marketplace are reviewed, potentially automatically, at least every two weeks to confirm they have no malicious code.<sup>126</sup>
- 5) The **API terms and conditions**, ideally consistent across banks, make it clear to third party app developers what they can and cannot do. For example, third parties cannot share account data further and only use it for the declared service.

## E. Security standards are “appropriate” as guided by recent technological developments and the Financial Conduct Authority (FCA)

- 1) Banks and Third Parties both need to ensure that data is held securely while in their possession. As mentioned above, the FCA provides thematic reviews on financial crime<sup>127</sup> which include guidance on IT security that should be adhered to.
- 2) To ensure that data is secure while being transferred from the Bank to the Third Party we recommend that APIs should only be available over HTTPS connections, and require HSTS and PFS to maximise security for client connections. We would recommend that implementers use the open source cryptographic library OpenSSL<sup>128</sup>, considered as the industry standard. There is more detail on these security standards in Chapter 5.
- 3) We also recommend that wherever possible Banks should encourage direct data transfers to Third Parties, rather than Users downloading files to a local device. User’s local devices will typically carry the highest risk of security vulnerabilities. Use of the OAuth 2 protocol for user authentication avoids the need for the user to store a copy of the data on their device

<sup>126</sup> Based on the example of Crédit Agricole’s CAStore, see Annexe A for more.

<sup>127</sup> [http://media.fshandbook.info/Handbook/FC2\\_FCA\\_20130401.pdf](http://media.fshandbook.info/Handbook/FC2_FCA_20130401.pdf)

<sup>128</sup> OpenSSL: <http://openssl.org>

unnecessarily.<sup>129</sup> Thus, the API framework is more user-friendly and in most circumstances more secure than a data download.

4) **phishing emails**<sup>130</sup> are a particular concern when dealing with financial services data. A number of precautions are recommended:

- a. Create a “*safe space*” in which users can download apps. This may be an industry-wide platform or an official appstore for each individual bank. Customers should be aware that only this place is authorised for third-party apps and any authorisation requests outside may be illegitimate and unsafe.
- b. Include information on how the third party access works on the website, for example, as part of the general guidance on security such as Lloyds online guide.<sup>131</sup>
- c. Where appropriate, repeatedly remind users how phishing works. For example, include a statement in the app authorisation process as follows: *You will only be asked to authorize access to your data at the point where you have chosen to give an application permission to do so. We will never send you an email, text or a website link asking you to allow access to your data.*

---

<sup>129</sup> See chapter 1 for details on how OAuth compares to alternative forms of authentication.

<sup>130</sup> <http://en.wikipedia.org/wiki/Phishing>

<sup>131</sup> <http://www.lloydsbank.com/help-guidance/security/phishing.asp>

### Three high level areas for considering privacy risks for third party data access

Following again the *Privacy by Design* framework, we can identify three areas for considering privacy issues when giving access to data to a third party. Privacy by Design is not currently a legal requirement but, the draft texts for the EU reform of the Data Protection legislation do point towards data protection impact assessment, privacy by design and privacy by default becoming requirements.

The first (out of seven) principle **proactive not reactive; preventative not remedial**, highlights the approach.

Information technology	Accountable business practice	Physical design and networked infrastructure
<p>‘Information technology’ encompasses the development and use of computers, devices, networks and associated applications which can be used to protect and control access to personal information. This includes access controls, audit controls, data integrity, authentication, and the security of transmission and storage of personal information.</p>	<p>‘Accountable business practices’ refer to a business’ actions, policies and procedures directed towards the collection, use and disclosure of personal information. These will be an organization’s overall privacy management processes, responsibilities and evaluation, including workforce privacy awareness and training, access policies and management, as well as contracts and agreements.</p>	<p>‘Physical design and networked infrastructure’ refers to the physical measures, policies and procedures that are aimed at protecting IT equipment and infrastructure, and securing the area they are located from unauthorized access. This includes controlling who has access to the facilities where equipment is located, as well as policies on the use of workstations, devices and other media.</p>
<p>For the bank sharing data this means, for example:</p> <ul style="list-style-type: none"> <li>• Using modern authentication protocols such as OAuth2</li> <li>• Auditing encryption practices</li> </ul>	<p>For the bank sharing data this means, for example:</p> <ul style="list-style-type: none"> <li>• Clear, comprehensive and voluntary informed consent</li> <li>• Due diligence in selecting third parties</li> <li>• Stiff terms &amp; conditions for third party use</li> </ul>	<p>For the bank sharing data this means, for example:</p> <ul style="list-style-type: none"> <li>• Extending internal IT standards to third parties</li> <li>• Following the recommendations from the FCA</li> </ul>

Source: Adapted from *Privacy by Design*<sup>132</sup>

### 5.3 Open data: sharing anonymised information with the public

**Providing anonymised bank account data as open data may help customers make better decisions and increase the transparency and stability of the financial system.**

More on the benefits of open data can be found in chapter 4.

**Anonymised data is exempt under the Data Protection Act.**

From the definition in the Data Protection Act 1998 (DPA) it follows that information or a combination of information, that does not relate to and identify an individual, is not personal

<sup>132</sup> [http://www.ipc.on.ca/site\\_documents/PbDBook-From-Rhetoric-to-Reality-ch12.pdf](http://www.ipc.on.ca/site_documents/PbDBook-From-Rhetoric-to-Reality-ch12.pdf)

data. The Recital 26 of the European Data Protection Directive (95/46/EC) also makes it clear that the principles of data protection shall not apply to data rendered anonymous when an individual is no longer identifiable.

Publishing anonymised data is *not* a disclosure of personal data. There is clear legal authority that this is the case even when the publisher holds other data that would allow an individual to be identified.

**Informed consent is not needed for creating anonymised data.**

The Information Commissioner's Office (ICO) states that "provided there is no likelihood of anonymisation causing unwarranted damage or distress – as will be the case if it is done effectively – then there will be no need to obtain consent as a means of legitimising the processing".

**Aggregation is an effective method for anonymising data.**

Aggregation, for example averages by region, is an effective method for mitigating the risk of publishing information about an individual, in just the same way as national statistics are created from the census by the Office of National Statistics. Data is shown as statistics or cross-tables. Crucial considerations for this anonymisation methods are around small numbers (low counts) and whether publishing multiple tables may be used for re-identification.

**The DPA recognises that the risk of anonymisation is never zero.**

*"The DPA is not framed in terms of the possibility of an individual being identified. Its definition of personal data is based on the identification or likely identification of an individual. This means that, although it may not be possible to determine with absolute certainty that no individual will ever be identified as a result of the disclosure of anonymised data, this does not mean that personal data has been disclosed."*

**ICO Anonymisation Code of Practice**

**The Open Government Licence can be used for anonymised data.**

The Open Government Licence does not cover the use of personal data, but anonymised data falls within the scope of the licence. Moreover, despite the difficulties of enforcing it, under the licence users and re-users are not permitted to re-identify, or enable re-identification of individuals.

## 5.4 Example: Crédit Agricole Store - Applications Mobiles

How it works for bank customers:

- 1) Choose a username and password specific to CAStore
- 2) Connect your online bank account using your account number and your pin.
- 3) Confirm and take advantage of all the applications in the catalogue!

Figure 5: Crédit Agricole app store



## Les applications

Les plus récentes | Les plus utilisées | Les mieux notées | Les plus commentées | Les applications Crédit Agricole

 <b>InfoComptes</b> Êtes-vous "dans le vert" ou "dans le rouge"? Avec InfoComptes, visualisez immédiatement la situation de votre ... Télécharger	 <b>Mon budget sant...</b> Avec Mon Budget Santé, suivez vos dépenses médicales ! Télécharger	 <b>Bankly</b> Avec Bankly, visualisez vos informations bancaires de façon claire, rapide ... et esthétique! Le design... Télécharger
---	---	---

Source: [http://www.bearingpoint.com/en-other/download/FIBA02V\\_CA\\_Store.pdf](http://www.bearingpoint.com/en-other/download/FIBA02V_CA_Store.pdf)

## 5.5 Example: Xero Add-ons

Figure 6: Xero Add-ons

The screenshot shows the Xero website's 'Add-ons' section. At the top, a blue navigation bar contains the Xero logo, the tagline 'Beautiful accounting software', and links for 'SMALL BUSINESSES', 'ACCOUNTANTS & BOOKKEEPERS', 'MORE', and 'SIGN UP'. The main heading is 'Add-ons', followed by a sub-heading: 'Manage all aspects of your business by integrating applications with Xero. CRM, inventory management, invoicing & job systems, plus a wide range of other software. Xero doesn't guarantee the service of any one Add-on, so make sure you check them out yourself.'

On the left, a navigation menu lists 'ADD-ONS' with sub-categories: 'Popular', 'Latest', 'Bills + Expenses', 'CRM', 'Debtor tracking', 'eCommerce', 'Inventory', 'Invoicing + Jobs', and 'Payments'. The main content area displays three featured add-ons:

- Receipt Bank**: Receipt Bank converts those annoying bits of paper – receipts and invoices - into Xero data! Buttons: Visit Website, Read Reviews.
- WorkflowMax**: A Xero product offering all-in-one workflow. 5000+ service businesses trust WorkflowMax for quotes, time sheets, job management, invoices and more. Buttons: Visit Website, Read Reviews.
- Fathom**: Management reporting and financial analysis tool which helps you to assess performance, monitor trends and identify improvement opportunities. Buttons: Visit Website, Read Reviews.

Source: Xero

Xero additionally relies on a community-driven review process.










Figure 7: Steps for becoming an Add-on partner with Xero.

### Become a Partner

Add-on Partner Conversion Partner Developer Partner

Xero Add-ons are the applications and services that integrate with Xero through the Xero API. We're always looking for good solutions, and are happy to offer help throughout the process of becoming a certified Xero Add-on. It's free to become a Partner.

<b>1</b>	<b>Register with us</b>	
<b>2</b>	<b>Integrate your product with Xero</b>	
<b>3</b>	<b>Demonstrate your integration to us</b>	
<b>4</b>	<b>Run a pilot test with Xero customers</b>	
<b>5</b>	<b>Have sufficient end user documentation</b>	
<b>6</b>	<b>Produce a landing page</b>	
<b>7</b>	<b>Publicise your integration</b>	

Source: Xero

## 6 Best practice technical standards for sharing bank data

This chapter will focus on the technical aspects of data access. We first identify a number of illustrative use cases, and use these to create a list of the types of data that an API should expose to third parties. We review current best practise in API design, and also review a number of existing financial data access APIs. We then make recommendations based on this review, both as to how a good financial data access API should be designed, and also how open data should be published.

The chapter is structured as follows:

<b>6.1 Use case definitions</b>	<b>69</b>
6.1.1 Account Switching	69
6.1.2 Business Loans	69
6.1.3 Budgeting Tools	69
6.1.4 Faster Payments Initiation	70
6.1.5 Direct Debit Setup	70
6.1.6 Identity Verification	70
6.1.7 Open data publication	71
<b>6.2 Technical requirements</b>	<b>71</b>
6.2.1 Private Data Access	71
6.2.2 Open Data	72
<b>6.3 Web-based API best practices</b>	<b>72</b>
6.3.1 REST	73
6.3.2 HTTPS	74
6.3.3 Formats	74
6.3.4 OAuth	74
<b>6.4 Evaluation of existing data access technologies</b>	<b>75</b>
6.4.1 OFX	75
6.4.2 FinTS	75
6.4.3 Crédit Agricole API	76
6.4.4 BBVA API	77
6.4.5 Open Bank Project API	77
6.4.6 Summary	77
<b>6.5 Recommended approach to private data access</b>	<b>78</b>
6.5.1 Application approval	78

6.5.2 Test data	78
6.5.3 OAuth scopes	79
<b>6.6 Recommended approach to open data publishing</b>	<b>79</b>
6.6.1 Licensing	80
6.6.2 Tabular Data Package	80
6.6.3 Open Data APIs	80
6.6.4 Open Data Certificates	80

### **Key messages**

- 1) Established standards like OFX and FinTS demonstrate that there are no technical barriers to providing detailed access and control to bank data. However, they lack some of the features expected from modern web APIs, such as third party delegation capability.
- 2) More modern implementations of the concept, such as Crédit Agricole and the Open Bank Project provide a good starting point for designing an API to contemporary standards.
- 3) The API should have REST architecture and use JSON or CSV encoding for requests and responses, depending on the type of data.
- 4) To ensure maximum security the API should employ HTTPS connections with HSTS and Forward Secrecy. The industry standard open source cryptographic library OpenSSL should be used.
- 5) The OAuth 2.0 protocol should be used for authentication. Authorisation should be very fine-grained so that each different type of data can be granted separately according to the specific needs of each Third Party application.

## 6.1 Use case definitions

Firstly, we will define some illustrative scenarios, known as “use cases”. These are taken from the examples mentioned in (Chapter 4). They allow us to identify the types of information and access required under different usage patterns.

### 6.1.1 Account Switching

As a comparison website operator, I want to be able to access transaction history and metadata (such as interest rates and charges) about a customer’s bank account, so that I can show them suitable alternatives that will offer them a better deal.

**Requirements:**

- Read only
- One-time access
- Single account
- Transaction history (at least 1 month, amounts only)
- Interest rates
- Service charge
- Overdraft facility

### 6.1.2 Business Loans

As a small business loan provider, I want to view transaction data from an applicant’s accounts, so that I can apply my own criteria to assess whether I want to lend to them, especially where they have been refused a loan by another provider.

**Requirements:**

- Read only
- One-time access
- All accounts
- Transaction history (at least 6 months, amounts only)

### 6.1.3 Budgeting Tools

As a personal current account holder, I want to use a third-party web-based tool to manage my budget and account balances, so that I can understand where my money goes, how I can save, and receive alerts for account activity.

**Requirements:**

- Read only
- On-going access
- All accounts
- Transaction history (at least 12 months, all data)
- Overdraft facilities

#### 6.1.4 Faster Payments Initiation

As a retailer, I want to create a Faster Payments transfer from a customer's account to mine, so that I can quickly create and verify their payment and can fulfil their purchase quickly.

**Requirements:**

- Single account
- One-time access
- Create single Faster Payments transfer
- Read transfer result

#### 6.1.5 Direct Debit Setup

As a utility provider, I want to quickly and efficiently create a direct debit from a new customer's account to mine as part of the online signup process, so that I can make the signup and switching process simpler for the customer.

**Requirements:**

- Single account
- One-time access
- Create direct debit instruction

#### 6.1.6 Identity Verification

As a consumer service provider, I want to be able to verify that a customer's name and address is correct, and that they have a bank account, so that I can ensure that they are real before I offer them my service.

**Requirements:**

- Read only
- One-time access
- Customer name
- Customer address
- Has account? Yes/No

### 6.1.7 Open data publication

As an SME lender, I want to be able to regularly obtain aggregated and anonymised data on the characteristics and performance of SME loan books.

**Requirements:**

- Read only access
- Regular releases (or real-time if possible)
- Aggregated and anonymised consumer transaction data

## 6.2 Technical requirements

From the use cases above, we can identify a set of technical requirements that the API must satisfy. This is not intended to be comprehensive, and there will certainly be extra features that could be added. Any API design should be designed for extensibility so that such features can be added easily without breaking compatibility with existing clients.

### 6.2.1 Private Data Access

There are a number of different types of data that client applications will need. We would suggest that access to each of these should be granted separately, using a fine-grained authorization mechanism (see OAuth section below). Examples are:

- Account scope:
  - Single (specified by number)
  - All
- Transactions scope:
  - No payee data (amounts and dates only)
  - All details
- Account metadata:

- Interest rates (credit & debit)
- Overdraft amount
- Service charges
- Customer data:
  - Customer name
  - Customer address
- Transfers/payments:
  - between own accounts
  - Faster Payments transfer to particular account
  - Faster Payments transfer to any account
  - create direct debit instruction
- Temporal scope:
  - One-off access
  - Time period access

## 6.2.2 Open Data

While we highlight one possible use case for open data publication above, there are very many possible uses for financial data that has been correctly anonymised and aggregated to provide general insights, and a number of reference datasets that would be useful to the stakeholders described in Chapter 4. It is therefore not possible to list all the ways in which this publication could be done; instead, different open datasets will have different technical designs and schemas. Rather than focusing on the detail of open data publication, we will simply make general recommendations on how such publication should be done.

However, while there may be many use cases within a bank for open data, those same use cases will be applicable to other banks, so banks should be encouraged to work together to define common open datasets and publication standards.

## 6.3 Web-based API best practices

Over recent years, a set of technologies has emerged that are generally used in the implementation of high-quality web-based APIs. These are considered to be current best practice in the software industry, so any modern standard should be informed by them wherever



possible.<sup>133</sup>

### 6.3.1 REST

Well-designed modern APIs make use of the REST (REpresentational State Transfer) architecture. REST APIs represent resources in the system as separate URLs, and use standard HTTP methods to perform operations on those objects. For instance, a customer would have the URL `/customers/1234`, while an account belonging to a customer would have the URL `/customers/1234/accounts/98765432`. Transactions, transfers etc., would be similarly nested. The human-readable web is an example of REST architecture in practice.

#### Domain

All API resources for a service should be grouped under a single domain; for instance `https://api.bankname.co.uk`.

#### Statelessness

An important aspect of REST design is that network transactions are *stateless*. Persistent sessions are handled with OAuth access tokens provided by the client (see below).

#### Error reporting

Errors that occur in handling a request should be reported using standard HTTP error codes, and may include data in the response body (for instance, in JSON) providing more detail.

#### Content Type

It is good practice for APIs to use a vendor-defined content type when delivering content to clients. The content type is a header that tells the client what sort of data is being sent; for instance, HTML content is sent with the content type `text/html`.

We recommend defining a custom content type, such as `application/vnd.uk-bank-account-data` (this name is only illustrative, we would suggest deciding on something shorter). Exact encoding type (see the JSON section below) is specified as an addition to the content type, e.g. `application/vnd.uk-bank-account-data+json`.

#### API versioning

APIs change over time, as new capabilities are added and old ones deprecated. There are many ways to specify which version of an API should be used, but we recommend specifying the version in the Accept header of the request made by the client. This accept header specifies which content types the client can accept. Content types should be defined for each version, with the generic content type referring to the latest version. For example, `application/vnd.uk-bank-account-data-v1-0-2+json`.

Version numbering should follow the Semantic Versioning scheme<sup>134</sup>.

---

<sup>133</sup> See “Web API Design: Crafting Interfaces that Developers Love” by Brian Mulloy for more detailed recommendations on API design: <http://info.apigee.com/Portals/62317/docs/web%20api.pdf>

<sup>134</sup> Semantic Versioning: <http://semver.org/>

### 6.3.2 HTTPS

In order to ensure security of client data, all API transactions should use secure HTTP (HTTPS). Banks are already quite used to this; they will already be using it for any online banking facility already in place.

There are two extensions to HTTPS that should also be used.

- HTTP Strict Transport Security (HSTS)<sup>135</sup> prevents third-party attacks that remove the secure aspect of the connection by telling clients that connections should *only* be made using HTTPS.
- Perfect Forward Secrecy (PFS) is a property of the cryptographic cipher used by the HTTPS connection which means that should the encryption of one network message be broken, other messages cannot be decrypted using the same keys<sup>136</sup>. Without PFS, if a server's private key is compromised, all messages sent to and from that server will be vulnerable. If PFS is used, this is not possible.

Modern best-practice APIs should only be available over HTTPS connections, and require HSTS and PFS to maximise security for client connections. We would recommend that implementors use the open source cryptographic library OpenSSL<sup>137</sup>, considered as the industry standard.

### 6.3.3 Formats

JavaScript Object Notation (JSON)<sup>138</sup> is a lightweight data interchange format, commonly used by web services and APIs. It is simple, human-readable, and highly flexible. We recommend that JSON responses should be available as a minimum for most types of requests.

Other formats could be available on request, particularly if they are recognised standards in the exchange of banking data. For example, an XML format would be requested using the content type *application/vnd.uk-bank-account-data+xml*. Bulk access to transaction data might be best delivered by CSV with the content type *application/vnd.uk-bank-account-data+csv*.

Whatever format is used, it's important that it is an open standard, developed through wide consultation with both consumers and publishers of banking data.

### 6.3.4 OAuth

As discussed in chapter 1, OAuth is an open standard for authentication and authorization between applications communicating across the web. It allows a user to delegate access to a service to a third party, without disclosing passwords or other secure credentials. It also allows simple revocation of third-party permissions, and fine-grained access control for third parties (known as *scopes*).

Many major web companies use OAuth as an authentication method; for instance Twitter, Facebook, Google and Microsoft. Most of these are now using the latest version of the standard,

---

<sup>135</sup> RFC 6797: HTTP Strict Transport Security: <https://tools.ietf.org/html/rfc6797>

<sup>136</sup> SSL Labs: Deploying Forward Secrecy: <https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy>

<sup>137</sup> OpenSSL: <http://openssl.org>

<sup>138</sup> JSON: <http://json.org/>

OAuth 2.0. Governments are also using OAuth to secure services, such as the Blue and Green Button initiatives in the US.

As OAuth (particularly version 2.0) can be hard to implement, we would recommend that API developers reuse one of the existing open source OAuth 2.0 implementations<sup>139</sup>, preferably one that is in use by a major platform such as Facebook. Such implementations will be well-tested, open to inspection for bugs, and more secure than taking an in-house development approach.

## 6.4 Evaluation of existing data access technologies

In this section we will summarise the existing data access technologies, highlight some of their capabilities, and note any drawbacks or limitations.

### 6.4.1 OFX

Open Financial Exchange (OFX)<sup>140</sup> is a standard for bank data access used widely across the USA, and supported by many software vendors. Over 5,500 banks and brokerages use OFX for data transfer. It can be considered both as a file format and an API. Many software tools such as Microsoft Money, Quicken, etc, support import and export of data in OFX file format, but also many US banks provide an OFX endpoint which software tools can connect to directly to download data.

The specification was created in 1997 by Microsoft, Intuit, and CheckFree to allow exchange of data between their software tools and their customers' banks. The specification is freely licensed, meaning that any software vendor or bank could create an interface that would conform.

The standard supports many features, including:

- Transaction data
- Transfers
- Payments
- Investments and securities
- Multi-factor authentication (added in latest specification)

Authentication in OFX is handled by the client application passing customer credentials to the server, meaning that customer logins and passwords are handled by the client code. This is only appropriate where the customer is using software they trust on a secure personal computer; it is unsuitable for use with the kind of secure third-party delegation capability that we want to achieve.

### 6.4.2 FinTS

FinTS is an online banking standard used in Germany with many similarities to OFX. It was

---

<sup>139</sup> A number of implementations are listed in the OAuth 2.0 specification: <http://oauth.net/2/>

<sup>140</sup> OFX: <http://www.ofx.net/>

originally named HBCI, the Home Banking Computer Interface, and was first defined in 1995. It is supported by over 2000 banks across Germany.<sup>141</sup> Unfortunately the latest standard is only available in German, but it supports many of the same features as OFX, but with some European variation:

- Transaction data
- Transfers
- Payment setup
- Direct debit setup
- Investments and securities
- PIN/TAN security (home card reader devices)

The latest version of the API appears to operate over an XML RPC-style connection, rather than the modern REST style that we recommend. It also appears to handle login credentials in a similar way to OFX, though it does support one-time passwords to add some extra security.

### 6.4.3 Crédit Agricole API

Crédit Agricole provide a REST-style API for their account data.<sup>142</sup> It is designed to allow CA bank customers to use numerous applications to handle their bank account information; they do this by providing their own “app store” for financial applications that support the API.<sup>143</sup>

The API has a limited feature set:

- Transaction data
- Credit cards
- Branch locations
- Transfers to accounts already set up by the customer.

It does not support creation of payments to arbitrary accounts via the API; users must set up a payment in the online banking service first.

Authentication is handled using OAuth 1.0a; this is what allows the third-party application marketplace to exist in a secure way, unlike the OFX and FinTS examples above.

Licensing of the API is unclear; it is not presented as an open standard which others could adopt.

---

<sup>141</sup> FinTS: <http://www.hbci-zka.de/english/>

<sup>142</sup> Crédit Agricole API specification: <https://www.creditagricolestore.fr/castore-data-provider/docs/V1/rest.html>

<sup>143</sup> Crédit Agricole Store: <https://www.creditagricolestore.fr/>

#### 6.4.4 BBVA API

In 2013, BBVA ran an innovation challenge and opened up anonymised account data to participants via an API. The API included purchase data for Madrid and Barcelona, demographic data of customers, and a number of time-based breakdowns of spending.<sup>144</sup> Detailed spending data was not included, and the API was not available after the end of the challenge.

The BBVA API is not relevant to our requirements for personal data access, but may show useful types of data and anonymisation levels for possible future open data releases.

#### 6.4.5 Open Bank Project API

The Open Bank Project is a startup company aiming to create an open standard for bank data access internationally. They have defined an API, and created a reference implementation of that API which they are deploying to a number of banking institutions across the world.

The API itself<sup>145</sup> is openly licensed for anyone to reuse and implement. It supports a basic feature set:

- Multiple banks per server (not necessarily one server for one bank)
- Transaction data
- Annotation of transactions
- Data “blurring” and views, which allow delegated access to subsets of data
- Experimental payment support

The API is designed in a modern way, using REST patterns, JSON, and OAuth for secure authentication. As well as the API, the project has created client libraries for many platforms, and has created a number of open source sample client applications.

The API does not include many of the technical requirements identified above, but it is continuously evolving, meaning that it is very open to extension and improvement.

#### 6.4.6 Summary

OFX and FinTS are well-established standards, with wide support in the US and German markets. However, they are not designed for the modern web, and leave much to be desired in aspects of API design, and in their security models which do not allow third-party delegation.

Credit Agricole have created a modern, well-designed API for their customers, and facilitated a marketplace around it by including OAuth security.

The Open Bank Project is an open standard built on modern API practices, with a good third-party

---

<sup>144</sup> Innova Challenge: <https://www.centrodeinnovacionbbva.com/en/innovachallenge/how-does-api-work>

<sup>145</sup> Open Bank Project API: <https://github.com/OpenBankProject/OBP-API>

security approach.

We can conclude that there are no technical barriers to providing detailed access and control to bank data, as shown by the long history of OFX and FinTS. Also, CA and OBP show us that such services can be provided using modern web standards, and that those standards enable third-party ecosystems to flourish.

## 6.5 Recommended approach to private data access

We recommend that an open API standard should be created with the input of financial institutions.

This standard should have the following features:

- REST architecture
- JSON encoding for requests and responses
- HTTPS connections with HSTS and Forward Secrecy
- OAuth 2.0 authentication
- Fine-grained authorisation using OAuth scopes (see below)

The Open Bank Project API would make a good starting point for the standard, as it already uses many of the recommended technologies, and is an open standard (although not developed through wide engagement in an open process) currently under development. It also has an existing reference implementation that developers and financial institutions can work with. Other existing standards are either closed, or reliant upon older, less secure architecture styles.

Nothing in this recommendation should be read as preventing financial institutions from providing alternative APIs for specific third parties, or from implementing other standards such as OFX and FinTS.

### 6.5.1 Application approval

In order to connect to a service, OAuth clients need a *consumer key* and *consumer secret*, credentials which are allocated by the service in question.

We would recommend that keys are not allocated by individual banks separately for each client application. This would increase the burdens of vetting both for banks and client applications. Instead, keys should be allocated either by an independent third party, or through a decentralised model in which banks do allocate keys for clients, but also accept keys issued by other banks. This is similar to the Service User Number model for direct debits. See Chapter 5 for more on the Application approval process.

### 6.5.2 Test data

API users should be able to develop and test applications without needing approval, through use

of a *sandbox* account provided by the bank, which should contain faked data for accounts and other entities. The sandbox service should respond realistically, but without making any actual financial transactions or using real data.

### 6.5.3 OAuth scopes

We recommend, at a minimum, that the following OAuth scopes be made available. Each must be specified separately to request the required data.

**Table 16: OAuth scopes**

period:single	Allow the third party to only make a single set of related calls (i.e. to make a transfer, or download a set of transactions once). Either this or period:duration <i>must</i> be specified. Servers may choose to implement this as a 1-hour or similar time window for requests.
period:duration:{ISO8601 duration}	Allow access for a particular period of time. Duration is specified in ISO8601 format; e.g. 5 days would be PT5D. Either this or period:single <i>must</i> be specified.
account:single	Access only a single specified account. The bank website should allow the customer to select which account is accessed. Either this or accounts:all <i>must</i> be specified.
account:all	Access all accounts. Either this or accounts:single <i>must</i> be specified.
transactions:anonymous	Transaction history, but no payee information
transactions:full	Full transaction history
account:metadata	Account metadata. Interest rates, service charges.
account:overdraft	Account overdraft facility information.
customer	Customer name and address
transfer:customer	Transfer money between customer accounts
transfer:external:{sort_code}:{account_number}	Transfer money to a specified external account
transfer:external:any	Transfer money to unspecified external accounts
direct_debit:create	Create direct debit instruction
direct_debit:list	List direct debit instructions

Source: ODI

## 6.6 Recommended approach to open data publishing

As mentioned above, it is not possible to define a particular schema for open data publishing, as there will be many different data releases with different formats. However, we can recommend a set of standards that will allow simple reuse of open data releases that financial institutions should conform to.

### 6.6.1 Licensing

Open data releases should be licensed under an approved, non-modified, open data license. We recommend the Creative Commons International Attribution License, which allows anyone to reuse the data, but requires data reusers to give attribution to the data publisher.<sup>146</sup>

### 6.6.2 Tabular Data Package

*Tabular Data Package* is a simple publishing format for tabular data, defined by Open Knowledge.<sup>147</sup> The standard defines the structure of a data release:

- One or more CSV files containing data
- A JSON file (datapackage.json) which describes the release, including column descriptions for each CSV file

Releasing data in TDP will make it easy for developers to reuse the data contained within, and allow integration with an increasing number of tools such as the Open Data Institute's CSVlint validation tool.<sup>148</sup>

The schemas contained in the datapackage.json file should be shared with other financial institutions so that similar data releases can be released in the same package format.

Further developments of standards for CSV publishing on the web, which are currently being undertaken at W3C<sup>149</sup>, should be monitored.

### 6.6.3 Open Data APIs

TDP is appropriate for distinct releases of data, but open data can also be made available continuously via an API. The BBVA API mentioned above is a good example of this sort of publishing, and financial institutions should be encouraged to release real-time open data via an API wherever possible.

### 6.6.4 Open Data Certificates

The Open Data Institute have created a quality standard for open data releases, known as the Open Data Certificate.<sup>150</sup> There are four levels which can be achieved, based on the answers to questions in four areas:

- **Legal** (rights, licensing, privacy)
- **Practical** (accessibility, accuracy & timeliness, quality, guarantees)
- **Technical** (formats, provenance & trustworthiness)

---

<sup>146</sup> Creative Commons Licence: <https://creativecommons.org/licenses/by/4.0/>

<sup>147</sup> Tabular Data Package: <http://dataprotocols.org/tabular-data-package/>

<sup>148</sup> CSVlint: <http://csvlint.io>

<sup>149</sup> CSV on the Web: <http://www.w3.org/2013/csvw>

<sup>150</sup> Open Data Certificates: <http://certificates.theodi.org>



- **Social** (engagement, availability of support, documentation & services)

Open data releases should aim to achieve the *Standard* level, which is for regularly published open data, with robust support that reusers can rely on.

## 7 The cost to a bank of implementing data sharing

In this chapter we attempt to give an indication of how much it would cost a bank to provide the kind of access to data that we have outlined in previous chapters. In order to help answer this question, we spoke to a range of individuals and organisations with experience of working with banks to deliver this kind of capability, including both incumbent and challenger banks.

It is important to say upfront that the estimates provided in this chapter are contingent on a range of factors that will vary considerably from case to case and from bank to bank.

The chapter is structured as follows:

<b>7.1 The importance of non-tech costs</b>	<b>84</b>
<b>7.2 Factors that make APIs more costly than manual file downloads</b>	<b>84</b>
<b>7.3 The challenges of working with legacy banking IT systems</b>	<b>85</b>
7.3.1 Accessing data without disturbing core banking systems	85
7.3.2 Drawing data together from multiple databases	85
7.3.3 Managing the increase in load volumes	86
<b>7.4 Skills and capabilities</b>	<b>86</b>
<b>7.5 Ballpark estimates on implementation costs</b>	<b>87</b>
<b>7.6 Implementation costs associated with publishing open data</b>	<b>88</b>

## Key messages

- 1) It may cost a bank more to decide what technology and standards to use, and to get the relevant legal clearances, than it does to build the tech itself. Guidance about standards and legal requirements could help reduce these costs.
- 2) Legacy IT systems are a complicating factor in implementing modern data sharing. However, experts who work with bank IT are confident that the challenges they pose can be managed.
- 3) Banks are building the skillsets for implementation and maintenance of high quality API ecosystems, although some have made more progress than others. However, a number of organisations provide ready-made API platforms which banks could deploy rather than building their own from scratch.
- 4) Non-bank experts that we spoke to said consistently that the cost of implementing data access is unlikely to surpass £1m for a bank. Banks were less confident about likely costs, but thought that the figure would be much higher.
- 5) Informed sources assert that it is possible for implementation to be completed from start to finish in less than 12 months. Longer processes may reflect the speed of banks' internal decision-making processes rather than the amount of time needed for technical implementation.
- 6) Once account and transaction data has been made available over an API, the additional cost of publishing aggregated and anonymised open data based on this source is likely to be very low. However, it could equally be created without an API also being made available by the banks.
- 7) It should be possible for banks to publish open reference data, such as PCA terms and conditions, at low cost.

## 7.1 The importance of non-tech costs

A consistent piece of feedback we received was that uncertainties about technologies, legal requirements and data security and privacy standards would have the potential to increase implementation costs considerably.

In fact, a number of interviewees agreed that for most banks, the process of choosing which technology to use, agreeing data and security standards, and getting legal sign off on the above would be significantly more difficult and expensive than the actual tech implementation itself.

At least in part, they told us, this is because banks have long and complex governance processes. This is particularly true for anything which raises uncertainty about security or regulatory compliance issues. An ex 'big-four' executive told us that in such circumstances, signing off a new product involved a process with 127 internal gateways (with board sign off being merely step 63).

These uncertainty costs apply more to APIs than to the manual file download that banks are currently delivering for March 2015. Banks pointed out that although it has taken them time to agree the details of the manual data download, the scope of this implementation remains narrow compared to the range of decisions that would need to be made to deliver API capability.

Guidance on these issues from government, regulators or other authoritative bodies therefore has the potential to make implementation of data access more straightforward and less costly. Frameworks in which banks can share the costs of vetting third party applications could also help to minimise implementation costs.

## 7.2 Factors that make APIs more costly than manual file downloads

There are additional factors that make APIs a more resource intensive method of providing data access than manual file downloads. In particular, delegated third party access rather than direct-to-consumer downloads would require banks to find ways to manage a new set of relationships.

Firstly, whilst banks already have processes in place for authenticating customers, they would need to establish and operate new processes for authenticating third parties. Our recommendation is that OAuth should be implemented for this purpose. Although it can be tricky to implement from scratch, there are libraries of existing open-source implementations that are widely used, well tested and can help reduce setup costs.<sup>151</sup>

Secondly, we also recommend that banks vet applications before giving them a key to connect to the API. This process would inevitably incur costs. In Chapter 5 we suggest an approach that allows these to be shared between banks and kept to a minimum.

Thirdly, making the most out of external APIs involves providing on-going support to the developers and third party organisations that make use of them. Good API management can involve providing samples of code, a curated support forum, a sandpit with dummy data, an up to date blog, FAQs and more.<sup>152</sup> Naturally, this all requires resource to maintain.

---

<sup>151</sup> <http://oauth.net/2/>

<sup>152</sup> See <http://apievangelist.com/>

## 7.3 The challenges of working with legacy banking IT systems

Most UK banks are dependent in large part on legacy IT systems. In many cases they are built from a number of different systems that were designed to run independently, and were then patched together as operations expanded, or banks grew by acquisition. Serious IT failures at RBS<sup>153</sup> and Lloyds<sup>154</sup> have raised questions about the stability of these IT systems, which have been identified as a risk to the sector by the FCA.<sup>155</sup>

The core IT systems were designed before many of the current uses and applications were envisaged, let alone modern data sharing techniques. This situation creates a number of specific challenges:

### 7.3.1 Accessing data without disturbing core banking systems

It is challenging to retrieve new data from the mainframes which typically constitute core banking systems. However, where data has already been made externally accessible, third party access can be built out from a more superficial level. The implementation challenge becomes correspondingly less complex. There are a number of different access points from which APIs could be developed without having to access core banking systems:

- All major UK banks now have their own mobile banking applications for retail customers. It is very likely that each of these applications accesses data from the bank's servers using a private API. These private APIs could provide a good access point for building public APIs that are designed to enable third party access<sup>156</sup>. The range of data accessible by these mobile services varies; for instance Lloyds allows you to see your full transaction history whereas FirstDirect is limited to the last 90 transactions. As such, if a consistent data standard was required, some banks would be better placed than others to meet it.
- Where banks have provided a direct feed for accounting software this could also provide API developers a platform to work from that does not require accessing core banking systems. These feeds tend to involve the transfer of a datafile once per day, rather than an API, and so are less versatile. Nevertheless, all the major banks except Lloyds currently have some kind of relationship with at least one accounting software provider (see Chapter 4).
- Bank accounts also provide data to the network of ATMs across the LINK network. The universal data standard across this network is the current balance of the account, and the six most recent transactions made. Although this is a fairly minimal dataset, this too could provide an entry point for external API access.

### 7.3.2 Drawing data together from multiple databases

If the accounts in question are held across multiple databases, this complicates the implementation of API access. Each different database will need to be connected to the API independently.

<sup>153</sup> <http://www.ft.com/cms/s/0/03b3554a-d640-11e1-b547-00144feabdc0.html#axzz3Aj4k6osF>

<sup>154</sup> <http://www.bbc.co.uk/news/business-25914013>

<sup>155</sup> <http://www.fca.org.uk/static/documents/corporate/risk-outlook-2014.pdf>

<sup>156</sup> It is important to note here that enabling third party access would not simply be a case of making these APIs public. Firstly, an OAuth layer to implement third party access would need to be introduced. Secondly, the private APIs are unlikely to be coded or documented in a way that makes them easy for third party developers to work with.

However, it is important not to overstate the impact of this variable. We were told that once access to the first database has been set up, the marginal cost of connecting additional databases to the API is of the order of 10% of the first.

Moreover, for web and mobile banking interfaces, APIs are already being brought together, involving multiple databases, further highlighting that many of the supposed challenges are already being overcome.

### 7.3.3 Managing the increase in load volumes

There was a divergence in views from experts we talked to about whether banking IT systems would be able to cope with a scenario where third party API access resulted in a significant increase in the volume of queries made.

We were told that, roughly speaking, a bank teller will conduct about five enquiries (eg balance enquiry) for every transaction. For online banking that ratio grows to 50:1, and with mobile it is more like 500:1. It is not implausible that if a user connects a large number of third party applications to their bank account, this ratio could grow further - perhaps even to 5000:1.

Some of the people we spoke to voiced concerns over whether banks' would be able to cope with another increase in enquiry volumes without changing the way that some of their systems work, or reducing the quality of their digital services - for example, by increasing the time it takes for each enquiry to return an answer.

However, the majority were more sanguine on this issue. They made the point that the amount of data sent over an API, for instance when a user logs on to a mobile banking app, is tiny - just 'bytes to kilobytes of data.' Loading an online banking website, which usually contains graphics, adverts and video, is significantly more data intensive. In this sense, if access to bank accounts over an API displaces access to online banking, the impact could actually be to decrease bandwidth loads, even as the numbers of queries rise.<sup>157</sup>

There are other ways in which the API layer can take away load from the core banking systems. For example, it is possible to "cache" data in the API system. The Open Bank Project API can store a temporary local copy of accounts and transactions in memory or disk for a user. Thus requests for (historical) transactions don't need to "hit" the internal APIs or databases once they have been gathered.

They also pointed out that uptake of third party API access was likely to be gradual, and so banks would be able to monitor load levels and then mitigate them if necessary (for example, by throttling requests to, say, one per minute).

## 7.4 Skills and capabilities

Building and maintaining an API ecosystem requires a very specific skill set. Not all APIs are created equal - some are well thought through and optimised for third party access; those which are not tend to stimulate less interest from third party developers.<sup>158</sup>

---

<sup>157</sup> APIs generally serve JSON which is much smaller than html pages.

<sup>158</sup> When a bank recently provided a group of external developers with access to some APIs for a hackathon, they were told that they were "not fit for human consumption."

This particular skillset has not been a core strength of banks. As such, we were told that most banks would probably need to invest in expanding their capabilities if they were to properly implement third party data access. That said, banks are already starting to recruit with this in mind, and some are growing their digital teams quickly.

Furthermore, as mentioned in Chapter 3, a number of organisations have built considerable expertise in designing and building bank APIs. For example, the Open Bank Project<sup>159</sup> and Standard Treasury<sup>160</sup> have already built third party API platforms for banks. Established players like Monitise<sup>161</sup> also have this capability as part of a wider set of technologies. Banks could therefore choose to implement some of these readymade solutions rather than build their own from scratch<sup>162</sup>.

## 7.5 Ballpark estimates on implementation costs

We asked a number of different organisations who have experience of working on similar products for banks how expensive and time consuming implementation of API access to data would be.

Whilst we should emphasise that this is far from a scientific approach, it is notable that their answers were consistently below £1m, and tended to cluster in the low-to-mid hundreds of thousands:

- The former CTO of a very large international bank told us that the upper bound cost, involving “a crack team and a high quality installation” would be around £1m. The lower bound would be “not a lot.”
- The Open Bank Project (see Chapter 3) gave us a detailed breakdown of how much they charge banks to implement third party access to data.
  - They told us that they charge banks around £40k to deploy a proof of concept API, and that this usually takes two or three months to complete, most of which is spent waiting for various sign offs.
  - To deploy an API, connected to live transaction systems, integrated with the bank’s authorisation system and rolled out across all customers for one account type, they would charge between £150k and £300k. For this implementation phase, they would also expect banks to allocate two internal staff to manage technology development and another two to manage compliance for up to a year (very roughly, perhaps £400k of internal staff cost).
  - Full implementation of the API could be done comfortably inside 12 months, and potentially inside 6 if the bank is able to make decisions quickly.
  - After the first year setup, OBP estimate total running costs of around £400k p.a. Around half would be external costs such as licence fees for software, and the other half internal

---

<sup>159</sup> [www.openbankproject.com](http://www.openbankproject.com)

<sup>160</sup> [standardtreasury.com/](http://standardtreasury.com/)

<sup>161</sup> [monitise.com](http://monitise.com)

<sup>162</sup> As above, technologies such as OAuth provide a number of existing opensource implementations (<http://oauth.net/2/>). It is much easier to work with one of these ‘readymades’ than it is to try and develop your own. Because some of these simple mentations are used by major platforms such as Facebook, they will also benefit from being well tested and more secure than an in-house implementation.

security, project and community management.

- The head of a digital consultancy that built the mobile banking app for a large Scandinavian bank told us that the project cost £300,000 and took 6 months from start to finish. This project was ‘very high quality work’ and included the creation of APIs that could very easily support third party access if the bank in question decided to enable it. It should be noted that this project did not involve implementing a mechanism for authenticating third party access, although we are told that this would only involve a modest increase in cost and complexity.
- The founder of a company that builds mobile banking applications for UK banks said he would be “amazed” if it cost of implementation for a bank reached £1m, and thought that the whole of the UK banking market could be transitioned to an API standard within 9 - 12 months. He also pointed out that some companies who build mobile infrastructure for banks already have this capability built into their platforms, and so in some cases it requires no more than banks ‘giving the nod’ and the platform operator flipping a switch to activate this service.
- A fast growing startup in the payments space told us that they had built a sophisticated and granular implementation of OAuth for their own product with a team of two people in slightly under two months. They could see no reason why it would take a bank much longer than this.

We also spoke to two banks about the costs involved with implementation. It was clear that it is very difficult for banks to estimate these costs accurately. As mentioned above, at least in part this is because of the uncertainty that banks currently have about which technologies to use, and how the Data Protection Act would apply in the event that third parties were able to access data over an API.

Only one bank gave us a number, and this was couched as a ‘rough guesstimate’. They told us that it would probably take ‘tens of millions of pounds’ for full implementation of third party API access, but that most of this cost would be compliance and legal rather than technical.

Although we did not speak to Crédit Agricole, their experience is also informative. As described in Chapter 1, their ‘CA Store’ is the probably most developed version of third party API access of any bank. Although we do not have figures on how much this cost, we do know that the CA Store was delivered in less than 12 months from concept to launch. The idea was first proposed in October 2011, agreed by the Board in Dec 2011 and then launched in Sept 2012.<sup>163</sup> It is also worth noting that Crédit Agricole was one of the earliest adopters of this technology, and so many elements were developed from scratch. A bank following this path today would be able to make use of pre-existing technology such as the Open Bank Project’s API.

## 7.6 Implementation costs associated with publishing open data

To publish a data set as OD, a banks would need to identify out whether the data contains any personal identifiable info and how to anonymise it if so, create a consistent data standard so that it is machine readable and host it on a publicly accessible website. The data should then be kept up to date.

It is very difficult to generalise about costs, as datasets vary in size, complexity and the need for anonymisation. For example, the staff cost per government department for providing the

---

<sup>163</sup> [bearingpoint.com/en-other/download/FIBA02V\\_CA\\_Store.pdf](https://bearingpoint.com/en-other/download/FIBA02V_CA_Store.pdf)



standard transparent releases required of them vary from £53,000 to £500,000 per annum.<sup>164</sup> A 3-year contract for developing the police.uk data portal cost £1.1million. This data involves extensive anonymisation, with data collection/processing and maintenance costing with an average of around £28,000 per month.<sup>165</sup>

Once the investment has been made to make a data source available over an API, the marginal cost of publishing aggregated and anonymised data from the same source as open data is likely to be very low. For example, preparing and publishing a single dataset such as aggregate SME loan performance data, and updating it monthly could take as little as one or two statisticians a couple of weeks to set up, and result in very small on-going maintenance costs after that.

Other types of open data, such as reference data about the locations of bank branches or PCA terms and conditions, do not bring the same levels of issues around anonymisation or complexity and change only rarely. Depending on whether this information is stored as data in the first place, these could be published simply as additional files on a bank's website, at low cost.

---

<sup>164</sup> <http://data.gov.uk/>

<sup>165</sup> <http://police.uk/>

## **8 Summary of measures that would help deliver the benefits outlined in this report**

### **Banks agree on an open API standard for third party access**

There are benefits for consumers, banks and third party customers of data to having an open standard for bank APIs that can be applied across the industry. Banks should agree to use this standard as and when they choose to implement data sharing.

### **Independent guidance provided on technology, security and data protection standards that banks can adopt to ensure data sharing meets all legal requirements**

Banks are unsure about the technology, security and data protection standards that they would need to apply to data sharing. The process of each bank acquiring this knowledge independently would be time consuming, expensive and duplicative.

### **Industry wide approach established to vet third party applications and publish a list of vetted applications as open data**

Given the sensitivity of banking data, third party applications who wish to connect to a bank's API should be subject to some form of vetting. However, it is important that this vetting process is designed in such a way that burdens for both banks and third parties are minimal. As such, a single vetting standard should be applied so that banks can share costs, and third parties need only be authorised once to access the whole market. A list of the applications that have been through the vetting process should be available as open data, so that they can be easily discovered and compared.

### **Standard information about PCA terms and conditions published by banks as open data**

Next generation switching services rely on benchmark data about the range of products on the market in order to provide customers with personalised advice. Without this kind of reference data, the impact of the core 'Midata' use case - PCA switching – may be constrained.

### **Credit data made available as open data**

New entrants to the SME lending market lack the historic data on loan performance that they need to build and calibrate a statistical model. This acts as a barrier to entry to the market. The more of this data that is available, the more that each player in the market has the opportunity to price risk more accurately, and to make better lending decisions.

Copyright © 2014 Open Data Institute and Fingleton Associates.  
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.