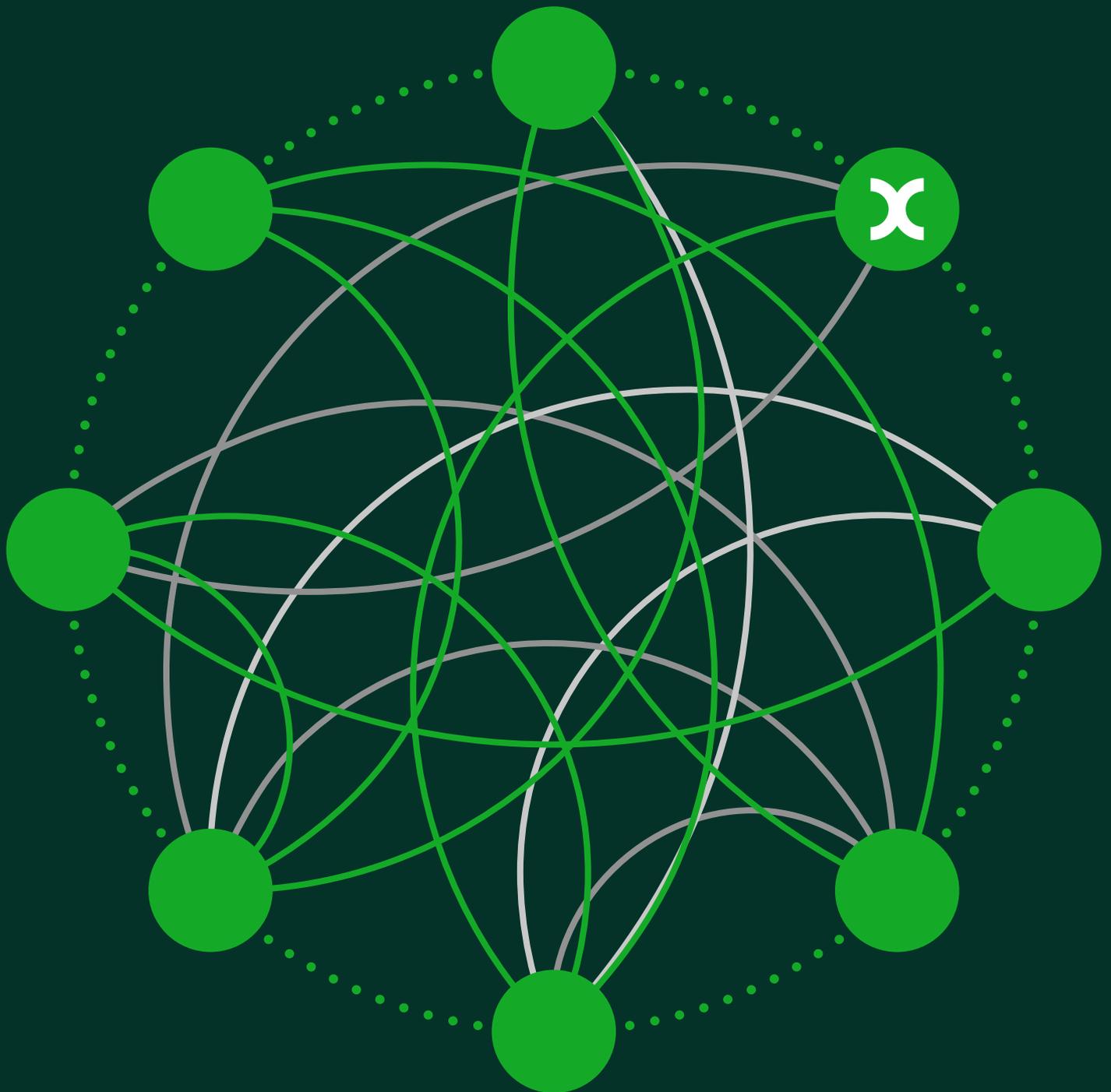


The (unmet) potential of Open Banking

Towards a system that provides incentives for all participants

4 July 2023



Contents

—

Executive Summary	1
1 Why was Open Banking introduced?	3
1.1 CMA Report	3
1.2 HM Treasury Open Banking Framework	5
1.3 PSD2	6
1.4 The structure of this report	7
2 How Open Banking currently works	8
2.1 Payments	8
2.2 Data	9
2.3 What impact has it had?	11
3 Challenges	14
3.1 Incentives for the expansion of Open Banking are not in place	15
3.2 There is an absence of alignment and coordination among ASPSPs	16
3.3 Impact of problems with existing system on liabilities	17
3.4 Internalising trade-offs	18
4 Market design of Open Banking	20
4.1 Identification of key economic characteristics of Open Banking as a product	20
4.2 Related roles for Open Banking as a product to be successful	24
4.3 Case studies	28
5 Possible models	34

Oxera Consulting LLP is a limited liability partnership registered in England no. OC392464, registered office: Park Central, 40/41 Park End Street, Oxford OX1 1JD, UK; in Belgium, no. 0651 990 151, branch office: Avenue Louise 81, 1050 Brussels, Belgium; and in Italy, REA no. RM - 1530473, branch office: Via delle Quattro Fontane 15, 00184 Rome, Italy. Oxera Consulting (France) LLP, a French branch, registered office: 60 Avenue Charles de Gaulle, CS 60016, 92573 Neuilly-sur-Seine, France and registered in Nanterre, RCS no. 844 900 407 00025. Oxera Consulting (Netherlands) LLP, a Dutch branch, registered office: Strawinskylaan 3051, 1077 ZX Amsterdam, The Netherlands and registered in Amsterdam, KvK no. 72446218. Oxera Consulting GmbH is registered in Germany, no. HRB 148781 B (Local Court of Charlottenburg), registered office: Rahel-Hirsch-Straße 10, Berlin 10557, Germany.

Although every effort has been made to ensure the accuracy of the material and the integrity of the analysis presented herein, Oxera accepts no liability for any actions taken on the basis of its contents.

No Oxera entity is either authorised or regulated by any Financial Authority or Regulation within any of the countries within which it operates or provides services. Anyone considering a specific investment should consult their own broker or other investment adviser. Oxera accepts no liability for any specific investment decision, which must be at the investor's own risk.

© Oxera 2023. All rights reserved. Except for the quotation of short passages for the purposes of criticism or review, no part may be used or reproduced without permission.

5.1	Key principles underlying possible alternative models	34
5.2	Expansion of the Open Banking mandate—coordination without incentives	35
5.3	Voluntary Premium APIs—incentives without coordination	36
5.4	The potential for a three- or five-party system	37
5.5	Conclusions	39

Executive Summary

The UK's implementation of Open Banking has been a qualified success. It is used by 7m consumers and businesses and 68m Open Banking payments were made in 2022. However, this success must be kept in perspective. The number of adults using Open Banking in the UK represents around 10% of the adult population. Payment cards and direct debits remain far more popular options for retail payments with more than 20bn card payments and 4.5bn direct debit payments in 2021. Furthermore, the adoption of account data services has lagged Open Banking payments. Open Banking use cases are limited and have not yet entered daily or weekly usage for most consumers and businesses.

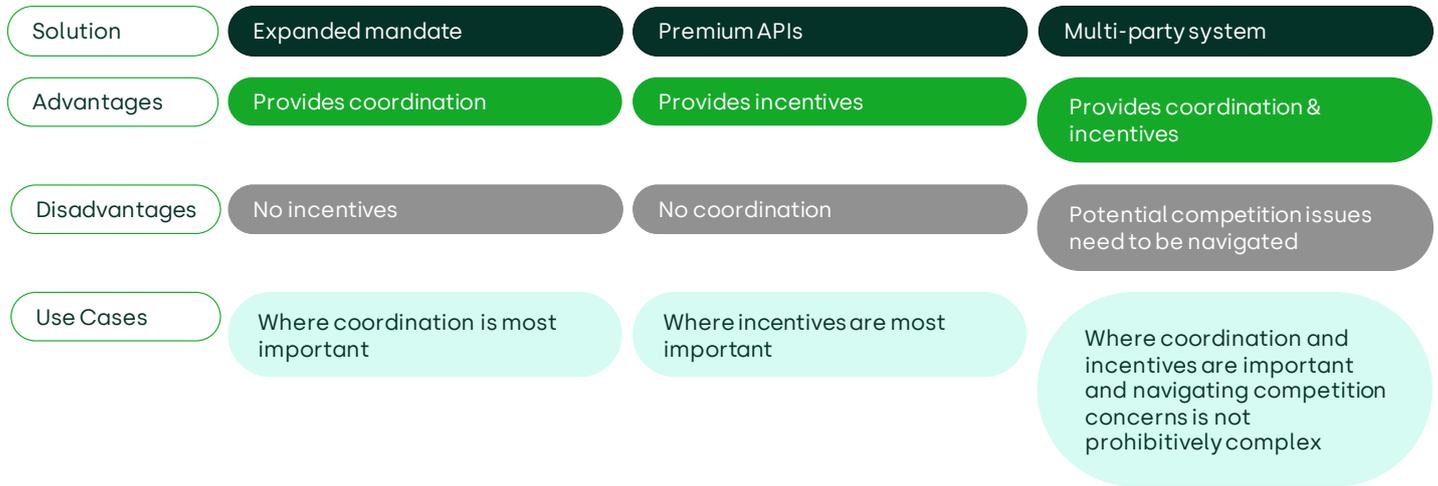
We have identified some of the key economic obstacles holding back wider adoption of Open Banking and the development of new use cases:

- A lack of commercial incentives for ASPSPs to improve the APIs they offer within the Open Banking mandate, beyond the regulatory minimum.
- A lack of coordination among ecosystem participants with respect to the development of APIs beyond the Open Banking mandate. This in turn depresses commercial incentives for ASPSPs to develop discretionary APIs.
- A suboptimal allocation of fraud liabilities towards ASPSPs and consumers. While there may be (costly) measures that TPPs could take to reduce fraud risks, they have no incentive to take them since they do not face any of the liabilities. This also means that there is currently no way to internalise trade-offs between convenience and security in the Open Banking system. For example, ASPSPs incur the costs of fraud but do not internalise the potential negative impact of fraud prevention measures on convenience for consumers and merchants at point-of-sale.

These obstacles are a direct result of some of the features of Open Banking products. First, any Open Banking use case will involve several firms in providing a single product to the consumer. This creates a need for coordination across the different parties and to trade-off their individual costs, liabilities and incentives. Second, network effects mean that some products may require universal availability—a merchant may only decide to accept (for example) a Digital ID product if such a product would be available to (nearly) all consumers irrespective of where they hold their current account.

In terms of solutions, there are broadly three possible routes forward. Different routes may be optimal for different use cases depending on which product features are most pertinent. It may even be the case that some use cases would benefit from hybrid approaches such as mandating API development but leaving banks free to decide their charging scheme individually.

Figure 1: Possible solutions for expanding Open Banking



Source: Oxera

1. Expand the mandate to additional use cases. Bring more use cases within the Open Banking mandate so that ASPSPs must provide the necessary data via APIs for free. This would provide coordination without commercial incentives. This may be the most appropriate mechanism for use cases where universal availability is the most pertinent product characteristic, but commercial incentives and dynamic innovation are less important and there are fewer trade-offs where costs and benefits fall on different parties.

2. Encourage ASPSPs to expand Open Banking use cases through Premium APIs. This provides commercial incentives, but little in the way of coordination. This may be the most appropriate option for use cases where commercial incentives and internalisation of trade-offs are most important, but universal reach is less important.

3. Enable multi-party schemes to emerge that have a commercial incentive to grow the ecosystem by finding the optimal balance between the various ecosystem stakeholders. This third option is suggested in this report and such multi-party schemes would be similar to the systems used in other European countries for the development of digital ID and credit-transfer based payment methods. Incentives and trade-off internalisation can be supported with commercial arrangements. Coordination in terms of the day-to-day management of the product can come from a commercially incentivised scheme operator. They would also be incentivised to set up appropriate rules concerning liabilities and put in place appropriate governance arrangements. Consideration would need to be given to the way in which the scheme entity was constituted and managed, to manage competition law risks.

The result of applying the correct framework to the correct Open Banking use cases should be faster roll out and adoption of Open Banking.

1 Why was Open Banking introduced?

Open Banking was launched in 2016 in the UK with the establishment of the Open Banking Implementation Entity (OBIE) by the nine largest banks in the UK (the CMA9).¹ It is funded by the CMA9, and was set up in response to an Order by the Competition and Markets Authority (CMA) in its 2016 'Retail banking market investigation' report.²

In addition to the CMA report and the Order, there were already calls from HM Treasury in 2014 to introduce Open Banking in the UK. Furthermore, the anticipated implementation of the revised Payment Services Directive (PSD2) improved the case for Open Banking to be adopted in the UK. Each of these is discussed in turn below.

The rest of this section sets out the context in which Open Banking was originally established in the UK, while section 2 briefly explains how Open Banking currently operates. Some readers may already be familiar with much of this material. However, as the debate over the future of Open Banking in the UK gathers pace, we believe it is important to be mindful of the context from which Open Banking has evolved. Therefore, all readers are likely to benefit from considering sections 1 and 2 in this light.

1.1 CMA Report

The CMA's 2016 report on the retail banking market identified several issues preventing that market from operating efficiently, including, but not limited to: barriers to accessing information; barriers to account switching; lack of customer engagement; incumbency advantages/barriers to entry and expansion for new entrants. The report concluded with a package of 17 remedies to address these issues, of which Open Banking was the foundation remedy through a CMA Order to the CMA9.³

This Order required the CMA9 to support the appointment of an Implementation Trustee, and to establish the OBIE.⁴ One of the main tasks was then to establish and adopt common Application Programming Interface (API) standards, and a trust framework.⁵

The Order also included the requirement that the CMA9 deliver the Open Banking roadmap, and make available key data through open

¹ These are the nine largest banks and building societies in the UK based on the volume of personal and business current accounts.

² Competition and Markets Authority (2021), '[Update on Open Banking](#)', (last accessed 30 March). The OBIE was established in September 2016 by the CMA9 banks in response to the draft Open Banking remedy.

³ Competition and Markets Authority (2016), '[Retail banking market investigation final report](#)', (last accessed 30 March), p. 499.

⁴ The original function of the Trustee was to seek consensus, and if no consensus could be built, to make binding decisions as to the way forward for implementing Open Banking.

⁵ The API standards included APIs with full read and write functionality and availability of personal and business account transaction data sets. A Trust Framework is a set of rules and standards which organisations agree to follow, to ensure secure data-sharing between ecosystem participants.

APIs. They are also required to maintain this open data on an ongoing basis.⁶

The CMA Order did not cover every kind of bank consumer data (see Figure 1.1 below).

The CMA intended that its remedies would increase rivalry among banks, and lower transactions costs for consumers.⁷ It was also expected that these measures would facilitate the 'emergence on a large scale of new service providers with different business models offering innovative solutions to consumers and SMEs'.⁸

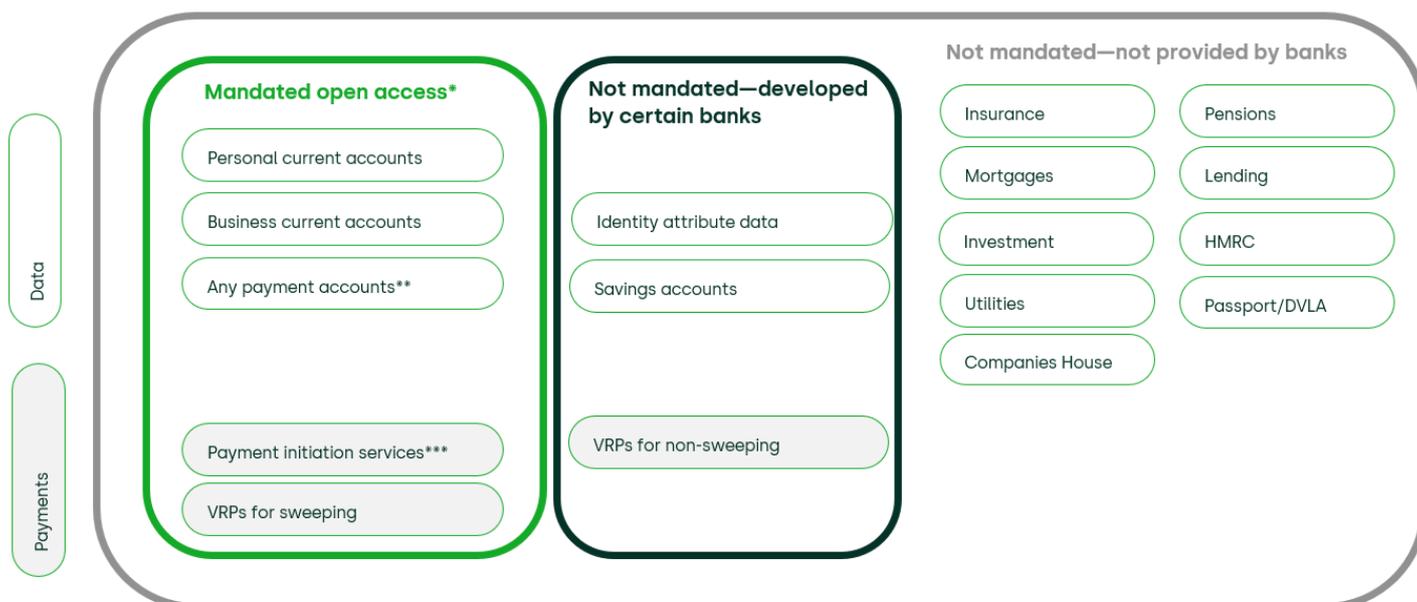
According to the CMA report, expanding the presence of FinTechs through open data access could support market developments which would lead to better outcomes for customers. This could include the unbundling of products typically sold together (e.g. overdrafts and current accounts), levelling the playing field between incumbents and new entrants through data-sharing of customer transaction data, and addressing customer inertia by helping customers take advantage of better offers more easily. In addition, using APIs to initiate payments had the potential to catalyse 'growth of a dynamic intermediary sector (including Payment Initiation Service Providers ('PISPs') and Account Information Service Providers ('AISPs'))' and facilitate the 'emergence on a large scale of new service providers with different business models offering innovative solutions to consumers and SMEs' such as price comparison services, personal finance tools, etc.

⁶ Competition and Markets Authority (2016), '[Retail banking market investigation final report](#)', (last accessed 30 March), p. 442.

⁷ Competition and Markets Authority (2016), '[Retail banking market investigation final report](#)', (last accessed 30 March), p. 442.

⁸ Competition and Markets Authority (2016), '[Retail banking market investigation final report](#)', (last accessed 30 March), p. 501.

Figure 1.1 Mandated areas of open access for the CMA9 (by CMA Order and PSD2 Requirements)



Note: *Mandated for the CMA9. For the relevant products, the CMA Order mandated access to 'open' data (information on branch and ATM locations, opening times, product prices, charges, T&Cs, features and benefits, customer eligibility criteria), 'read' data (current account transaction and account details), and 'write' data (payment initiation). ** Access to any payment account, including payment-enabled savings accounts was a PSD2 requirement, rather than due to the CMA Order.

***This includes bulk/batch payments

Sources: CMA (2017), '[The Retail Banking Market Investigation Order 2017](#)', Joint Regulatory Oversight Committee (2023) '[The future development of Open Banking in the UK](#)'.

1.2 HM Treasury Open Banking Framework

HM Treasury published a report in December 2014 which encouraged the potential for partnerships between third-party providers and Account Servicing Payment Service Providers (ASPSPs)—typically banks and building societies—noting that this arrangement could allow ASPSPs to benefit from new innovations that might otherwise have replaced existing revenue streams.

Prior to the CMA retail banking market investigation, HM Treasury published a report in December 2014 that considered how FinTech firms could use open data and APIs to improve banking services for customers.⁹ Many of the themes considered by the Treasury and the CMA were similar, such as identifying the role that access to data can play in improving the UK's retail banking market by increasing competition. But there were key differences in the focus of the Treasury report.

The Treasury report primarily focused on APIs that enabled customer sharing of their transaction data with third parties, as well as the publication of non-personal data (i.e. aggregated account data, reference data) as open data. It emphasised that demand for banking data was strong among organisations such as alternative lenders (i.e. FinTechs), accounting software firms, comparison services, etc., and that these organisations could innovate new service offerings if given access to this data.

Notably, the report made reference to the potential for banks to benefit from creating APIs of this kind as 'encouraging third party integration and becoming a "platform", and as a possible strategy to mitigate the threat of being "unbundled"'.¹⁰ In other words, it

⁹ HM Treasury, '[Data sharing and open data for banks](#)', (last accessed 30 March).

¹⁰ HM Treasury, '[Data sharing and open data for banks](#)', p. 5.

encouraged the potential for partnerships between third-party providers and Account Servicing Payment Service Providers (ASPSPs)—typically banks and building societies—noting that this arrangement could allow ASPSPs to benefit from new innovations that might otherwise have replaced existing revenue streams.

HM Treasury issued a consultation following the publication of their report to seek stakeholder views. The consultation responses echoed strong support for open data in retail banking to support increased competition and potential innovations. The responses called for the development of industry standards to mitigate against risks such as data privacy breaches.

The Open Banking Working Group, a government/industry initiative, established in 2015 by HM Treasury, subsequently published The Open Banking Standard report with the purpose of outlining 'a framework for developing and operationalising an Open Banking Standard across UK banking'.¹¹ The Framework sets out some of the key objectives of Open Banking as follows:

- to comply with the General Data Protection Regulation (GDPR);
- to get ahead of the revised Payment Service Directive (PSD2);
- to leverage the mature technology of APIs to facilitate data sharing more easily;
- to digitise UK banking and strengthen UK FinTech—in order to help both the banking and the FinTech industry grow, while encouraging competition;
- to improve the customer experience for existing products;
- to introduce new innovation, including current account comparison services, personal financial management, access to credit, affordability checks, online accounting and fraud detection.

1.3 PSD2

The European Commission published the Payment Services Directive (PSD1) in 2007, which became the Payment Services Regulations in 2009 in the UK, in order to increase competition in payments (including by non-banks) while ensuring consumer protection. This was subsequently reviewed, and a proposal for its revision (PSD2) was set out by the European Commission in July 2013, with PSD2 issued in 2015.¹² It requires ASPSPs to deliver a dedicated interface which authorised TPPs can use to access payment accounts with the customer's consent. ASPSPs must provide parity with respect to the functionality available to the customer in direct digital channels.

As HM Treasury and the CMA were publishing their respective reports referenced above in 2014 and 2016, the PSD2 was at proposal stage, and it was expected that compliance with the PSD2 once implemented (in January 2018 in the UK)¹³ would likely require many of the same structures that were already being considered to enable Open

¹¹ Open Banking Working Group (2016), '[The Open Banking Standard](#)', p. 24

¹² Open Banking Working Group (2016), '[The Open Banking Standard](#)', p. 82.

¹³ Financial Conduct Authority (2017), '[PS17/19: Implementation of the revised Payment Services Directive \(PSD2\)](#)', (last accessed 3 April). PSD2 was incorporated in the Payment Services Regulations Act in 2017. Banks then had until September 2019 to comply with its requirements.

Banking. For example, PSD2 was expected to require ASPSPs to allow third parties to initiate payments from customer accounts, subject to appropriate consent, on the same terms (i.e. same fees) as the account owners. By enabling this kind of payment initiation through APIs as part of Open Banking, the retail banking market would be able to pro-actively comply with PSD2, effectively meeting both objectives.

1.4 The structure of this report

The next section provides a brief overview of how Open Banking works in the UK today. Readers familiar with the UK's Open Banking ecosystem might be able to skip this section, but we believe it is helpful to provide this context at the start of the report. Section 3 outlines the challenges faced in attempting to expand the UK's Open Banking ecosystem to cover new use cases. Section 4 then discusses how those challenges are a result of the innate characteristics of Open Banking products. Section 5 then considers the possible models that could be used to expand the Open Banking ecosystem and which models might be most appropriate in which circumstances, which depends on which of the Open Banking product characteristics previously identified are the most pertinent in the relevant use case.

2 How Open Banking currently works

This section provides a short explanation of how the UK's Open Banking system works, for both payments and data. A detailed explanation of the UK's Open Banking system is beyond the scope of this report.¹⁴

Much has already been achieved to date in laying the groundwork, and in the development of Open Banking in the UK. However, the use cases are still limited, and volumes are relatively low (as explained in section 2.3). Further advances are required in order for Open Banking to attain its potential in terms of more widespread adoption and further use cases. While there is some scope for additional expansion, there is a risk of consumer adoption in Open Banking stalling due to the limitations of data availability and lack of additional use cases, and customer concerns around the risks.¹⁵

2.1 Payments

A standard, simplified flow in the Open Banking payments space, as illustrated below in Figure 2.1, involves account providers (i.e. ASPSPs, which include the CMA9 banks) enabling access to payment accounts (e.g. personal current accounts, business current accounts, credit cards, e-money accounts) through open, standardised APIs. As shown in Figure 1.1, this can include mandated open APIs such as payment initiation services, sweeping variable recurring payments (VRPs), as well as non-mandated APIs such as VRPs for non-sweeping purposes.¹⁶

Third Party Providers (TPPs) can then use these APIs to initiate payments on behalf of the payer, subject to receiving consent from the payer. Authorised TPPs that initiate payments are termed Payment Initiation Service Providers (PISPs).

The account provider authenticates the payer (i.e. confirms that the payer is the account holder and wants to initiate the payment), and a credit transfer payment is made from the payer's account to the payee.

There is no charge from the account provider to the PISP for the use of mandated Open APIs. Normal fees (if any) will be charged by the

¹⁴ See: <https://www.openbanking.org.uk/what-is-open-banking/>, (last accessed 5 June 2023) for a more detailed explanation of the Open Banking Ecosystem.

¹⁵ For example, these concerns may include the risks of 'consent' being easily given without understanding the consequences and worries about lack of control, privacy. However, there is evidence that UK consumers' concerns about data sharing has started to reduce. See Open Banking (2017), '[A consumer perspective](#)'; and Joint Regulatory Oversight Committee (2023), '[The Future Development of Open Banking in the UK](#)', p. 105 (both last accessed 5 June 2023).

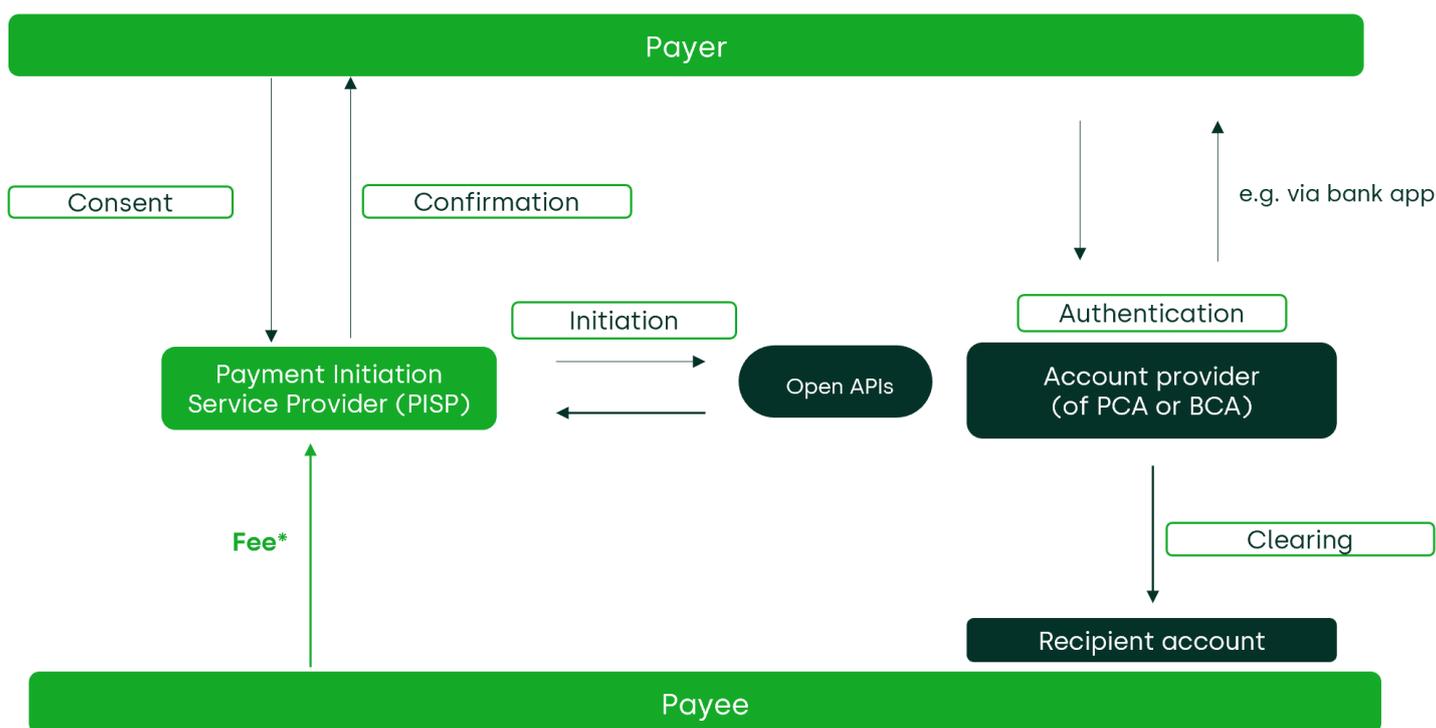
¹⁶ 'Sweeping VRP' refers to variable recurring payments between accounts controlled by the same account holder. For example, if an account holder has a savings account that yields a high interest and a current account, they might set up a sweeping VRP so that the excess funds in their current account beyond a certain level which they do not need to cover their living expenses should be regularly transferred to the savings account. A non-sweeping VRP would regularly transfer variable sums of money between accounts that are not controlled by the same person and may have use cases in terms of offering a more efficient regular payment product than e.g. Direct Debit or card on file.

account provider to the payer for sending the credit transfer.¹⁷ The recipient's account provider will also charge the normal fee (if any) to the payee for receiving the credit transfer.

The PISP may charge the payee for the service provided. This may be directly, or via a payment services provider/payment method (which in turn may charge the payee).

For non-mandated payments, the account provider may charge the PISP for the use of its APIs.

Figure 2.1 Illustrative diagram of current Open Banking flows (simplified – payments example)



Note: *Normally only applicable if the payee is a merchant.
Source: Oxera.

2.2 Data

In addition to payments as described above, Open Banking also covers data-sharing (see Figure 2.2 and Figure 2.3 below). Account providers (i.e. ASPSPs including the CMA9) enable access to account information, including transaction data for personal current accounts, business current accounts, credit cards, e-money accounts, etc., through open, standardised APIs. As shown in Figure 1.1, this can be for mandated APIs, such as data sharing for any personal or business current account or any payment account, as well as for non-mandated APIs such as customer-attribute data.

TPPs can then use these APIs to access this transaction data, subject to receiving consent from the user.¹⁸ Authorised TPPs that access account information are AISPs. In the case of mandated APIs, the data

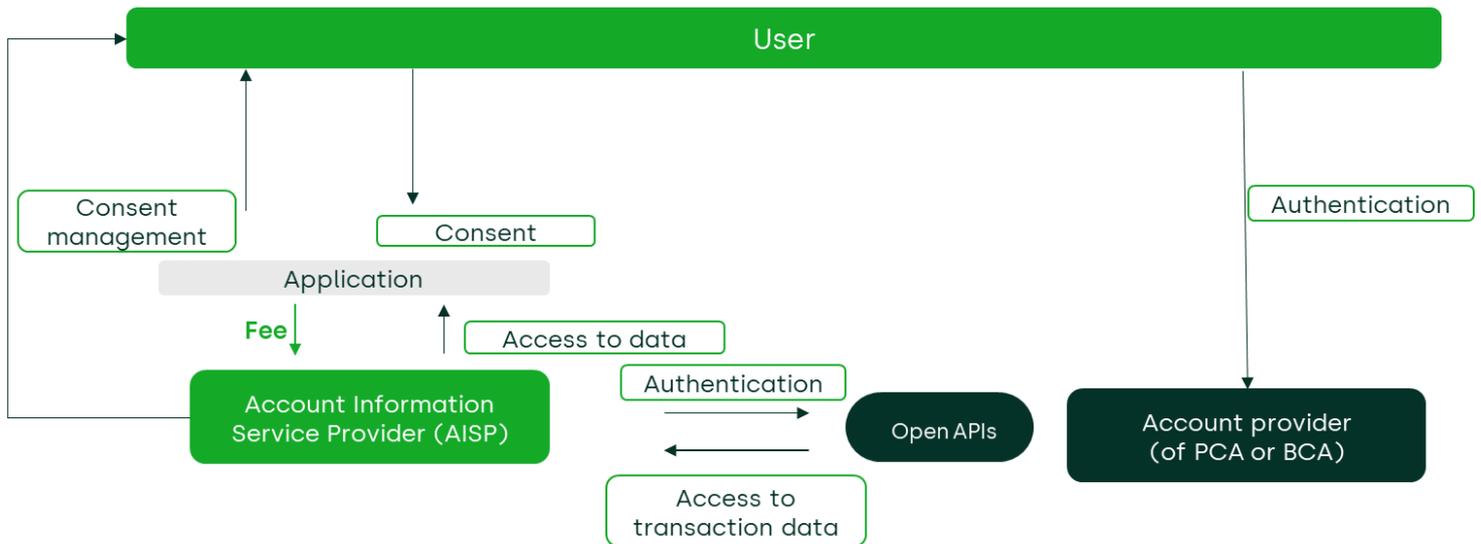
¹⁷ Fees for sending or receiving credit transfers tend to only apply to business current accounts, not personal current accounts.

¹⁸ For long-lived access, consent must be reconfirmed every 90 days.

sharing is restricted to account information from the user's account, such as balances, transactions, beneficiaries, etc., that can be viewed by a customer in the direct digital channel. This facilitates products and services such as personal finance apps that allow users to manage their finances and budget, as shown in Figure 2.2.

There is no charge from the account provider to the AISP for the use of mandated Open APIs. The AISP may then use the data to offer products and services, such as tax-filing software or automatic filling of a loan application, to the end user (including through a third party, e.g. personal finance applications) and may charge a fee for the service provided.

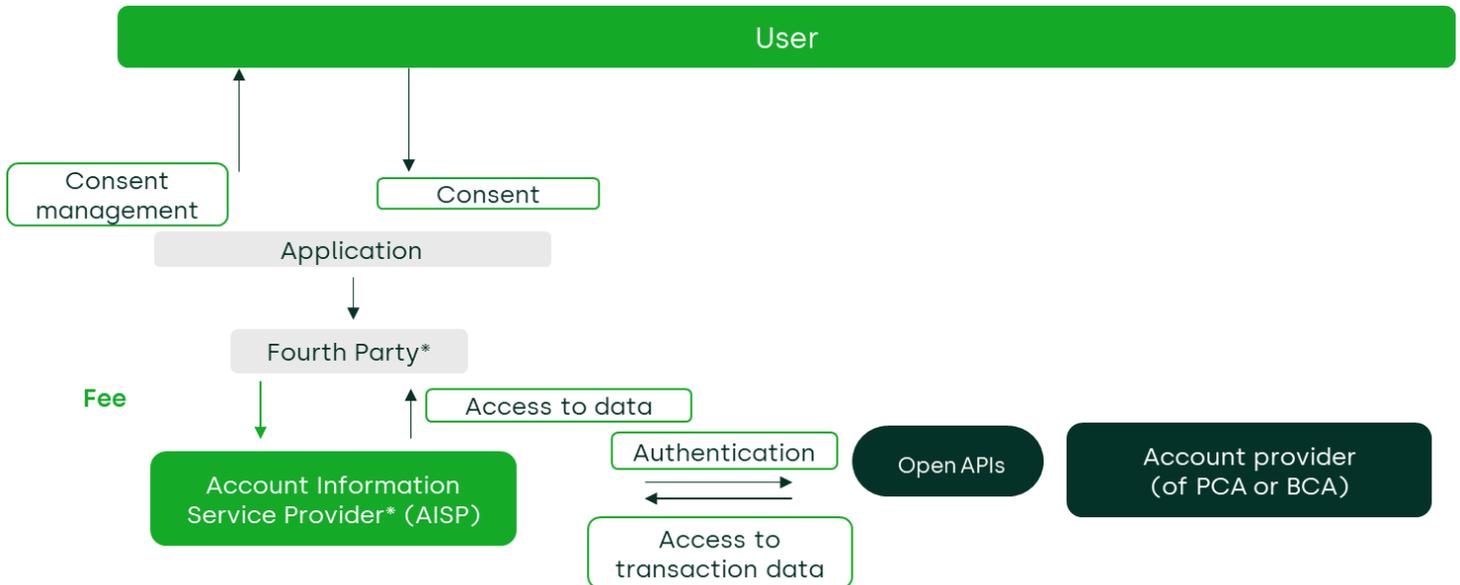
Figure 2.2 Illustrative diagram of current Open Banking flows (simplified – data example)



Source: Oxera.

Alternatively, as shown in Figure 2.3 below, in some cases the AISP may not be the application provider, but could for example be a consumer credit reporting agency. In this scenario, the AISP provides a service to a fourth party (e.g. a lender) by accessing Open Banking and may then monetise this access by charging a fee to the fourth party rather than the end user. We understand that while API standards support the provision of fourth party details in the authentication/access flow, there is no regulatory requirement mandating this on AISPs.

Figure 2.3 Illustrative diagram of current Open Banking flows (simplified—data example—fourth party)



Note: *Where the AISP is a credit reporting agency.
Source: Oxera.

2.3 What impact has it had?

There can be little doubt that the current model of Open Banking in the UK has had tangible positive impacts on various aspects of the retail banking ecosystem. Open Banking products are used by 7m consumers and SMEs in the UK to initiate payments, apply for loans, (automatically) top-up other accounts (e.g. savings, international transfers), and many other day-to-day activities. The successful implementation of Open Banking has cemented the UK as a leader in this space, and the 'UK/EU model' has been used as the basis of development and/or adoption of Open Banking in countries such as Australia and Hong Kong,¹⁹ which have expanded the model and adapted it to their unique markets.

Australia, for example, has put its Consumer Data Right (CDR) central to its approach and extended the CDR to other sectors (energy, insurance, pensions)²⁰ beyond financial services. It gives consumers control over their data sharing with third parties, which according to proponents, has the potential to enable innovation.²¹ The Australian system also allows for reciprocity in data sharing between TPPs, ASPSPs and customers to support a more flexible and dynamic Open Banking system.²² Brazil has also followed a similar path to the UK in terms of a similar regulatory approach involving mandates. However,

¹⁹ King & Wood Mallesons (2021), '[Open Banking moves forward in Hong Kong](#)', 24 November. King & Wood Mallesons (2021), '[Open Banking moves forward in Hong Kong](#)', 24 November (last accessed 17 May 2023).

²⁰ The London School of Economics and Political Science (2022), '[Open banking and Australia's data-sharing regime: six lessons for Europe](#)', 28 April (last accessed 5 June 2023).

²¹ For example, see The New Statesman (2021), '[How Australia is challenging the UK on open banking](#)', 14 April.; and Australian Banking Association, '[What is Opening Banking?](#)' (both last accessed 17 May 2023)

²² Treasury of Australian Government, '[Summary of proposals – Open Banking Designation Instrument](#)', (last accessed 17 May 2023).

they also included mandated certified performance, meaning that the parties' implementation of the technology had been tested and proven.²³ This may have helped to accelerate adoption.

To some extent, the desired outcomes of Open Banking—to increase competition and innovation, and reduce transaction costs—are being realised in the UK. Facilitated by data-sharing APIs, new non-bank entities and third-party providers have been able to enter the retail banking market, increasing the service offering from incumbents and new entrants alike. Payment APIs in Open Banking have seen higher market penetration than account information services. However, the use cases are still limited and it has not been applied in the “spontaneous payments” space as an alternative means of paying for consumer daily spending. For example, the majority of Open Banking payments involve topping up a secondary account owned by the same customer, credit card bill payments, and tax payments to HMRC. While there is some scope for additional expansion into other types of bill payments, there is a risk of consumer adoption in Open Banking payments stalling due to the limitations of data availability, lack of additional use cases and consumer concern around the potential risks.²⁴

Building on the successes of mandated APIs, some ASPSPs have begun exploring opportunities for monetising APIs and have launched a few premium APIs with additional features as test cases. The launch of these premium API test cases may lead to possible future innovations.

Over 68m Open Banking payments were made in the UK in 2022.²⁵ This sounds like a large number but to put it in the correct context, one must bear in mind that over 20bn card payments were made in 2021 in the UK and 4.5bn direct debit payments.²⁶ More generally, 6.25m consumers used Open Banking (covering both payments and data) in 2022,²⁷ this is just over 10% of the UK's adult population. To put that number in context, in 2021, 57% of UK adults used mobile banking and 65% used online banking (introduced around 15 and 25 years ago respectively).²⁸ To provide some international context, 80% of Belgians use the Belgian digital ID app, itsme that uses data provided by banks which shows that rapid adoption within Open Banking use cases is possible.

Building on the successes of mandated APIs, some ASPSPs have begun exploring opportunities for monetising APIs and have launched a few premium APIs with additional features as test cases. These 'premium APIs' are those that go beyond the mandated use cases and offer additional access and technical functionality. The bank is permitted to charge a fee to the TPP for this additional functionality, and Premium APIs therefore have the potential to enable further service improvements and provide an enhanced user experience. While take-

²³ See e.g., Fabio de Almeida Braga and Daniel Oliviera Andreoli (2021), '[How Brazil regulates Open Banking](#)', *International Bar Association* (accessed 5 June 2023).

²⁴ For more details, see footnote 15.

²⁵ Joint Regulatory Oversight Committee (2023), '[The Future Development of Open Banking in the UK](#)', *Final Report*, para. 1.2 (accessed 5 June 2023).

²⁶ UK Finance (2022) '[UK Payment Summary 2022](#)', August, and UK Finance (2021), '[UK Payments market summary, June 2021](#)' (accessed 5 June 2023).

²⁷ Joint Regulatory Oversight Committee (2023), '[The Future Development of Open Banking in the UK](#)', *Final Report*, para. 1.2 (accessed 5 June 2023).

²⁸ UK Finance (2022) '[UK Payment Summary 2022](#)', August (accessed 5 June 2023).

up in the market has been limited to date, the launch of these premium API test cases may lead to possible future innovations.

This is not a unique proposition within the UK – in fact, the European Payments Council (EPC) is due to publish a rulebook that covers the rules that are needed to create an ecosystem for the Single Euro Payments Area (SEPA) Payment Account Access Scheme (SPAA). This scheme is effectively the EPC's version of Open Banking payments supported by premium APIs.²⁹ The SPAA rule book at this stage is completely optional, but will establish minimum API requirements that all participants will need to support to ensure interoperability and fees that will be permitted for ASPSPs to charge TPPs for the use of premium APIs in order to 'unlock potential benefits for their respective customers'³⁰.

²⁹ European Payments Council (2022), '[The SEPA Payment Account Access \(SPAA\) Scheme Rulebook](#)', (last accessed 25 May).

³⁰ European Payments Council (2022), '[SPAA Scheme Status Update 17 June 2022](#)', last accessed 26 May. European Payments Council (2022), '[SPAA Scheme Status Update 17 June 2022](#)', (last accessed 26 May).

3 Challenges

This section explores the challenges limiting the further development of the Open Banking system in the UK, which are underpinned by the innate economic characteristics of Open Banking that we will introduce in section 4. In short, the challenges are related to incentives, coordination, liabilities and trade-offs within the Open Banking system. In section 5, we propose alternative structures that would address these challenges and help the system advance to the next phase of Open Banking.

Open Banking has been a qualified success to date. Products have been developed and are being used by SMEs and consumers. However, market penetration remains low as a proportion of the population. The current model has limitations which threaten to curb the potential if it were to be expanded beyond the perimeter of the Open Banking mandate. The Joint Regulatory Oversight Committee's (JROC's) April 2023 report entitled 'The Future Development of Open Banking in the UK' identified several broad-ranging challenges for the next phase of Open Banking, as described in Box 3.1 below. These include:

- establishing priorities amongst parties;
- ensuring ecosystem reliability, managing fraud risk;
- addressing consumer protection.



Box 3.1 The JROC report on the future development of Open Banking

Specifically, the JROC report established three priorities:

- to establish a sustainable and competitive footing for the ongoing development of the Open Banking ecosystem so that it can grow beyond the current functionalities and bring further benefits to end users;
- to unlock the potential for open banking payments;
- to adopt a model that is scalable for future data-sharing propositions.

To deliver this vision and the three priorities identified, the JROC report sets out a roadmap of 29 actions spanning six core themes:

- levelling up availability and performance;
- mitigating the risks of financial crime;
- ensuring effective consumer protection if something goes wrong;
- improving information flows to TPPs and end users;
- promoting additional services using non-sweeping VRP as a pilot;
- finalising the design of the future entity.

The success of these objectives will be measured by three broad categories of key performance indicators, including competition, growth and consistency.

- **Competition:** success will be measured in terms of greater innovation, lower prices or costs and improved quality of services.
- **Growth:** success will be measured by the number of products and services offered, the increased use of and reliance on open banking by consumers and businesses, any significant increase in the total number of active users, the overall growth in investment in Open Banking, and the development, functioning and take-up of a commercial framework.
- **Consistency,** success will be measured by a low number of incidents and issues, the way in which those are resolved, and the scale of any resulting consumer loss.

Source: Joint Regulatory Oversight Committee (2023) 'The future development of Open Banking in the UK'.

Our analysis shows that the issues highlighted by JROC are symptoms of four underlying economic challenges (the focus of this section) that result from the economic characteristics of Open Banking as a product, which is the focus of section 4. Section 4 also identifies the roles that must be filled in order to ensure that the Open Banking ecosystem can add value to banking services for consumers and SMEs. This discussion reveals how the properties of Open Banking products, and the (presently) unfilled roles have created the challenges outlined in this section. Further discussions on what market design might resolve these challenges are found in section 5.

There are several underlying economic challenges faced by the Open Banking ecosystem.

- **Incentives** for the expansion of Open Banking are not in place. The limited ability to commercialise API offerings has limited the viability of innovation for ASPSPs
- **Coordination,** between ASPSPs themselves, and between all parties, must be improved to create a commercially viable market for better designed APIs.
- **Liabilities** fall disproportionately on ASPSPs and their customers. This results in costs for ASPSPs and their customers. Attempts to avoid these costs (for example by putting in place appropriate security features in case of fraudulent transactions) may then come at the expense of convenience and usability of the products that Open Banking would deliver.
- **Trade-offs** between security and ease of use under the current model are not internalised by any one party, potentially resulting in a sub-optimal design of products.

The remainder of this section discusses each of these points in turn.

3.1 Incentives for the expansion of Open Banking are not in place

The lack of incentives is driven by a lack of remuneration, the absence of alignment among ASPSPs on perceived benefits of APIs, and the

Without any form of compensation from TPPs to ASPSPs, ASPSPs are unlikely to be able to justify the further investment required to design better APIs for the services within the Open Banking mandate.

absence of coordination between ASPSPs. Without resolving these issues, the potential for expanding or improving Open Banking is likely to be more limited.

Designing APIs to meet mandated requirements can be a resource intensive exercise. UK Finance estimates that the cost incurred from 2016 up to 2019 was £1.5bn to establish the infrastructure.³¹ Without any form of compensation from TPPs to ASPSPs, ASPSPs are unlikely to be able to justify the further investment required to design better APIs for the services within the Open Banking mandate.

3.2 There is an absence of alignment and coordination among ASPSPs

In an Open Banking ecosystem, there may be limited incentive for any one ASPSP to provide premium APIs to cover additional use cases, unless all or most other ASPSPs also provide similar premium APIs to cover the same use case. This need arises because the merchant side of the market may only be interested in an Open Banking product if it has universal availability (see Section 4.1.5). This may be unlikely if there is a lack of alignment between ASPSPs on whether developing premium APIs that can be monetised will be a net positive.

For example, some ASPSPs may not see the investment case in the adoption of non-sweeping VRPs, one potential premium API, given that it may become a threat to existing payment methods where arrangements are in place to ensure revenues are generated to cover costs and investments. Other ASPSPs may take a different view, and reason that, in a dynamic environment, the opportunity to diversify revenue streams provides a sufficient return on the investment.

There may be similar issues in terms of data and a Digital ID product. The technology elements to share data from bank accounts already exist and are well proven. It would be relatively simple to add some customer characteristics or ID and enable access to this data on the same terms as any other AISP API call. However, in order to do so there would need to be coordination among ASPSPs in order to ensure that such a system could work irrespective of where the consumer banked. The obstacles seem to be in terms of coordination rather than technological.

Even if this lack of alignment between ASPSPs on the perceived benefits of better APIs was resolved, there are other issues around the absence of (i) coordination between the ASPSPs and (ii) collaboration between ASPSPs and TPPs on technical and business issues. All parties are involved in the provision of Open Banking products, and so they all need to interoperate seamlessly to provide one consumer experience.

³¹ UK Finance, '[UK Finance proposes next steps for Open Banking](#)', (last accessed 17 May 2023). Note that based on the estimate of 7m Open Banking users, this would amount to a cost of approximately £214 per Open Banking user. We also note that the CMA, at the time of the Market Investigation estimated that the cost of support to the OBIE in terms of staff time and procured assistance from professional service firms would not exceed £20m (see Competition and Markets Authority (2016), '[Retail banking market investigation final report](#)', (last accessed 30 March), p. 461.). The CMA ex ante estimate and the UK Finance ex post estimate may not be directly comparable however, as the latter may include costs that would have been incurred anyway in order to comply with PSD2.

Among other things, this means they must be aligned on issues such as liabilities and dispute resolutions.

3.3 Impact of problems with existing system on liabilities

There are different types of risk associated with a payment for a product or service, some of which relate to the payment itself (payments risk) while others relate to the delivery or the condition of the product or service (purchase risk). For example, payments risk refers to the risks associated with the money transfer itself due to human error (e.g. entering the incorrect account number), scams (e.g. fraudsters tricking someone into sending a payment to a bank account controlled by the fraudster) and other fraudulent activities. Purchase risks relate to the risk of not receiving the product or service when purchasing something online; and there are risks in relation to the product itself: receiving a faulty or damaged product, or the service not being in line with how it was described when purchased.

ASPSPs and/or customers face most of the liability of fraudulent transactions, and so are incentivised to put in place security features in order to limit their liability.³² Provided the resulting APIs still satisfy minimum standards, ASPSPs may not be concerned if these security features lead to a 'clunkier' experience for TPPs and their customers. TPPs, that are not liable for fraudulent transactions become frustrated by any additional friction.

While there is some consensus that consumers need to be protected against fraudulent activities in relation to the transfer of money, there are different views on whether a more extended version of consumer protection – in terms of protection against purchase risk and/or payment risk as discussed above – should be offered.³³ For example, while the JROC report found that most ASPSPs (and consumer champions) view purchase protection as an important consideration, a few ASPSPs, retailers and most TPPs believe that purchase protection was not required. This difference in view again highlights the lack of alignment between parties in the ecosystem.

It is worth noting that this difference in opinions is also due to different levels of risk being associated with different use cases—some use cases are higher risk compared to others, and therefore potentially warrant more buyer protection. This will mean a single approach to buyer protection in the Open Banking system would likely be ineffective due to the broad uses of Open Banking payments.

We note that there have been some proposals to delineate responsibility for fraud and other customer-protection issues. For example, proposals from TrueLayer (a TPP) would assign liability for misuse of VRPs by a merchant the TPP had onboarded to the TPP. Liability for unauthorised payments or scams would remain with the

³² This is especially pertinent given that regulatory requirements are based on direct digital channels which are subject to an increasing level of Authorised Push Payment (APP) scams (An APP scam is where an account holder is tricked into paying someone posing as a genuine payee). See UK Finance (2022), '[Half Year Fraud Update 2022](#)', (last accessed 24 April).

³³ Joint Regulatory Oversight Committee (2023), '[The Future Development of Open Banking in the UK](#)', Final Report , p. 64.

customer's bank.³⁴ This may still fail to internalise trade-offs as TPPs may be a gateway to some kinds of unauthorised payment fraud. These proposals would not seek to replicate the chargeback mechanisms of card schemes, but rather rely on merchants offering refunds.

Until these liability issues are resolved, the dynamics of the current Open Banking model, as described above, means that ASPSPs will be incentivised to minimise their liabilities and prioritise security over user experience, while FinTechs will find the API offering by ASPSPs to be insufficient as they ignore the potential liabilities of the ASPSPs involved. Economic efficiency would suggest that parties should take on the liabilities over which they have the most control: this may assign some of the liability for payment frauds to TPPs rather than ASPSPs. Risk-sharing between all parties could mean that TPPs and ASPSPs have more opportunities to profit from Open Banking, while merchants could benefit from lower costs.

3.4 Internalising trade-offs

An overarching theme of the issues examined in this section is that the design of any system involves trade-offs. In this case there are trade-offs between the desire for innovation by TPPs and the costs incurred for enabling innovation by ASPSPs (section 3.1); and between security and ease of use (section 3.3). These trade-offs could be made optimally if the costs and benefits were to be internalised. Financial payments offer a means of (at least partially) internalising such costs and benefits, and so getting closer to an optimal trade-off.

To illustrate the issues of trade-offs more fully, consider APIs. Like most IT systems, APIs involve trade-offs between, on the one hand, ensuring data security, fraud protection, and customer protection, and on the other hand, delivering a user-friendly and intuitive front-end. In the current Open Banking model, the different sides of that trade-off are experienced by different parties, and there is currently no way to internalise the trade-off.³⁵

Information sharing from TPPs to ASPSPs might go some way to ameliorating this issue. While the OBIE has conducted extensive work in relation to developing and implementing transaction risk indicators (TRIs), PISPs are only recommended, but not mandated, to implement TRIs.³⁶ Without the adequate assessment of transaction risks, ASPSPs have little visibility over the risks that they take on by executing PISP-initiated transactions. Therefore, to achieve JROC's objective of mitigating fraud risks and supporting higher-value transactions, the PISPs also need to be incentivised (or even mandated) to improve their information sharing with the ASPSPs.

There are trade-offs between the desire for innovation by TPPs and the costs incurred for enabling innovation by ASPSPs and between security and ease of use. These trade-offs could be made optimally if the costs and benefits were to be internalised.

Financial payments offer a means of (at least partially) internalising such costs and benefits, and so getting closer to an optimal trade-off.

³⁴ TrueLayer (2023), '[Beyond Sweeping: A blueprint for commercial VRP](#)'.

³⁵ There are some proposals the PSR is considering such as 'requiring PSPs to reimburse victims of APP scams' through a 50:50 reimbursement cost split between the receiving and sending PSPs. However, this would be limited to APP scams, and it does not include TPPs, which therefore arguably does not address the incentive alignment problem on liabilities between ASPSPs and TPPs. See Payment Systems Regulator (2023), '[APP Scams: Measure 1](#)', March, (last accessed 24 April).

³⁶ Joint Regulatory Oversight Committee (2023), '[The Future Development of Open Banking in the UK](#)', *Final Report*, para. 4.24.

A means of sharing the costs of fraudulent transactions or execution issues between these parties would result in a system where the downside of any risks to ASPSPs of better designed APIs from a security perspective would be mitigated. Furthermore, TPPs would appreciate that the security features of APIs they might find create friction would also protect them from the costs of fraudulent activity and may even help to deliver better front-end services that limit the risk of execution issues. This could result in the removal of a barrier currently preventing ASPSPs from improving APIs.

However, under the current model there is no one party that is internalising the key trade-offs. This point should be borne in mind when considering the expansion of Open Banking beyond ensuring free provision of the basic set of APIs into other areas, and how best this might be achieved.

4 Market design of Open Banking

To understand how the design of Open Banking can be expanded and potentially improved, it is important to identify its innate economic characteristics as a product. That is the focus of this section. We identify both the innate economic characteristics of Open Banking as a product and the roles that must be fulfilled in an Open Banking ecosystem to be able to successfully deliver products, given these innate economic characteristics.

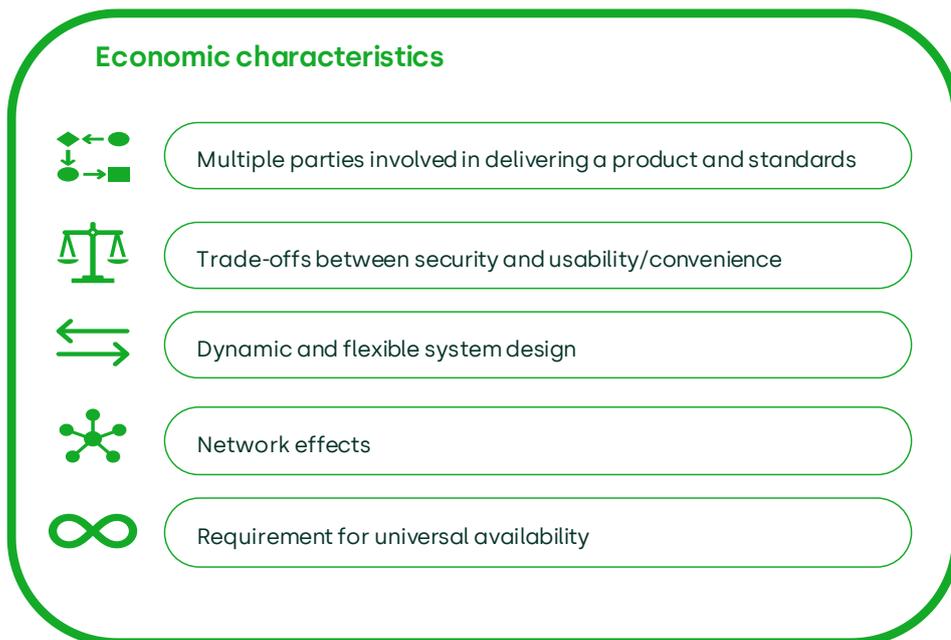
We find that the economic challenges discussed in section 3 are driven by the innate economic characteristics of Open Banking as a product, and will need to be addressed for the Open Banking system to successfully expand and improve. In other words, a model is required that provides incentives for all parties involved, allows for internalisation of trade-offs, and provides coordination. It is likely that no one model will meet these criteria for all use cases, and thus we consider three different models which may serve different use cases depending on whether coordination or incentives are more important, or if both are equally important. We discuss this in more detail in section 5.

We also consider case studies from different ecosystems. Each of these case studies has both similarities and differences compared with an Open Banking ecosystem, and illustrates how alternative models have created successful ecosystems.

4.1 Identification of key economic characteristics of Open Banking as a product

The key innate economic characteristics of Open Banking as a product are summarised in Figure 4.1 below.

Figure 4.1 Economic characteristics of Open Banking as a product



Source: Oxera.

4.1.1 Multiple parties together deliver one product

Open Banking necessitates that multiple parties coordinate to deliver a product or address a consumer need. This is true for both payments and data sharing. On the payments side, in a simplified model, ASPSPs provide authentication, clearing and settlement to facilitate services offered by PISPs. Merchants may pay a fee to the PISPs for the particular service, and customers provide consent for the transaction to proceed. On the data side, in a basic model, ASPSPs provide access to transaction data to enable products and services offered by AISPs. AISPs may charge a fee for the use of their products and services, and must also receive consent from the end customer.

The many interactions between players, therefore, necessitate a certain level of standard setting.³⁷ Standards which are common across the industry can reduce implementation costs. As such they can reduce a barrier to entry for potential new providers, making it a more level playing field for new entrants. Common standards also help to ensure a more consistent experience for end users, and reduce the risk of market fragmentation.

Common minimum standards are more likely to be adopted when non-adherence has some economic and/or reputational consequence. However, more generally, a certain degree of coordination is also required, in particular in relation to the design of the product in the first instance and then the delivery and subsequent adoption of the product.

4.1.2 Trade-offs between security and usability/convenience

Open Banking involves trade-offs between ensuring security and convenience: a secure system that provides user protection while also providing the best possible functionality and usability on the front-end.

As discussed in section 3 above, trade-offs may not be optimally made if they are not internalised (i.e. the costs and benefits are spread across multiple parties within the ecosystem). This is the case under the current model which does not offer the opportunity for this kind of internalisation in most situations. It also means that risk-reducing efforts might be foregone by a party not exposed to the costs of these risks. Importantly, the decisions as to how to balance these trade-offs are usually better made by market participants who understand the risks and rewards more than a public body such as a regulator.

Designing an interface that is user-friendly and convenient is difficult, and is made even more difficult when factoring in the trade-offs associated with security risks. User experience of Open Banking solutions will be driven by the design choices within the APIs, as well as the rules and standards implemented by different parties within the ecosystem. This requires a constant process of trial, feedback, and

³⁷ At some level, this can be compared with, for example the common standards that are required in telecoms and IT infrastructure to ensure that voice and text communications are converted into data packets that can be converted back to sound or text by another operator at the other end of the communication.

improvement. It is an area that even some of the most successful technology companies sometimes get wrong by failing to take customer feedback on board.³⁸ Innovation in this area is an inherently dynamic activity, which is the next product characteristic.

4.1.3 Dynamic

Open Banking also requires a dynamic and flexible system as certain features or offerings have to be optimised over time due to the changes in risks (e.g. cyber threats), regulations, and requirements to improve usability and convenience. In particular, regulatory API standards face administrative burdens, making them slow to evolve and respond to new needs.³⁹

To combat the limitations of regulatory API standards, NatWest has introduced changes to the commercial VRP standard (e.g. merchant name in payment flow), which can be enforced on PISPs via contractual agreements. While the overlay of commercial and regulatory standards would likely increase the complexity of the ecosystem, it helps improve the agility and flexibility of Open Banking, providing enhanced functionality beyond the regulatory minimum.

Moreover, innovation in relation to security is an inherently dynamic environment, as no system can be designed to be fool-proof. Software developers are engaged in a constant game of cat and mouse with malevolent actors constantly searching for security weaknesses to exploit.⁴⁰ A static system where the relevant changes can only be made at set intervals after consulting multiple stakeholders would limit the ability of players to respond to new threats. Any improvements may require new trade-offs which have not yet been internalised by one party.

A static system where the relevant changes can only be made at set intervals after consulting multiple stakeholders would limit the ability of players to respond to new threats.

4.1.4 Network effects

Network effects are inherent in Open Banking. In terms of payments:

- the more merchants are willing to accept a payment mechanism, the more valuable it will be for consumers;

³⁸ And, in one or two high profile cases, even telling customers that they are the ones at fault. For example in 2008, Microsoft took out adverts effectively describing the critics of their new Operating System, Windows Vista as people who believed the Earth was flat. See Kingsley-Hughes, A. (2008), 'Microsoft's "flat Earth ad falls flat for me', *ZDNET*, 22 July, (last accessed 10 April 2023). Similarly, Apple was mocked after the release of the iPhone 4 for telling consumers to hold their phone differently to avoid antenna and signal issues. See Sarno, D. and Milian, M. (2010), 'Don't hold iPhone 4 that way, Apple says', *Los Angeles Times*, 26 June, (last accessed 10 April 2023).

³⁹ Regulatory API standards are designed by stakeholder forums and consultations which can result in long decision-making processes. For instance, discussions in relation to an update to the regulatory standard (v3.1.11) started in November 2022, followed by an Expert Advisory Group being formed and draft standard for consultation being issued in April 2023 for some minor changes. We understand that this will likely result in the standard being published by July 2023, with six months for banks to implement the changes. Overall, v3.1.11 will have taken 14–15 months to deliver these relatively minor changes.

⁴⁰ Consider, for example, the frequent software updates for operating systems on computers and phones which are required to fix critical security flaws.

- the more consumers who want to, and whose banks provide the facility to use a payment mechanism, the larger the number of merchants that will be willing to accept it.

Similarly, in terms of data:

- the more valuable uses there are for Open Banking data (or the greater the utility of individual use cases), the more consumers (whose banks offer the ability) will be willing to use Open Banking applications;
- the more applications there are using access to a consumer's data to save the consumer time or money, the more consumers will be willing to grant such access.

The existence of network effects means that certain products based on Open Banking will only be successful if it reaches a certain scale and critical mass. As explained in section 3 above, Open Banking in the UK has not yet reached a scale and critical mass to make it an unequivocal success. There will be implications here for carefully assessing demand, and designing a proposition that will sufficiently attract customers on both sides, as discussed in section 3.2.

4.1.5 Requirement for universal availability

Universal reach goes beyond network effects, and may be required for certain types of products or services. It is partly driven by consumer expectations. For example, when using a mobile phone network, consumers would expect to be able to reach anyone else that has a phone, irrespective of the type of network used by other consumers. Similarly, in the case of credit transfers, universal reach is an important characteristic—consumers would expect to be able to transfer money to anyone with a bank account, and a bank would be unlikely to be successful if it could only send credit transfers to a subset of all banks in a country (or the world). In practice, this means that there *is* interoperability between mobile phone networks and that countries either have one credit-transfer processing system to which all banks are connected, or multiple systems with interoperability.

Related to the concept of universal *reach* is the idea of universal *availability*. PayPal has universal availability in terms of everyone *can* sign up to get a PayPal account even if it does not have universal reach (i.e., not everyone *has* signed up).

The requirement for universal availability may apply to certain products based on Open Banking. Without universal availability, (i.e. participation by all ASPSPs), certain products may simply not be sufficiently convenient or credible. For example, an age verification product that only gives access to customers of a few ASPSPs, may not be sufficiently attractive to businesses. At the very least, it would introduce friction or confusion in the consumer experience. Being able to check the age of—in principle—anyone, irrespective of where they hold their current account, is likely to be the minimum expectation. Universal availability can be achieved by bringing use cases within the Open Banking mandate, but in the absence of a mandate, incentives must be provided to bring ASPSPs on board.

An age verification product that only gives access to customers of a few ASPSPs, may not be sufficiently attractive to businesses. At the very least, it would introduce friction or confusion in the consumer experience. Being able to check the age of—in principle—anyone, irrespective of where they hold their current account, is likely to be the minimum expectation.

Universal reach is not required in relation to the *acceptance* and *holding* of payment methods. A payment product such as debit and credit cards can be successful even if only some consumers hold it or some merchants accept it—consumers and merchants can always switch to another payment method.

A payment method that lacked *universal availability* (or at least very widespread availability), i.e. could only be used to initiate payments from one or two banks (and therefore could in principle only be used by a minority of customers) may not be sufficiently attractive for merchants to be willing to accept. For certain use cases, then, the products would only be successful if most major ASPSPs participate.

However, a payment method that lacked *universal availability* (or at least very widespread availability), i.e. could only be used to initiate payments from one or two banks (and therefore could in principle only be used by a minority of customers) may not be sufficiently attractive for merchants to be willing to accept. For certain use cases, then, the products would only be successful if most major ASPSPs participate.

Note that the requirement may not, for all use cases, strictly speaking, be 'universal'. Nevertheless, there will be some critical mass of consumers for whom the product must be *available* in order for the payment product to be sufficiently attractive to merchants.

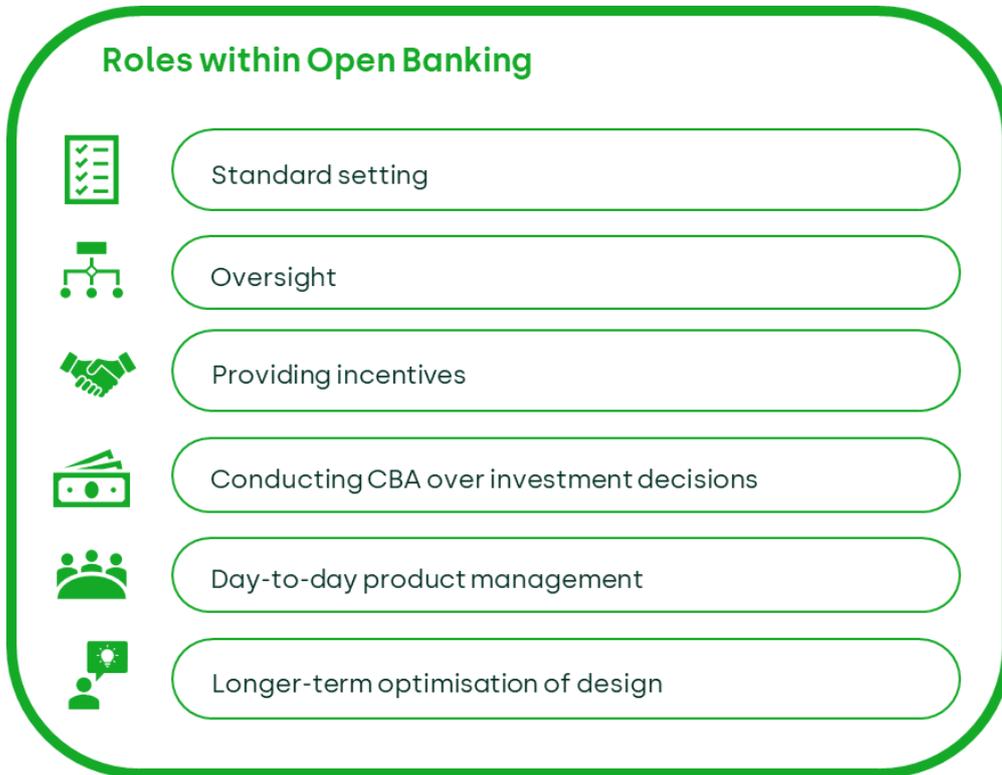
Essentially, *availability* needs to pass a threshold on one side of the market in order for the product to be attractive to the other side of the market. As such the issue is related to the characteristics of network effects discussed above, but in terms of one side of the market recognising that there is the *potential* on the other side.

Alongside universal availability, a product based on Open Banking will achieve greater market penetration faster if it becomes associated with a branded logo to show where it may be used. For example, the contactless symbol showed consumers where they could use the contactless payment feature of their card.

4.2 Related roles for Open Banking as a product to be successful

In addition, for Open Banking to be successful, there are key roles that must be filled, as shown in Figure 4.1 below. The question remains as to which party is best suited to which role.

Figure 4.2 Key roles in Open Banking



Source: Oxera.

4.2.1 Standard Setting

Within a particular use case, standard setting, whether established by an industry body or regulator, or developed competitively, can reduce entry costs, making it a more level playing field for new entrants (see section 4.1.1). However, there is a distinction between the economic benefits of common standards, and who sets them.

A clearly defined role for an entity to provide standard setting is key for an Open Banking system to function well. As discussed in section 4.1.1 above, when multiple parties need to coordinate to deliver a system, standards for both payments and data must be established. This standard setting may include, for instance, the standardisation of dispute processes or provision of certificates for approved actors within the ecosystem. It may be necessary to draw a distinction between broad principles for the ecosystem which might be set by a regulator, and product-specific standards which might be set by a market participant. There may be costs to fragmentation as a result of multiple sets of standards, but the more agile standard setting of a body with commercial incentives might provide advantages in a dynamic environment; while broad principles established by a regulator can promote fairness objectives.

Sometimes, standards might be established by an external party such as an industry body with various stakeholders (a federated body or trust model) or by a regulator (a 'single centralised model').⁴¹ For example, with respect to the former, the SPAA scheme discussed in

⁴¹ Strategic Working Group (2023), 'The Future Development of Open Banking in the UK', February, p. 186.

section 2.3 is not only led by a multi-stakeholder group made up of industry participants⁴², but also receives input on its draft deliverables from a dedicated group of non-EPC members.⁴³

4.2.2 Oversight

There is also a role for an entity to provide oversight and coordination in the system as a whole to ensure standards are being observed and parties are able to coordinate effectively. Without this role, parties may not always adhere to standards that are necessary for the system's stability and interoperability. As a result, the Open Banking system would not be able to operate as intended, and the parties would not be able to realise its intended outcomes.

However, retaining both regulatory oversight and oversight of commercial/contractual rules and standards within the same entity can lead to risks around governance, and how potential conflicts of interest are managed.

The regulator may be required to oversee the Open Banking ecosystem to ensure that regulatory obligations are being met by market participants. This role would be distinct from a commercially oriented entity, led by market participants, that could fulfil other roles discussed below such as day-to-day product management and more detailed product design.

4.2.3 Providing Incentives

There is an important role for an entity to work with all parties that are involved in delivering the product or service to design a system that creates the correct incentives for the Open Banking ecosystem to be successful.

This involves aligning incentives for key parties and allowing for the internalisation of trade-offs, as discussed in section 3. It should also allow for sufficient flexibility within that system to evolve, as incentives may change due to changes in risks and new innovations. Incentives may also need to be aligned in relation to the analysis of the costs and benefits of investment decisions.

4.2.4 Conducting cost–benefit analysis over investment decisions

Any firm or public body considering an investment to deliver innovation would normally attempt to assess the net benefit through a cost–benefit analysis (CBA).

There is an important distinction between unilateral and collective innovations. Collective innovations involve the adoption of a new approach across the whole industry. Unilateral innovations can be brought forward by a single company, which then bears the cost of the innovation (and receives the benefits).

⁴² European Payments Council (2023), '[SPAA MSG Membership List](#)', (last accessed 26 May).

⁴³ European Payments Council (2022), '[SPAA Scheme Status Update 17 June 2022](#)', (last accessed 26 May).

Absent a coordinating entity, the Open Banking ecosystem would consider proceeding with the investment only if it passed the CBA case for each individual player.⁴⁴ However, collective innovation that is desirable from an ecosystem or product perspective might not pass the private CBA case for each party (or—indeed—for any individual party). In this case, the investment would not be taken forward. This is similar to the classic public goods provision problem in economics.⁴⁵

A lack of alignment between industry participants may mean that different approaches to the CBAs are taken, with varying results. One or two participants with low CBA estimates could, in this situation, become 'hold outs'—preventing an investment from going ahead. On the other hand, a third party entity conducting its own CBA may not have the relevant information or expertise to be able to accurately assess the costs and benefits, and therefore what level of investment is justified.

Therefore, within a successful ecosystem, there is a need for an entity to conduct a cost–benefit analysis on a collective basis, to decide whether an investment is justified as part of a whole-system approach. Once the CBA has been undertaken, the central entity then also needs to align incentives so that the parties that mainly benefit remunerate the parties that mainly incur the costs. Such an entity may also need to consider the role of incentives in bringing participants on board, where otherwise a private CBA may lead to underinvestment. This would depend on the specific context, but may include payments to incentivise participation or mandates to ensure participation.⁴⁶

Collective investment decision-making may be most effectively delivered through a commercial entity playing a coordinating role, although there can also be a role for some regulatory oversight here, as described in section 4.2.2 above.

4.2.5 Day-to-day product management

There is also a role for an entity to provide day-to-day management of the products within Open Banking. This role may include the management of the technical functioning of the product, marketing, as well as business functioning of the product (such as disputes and escalations) etc. The role would be separate from, but may ultimately report to, the regulatory entity providing oversight of the ecosystem discussed in section 4.2.2.

The entity managing the ecosystem as a whole may still be involved in the day-to-day product management of individual Open Banking products. However this would happen more as a regulator ensuring that objectives such as fairness and other stakeholder interests are

⁴⁴ Or a sufficient number that critical mass could reasonably be expected to be achieved (see section 4.1.5).

⁴⁵ The difference comes from the fact that not all of the benefits of each firm's participation/provision are non-excludable and non-rival.

⁴⁶ The coordinating entity may alternatively conclude from its analysis that the initial buy in from participants already provides critical mass (see section 4.1.5). Here, the product can be launched, with the expectation that the incentives of 'hold outs' will change, and they will eventually decide to join, as the costs of not joining when others have are too high.

represented within the ecosystem. The degree of their involvement would depend on the particular Open Banking use case.

4.2.6 Longer-term optimisation of design

All parties within the system are responsible for longer-term optimisation of some elements of the design. This may occur through dynamic responses to changing incentives on the part of PISPs or ASPSPs.

This may also be the responsibility of the standard-setting entity discussed in sections 4.2.1 to adapt the standards as required in response to any commercial or market development. The alternative to this responsive adaptation of standards is that, the standards from inception have sufficient flexibility such that they can be dynamic in order to allow the longer-term optimisation of design.

Exactly who has responsibility over which area of market design may differ depending on what product is being considered. Market participants would expect to have responsibility for their own particular services and offerings, but designing new features to the core APIs may be better addressed by an overarching ecosystem focused entity (i.e. the standard setting entity discussed in 4.2.1).

4.3 Case studies

In this section we turn to consider four case studies of different ecosystems. We use these case studies to illustrate various product characteristics and roles within the ecosystem, as outlined above, and their importance.

Each of these examples have both similarities and differences compared with an Open Banking ecosystem. However, across each example we observe a need for ecosystem-wide solutions, with some degree of standardisation or interoperability. Some examples show that where continuous optimisation of a product is less relevant, industry coordination around standards can be achieved without an additional formal entity fulfilling the key economic roles (described in section 4.2 above) on a day-to-day basis. This is the case for the communications or video-game-console case studies, as discussed below.

We also see that, in examples where there exists a greater need for dynamic optimisation, and where trade-offs exist within the system, a separate coordinating entity is often established. These bodies then have a degree of decision-making power to ensure incentives are aligned, and optimal investment and innovation decisions are taken. Examples of this can be seen in the case studies on iDEAL and Digital ID.

4.3.1 Communication systems

An example where universal reach is particularly important is mobile phone networks. Consumers would expect to be able to reach anyone that has a mobile phone or landline irrespective of the networks used by other consumers. This means that the mobile phone networks and mobile phone manufacturers have had to develop their devices and

Common open standards means that all email services are interoperable (i.e.

emails from different services, say Gmail and Outlook, can be easily exchanged). Standards

services according to an agreed standard that ensures interoperability. This involves coordination between the various parties involved on the technical standards, including on security. It also involved putting in place arrangements for the fees that networks charge to each other for the use of their network (e.g. call termination charges).

Email is another example of a mode of communication that is provided as a single service (i.e. an email account), but where multiple parties are involved in its provision. It is essential that the user of an email service is able to contact any email address they choose, regardless of the email provider they are using.

This is made possible through common open standards which mean that all email services are interoperable (i.e. emails from different services, say Gmail and Outlook, can be easily exchanged). Standards and protocols have been developed and adopted over time by industry participants. However, in these cases there is less need for dynamic optimisation over time, or for an entity setting rules and incentives in order to internalise trade-offs.

In each case, the parties are incentivised to participate in standardisation efforts, since the value of the offering is greatly enhanced if users can reach every other user. In telecoms, the value of a mobile contract is higher if it allows consumers to communicate with users on other networks—therefore a degree of cooperation on interoperability standards benefits all providers. Email providers typically do not charge users directly, but may be incentivised through the potential for advertising revenue, and larger user bases within a broader ecosystem.

4.3.2 Video game consoles

Video game consoles are another example of an industry which relies on an ecosystem of providers. Consumers purchase consoles and games (either directly or as part of a games subscription). Games are created by several games developers. Typically, gamers will use only one console, supplied by providers such as Microsoft (Xbox), Sony (PlayStation) and Nintendo (Switch). Within each ecosystem the console maker sets standards and publishes them to encourage developers to make games for their platform.⁴⁷

The success of these ecosystems also depends on a degree of quality control. In 1983, the market for video games crashed largely because the major console manufacturer at the time, Atari, did not 'lock-out' unauthorised games. Opportunistic developers flooded the market with poor quality games, and so the market unwound.⁴⁸

⁴⁷ Many games are developed to be played on more than one console. For example FIFA (Electronic Arts) Call of Duty (Activision) and Fortnite (Epic games)—three popular games—can each be played on Xbox, PlayStation and Switch.

⁴⁸ Hagiu, A. (2014), '[Strategic Decisions for Multisided Platforms](#)', *MIT Sloan Management Review*, 55:2, pp. 71–80.

4.3.3 iDEAL

iDEAL is a payment method established in the Netherlands in 2005 (i.e. pre-PSD2). iDEAL was (until recently) owned by the major retail banks in the Netherlands through a company called Currence—although the system supports many other participants, such as non-bank acquirers.⁴⁹

It is currently the most popular payment method for online transactions in the Netherlands (over 1bn transactions are made using iDEAL each year, approximately 70% of online transactions in the Netherlands).⁵⁰ It works by generating a SEPA credit transfer from within the online banking portal of a customer. Merchants receive real-time confirmation of payments. There is no additional buyer protection (i.e. protection in relation to the delivery).

We understand that retailers pay a per-transaction fee, and there is an interchange fee arrangement in place whereby acquirers compensate issuers for the costs incurred.⁵¹ This also means that the firms within the system are incentivised to participate in the development and implementation of common standards.

Currence sets the rules and standards of the system, and participants (including issuers and acquirers) must be certified by, and enter into a licence, certificate or accreditation agreement with Currence.⁵² These rules have been updated over time, and an expanded version of iDEAL is currently being rolled out,⁵³ which focuses on an improved customer journey and additional acquirer functionalities.⁵⁴

4.3.4 Digital ID

Each of the above identified roles, and some of the economic characteristics relevant to Open Banking, can also be seen as having been applied in the development and delivery of Digital ID products in various European countries.

A Digital ID is an electronic version of a physical identity document (such as a passport or driving licence) stored on a device, such as a phone. Digital technology is used to validate consumer identity through secure credentials, and could be constructed in various ways for different use cases.

⁴⁹ We note that iDEAL has recently been acquired by EPI, a European organisation owned by major European issuers and payment service providers. See EPI Company (2023), '[EPI Company announces acquisitions, additional shareholders and the coming launch of its new instant payment solution](#)', 25 April 2023, (last accessed 3 May 2023). EPI's goal in the acquisition is to create a Europe-wide instant payments solution. This acquisition does not alter the relevance of iDEAL as an example of a payments system that solves many of the challenges faced by Open Banking. If anything, the acquisition confirms that iDEAL has indeed resolved these issues successfully in setting up their ecosystem.

⁵⁰ iDEAL website, '[The New iDEAL](#)', (last accessed 31 March 2023).

⁵¹ Currence website, '[iDEAL, iDIN and eMandates role model](#)', (last accessed 31 March 2023).

⁵² See Currence website, '[Rules & Regulations](#)', (last accessed 31 March 2023).

⁵³ [iDEAL website](#), (last accessed 31 March 2023).

⁵⁴ The Paypers (2021), '[iDEAL 2.0 - a new chapter with Daniel van Delft](#)' (last accessed 31 March 2023).

While the precise model behind each of these propositions differs, each involves some common features. This includes a separate body which acts to ensure adequate coordination between the various players involved (e.g. banks, consumers and service providers), and that there are appropriate incentives in place, similar to those required in Open Banking.⁵⁵

Similarly, standard setting and oversight are also important elements for Digital IDs, and are typically undertaken by this body, and by the government (e.g. European eIDAS regulation,⁵⁶ and technical standards). Digital ID solutions are renewed or replaced over time as security requirements are updated and new technologies are developed.

Details of some Digital ID propositions from various countries are set out below. We note that this is not an exhaustive list of all the Digital ID propositions that have been developed.

- **Netherlands (iDIN).** This service is a digital ID allowing consumers to identify themselves, confirm their age or that they meet age criteria on websites (e.g. public institutions, insurance companies and online shops). Currence (an entity set up by the banks in the Netherlands, which is also the owner of iDEAL), is the owner of the digital ID product and performs various tasks including determining, managing and updating the rules and regulations, certifying and monitoring licensees, and coordinating anti-fraud measures.⁵⁷ To perform the role of issuer or acquirer, firms must obtain a licence from Currence, and businesses can participate through an acquirer, or via a 'Digital Identity Service Provider'.⁵⁸ Prices are charged by the participating banks in order to recoup their costs for providing iDIN through fee agreements with acquirers.⁵⁹
- **Belgium (itsme).** Established in 2017, itsme provides identity verification services and digital signatures.⁶⁰ It now has over 6m individual users (80% of Belgians use the itsme app), and over 800 companies and government platforms.⁶¹ The service is issued by Belgian Mobile ID, a joint venture of the major Belgian banks and (unlike the example from the Netherlands) telecoms operators. Government services access the service through brokers, while private sector services may access it directly.

⁵⁵ MitID website, '[About MitID](#)', (last accessed 17 May 2023).

⁵⁶ The Regulation on electronic identification and trust services for electronic transactions in the internal market ('eIDAS'). See European Commission, '[eIDAS Regulation](#)' (last accessed April 11 2023). The UK eIDAS regulations are an amended form of the EU rules, tailored for use within the UK. See Information Commissioner's Office website, '[What is the eIDAS Regulation?](#)' (last accessed 11 April 2023).

⁵⁷ iDIN website, '[Schemes](#)', (last accessed 3 May 2023).

⁵⁸ iDIN website, '[Partners](#)', (last accessed 3 May 2023).

⁵⁹ Currence website, '[iDEAL, iDIN and eMandates role model](#)', (last accessed 31 March 2023).

⁶⁰ Itsme website, '[The most secure identity solution for your business](#)', (last accessed 17 May 2023).

⁶¹ itsme website, '[itsme turns 5: 80% of Belgians already use the app](#)', (last accessed 17 May 2023).

- **Norway (BankID),⁶² Denmark (MitID),⁶³ and Sweden (BankID).⁶⁴** Each of these services are digital ID propositions where an organisation owned by the banks plays the role of coordinating actor.⁶⁵ In each case, the entity operates and develops the service. Service providers (including public authorities and businesses) access the Digital ID either through certified brokers, or in some cases directly through the participating banks—with mechanisms and agreements in place to compensate the issuing banks for the costs involved.⁶⁶
- **Australia (ConnectID).** ConnectID is an initiative of Australian Payments Plus (AP+), an organisation owned in part by the major banks in Australia.⁶⁷ It facilitates exchange between identity providers (i.e. issuing banks) and merchants (or government departments),⁶⁸ and is gradually being rolled out across various use case (such as age verification, authentication and document signing).⁶⁹ It uses the Open Banking principles of enabling consumers to consent to data providers sharing their data with approved TPPs. This allows multiple parties to be the providers of identity data, and from a consumer perspective is more accessible than needing to seek out a new form of ID as per other systems. ConnectID was accredited in 2021 under Australia's Trusted Digital Identity Framework (TDIF),⁷⁰ which monitors rules and standards set by the Australian Government.⁷¹ We understand that a mechanism is likely to be in place for the issuing banks to recoup their investment in providing the service, though details are not publicly available.⁷² The introduction of ConnectID represents a more holistic collaboration (via an industry body) than Australia's regulatory-driven CDR discussed in section 2.3. It is also potentially a cost-reduction

⁶² BankID was launched in 2004, and is now used by 4.4m consumers. See BankID website, '[About us](#)', (last accessed 17 May 2023).

⁶³ MitID is a digital ID service developed by the Danish Authority for Digitisation and Finans Danmark—an organisation representing Danish banks. See MitID website, '[About MitID](#)', (last accessed 17 May 2023). It is replacing previous schemes which were first issued by the Danish financial sector in 2010. See Agency for Digital Government, '[eID in Denmark](#)', (last accessed 17 May 2023).

⁶⁴ BankID was established in 2003 in Sweden, and is now widely used (6bn times in 2021). See BankID website, '[Six billion times](#)', (last accessed 17 May 2023).

⁶⁵ For example, in Norway the service is issued by the major Norwegian banks, with BankID Norway AS playing the role of coordinating actor. See BankID website, '[About us](#)', (last accessed 17 May 2023).

Similarly, in Sweden the banks are the issuers, coordinated by Financier ID-Teknik AB (a company owned by the banks). See BankID website, '[Introduction](#)', (last accessed 17 May 2023).

⁶⁶ In Norway BankID operates and develops the service and sells it to Norwegian companies via a third party dealer system. See BankID website, '[Pricing](#)', (last accessed 17 May 2023).

In the case of Denmark, service providers access the scheme through certified brokers, who pay per transaction fees to MitID. See MitID, '[Brokers contribute to the strength and security of the MitID solution](#)', (last accessed 17 May 2023).

⁶⁷ ConnectID was originally developed by eftpos (Australia's domestic debit card scheme owned by the major banks), which has since merged with other domestic payment companies to create AP+.

⁶⁸ Connect ID and Australian Payments Plus (2022), '[Industry Backs AP+ ConnectID for Aussie Digital Identity](#)', press release, 1 September, (last accessed 17 May 2023).

⁶⁹ ConnectID, '[See how ConnectID can work for your business](#)', (last accessed 17 May 2023).

⁷⁰ Australian Payments Plus (2023), '[ConnectID continues to tick all the right boxes for data security](#)', (last accessed 17 May 2023).

⁷¹ Digital Identity System [website](#), (last accessed 17 May 2023).

⁷² Eyers, J. (2022), '[Banks ready to launch new digital identity checking service](#)', *Australian Financial Review*, 31 August, (last accessed 17 May 2023).

exercise both for individual banks in providing access to verified consumer credentials, but also in terms of cost avoidance for each bank in delivering a data-sharing ecosystem in a coordinated way.

In each of the cases set out above in this section, the providers of the Digital ID products are incentivised to develop the service and standards in part through regulatory supervision, but also through commercial remuneration agreements.

We also note that in some instances public entities have created Digital IDs directly for use with online government services. In part this is because the public sector is often both a provider and user of personal attribute data (for instance the UK's HMRC).

4.3.5 Case studies: common themes

As explained above, these case studies cover ecosystems which each have similarities and differences when compared with Open Banking. While the specific details vary, some key themes emerge across the examples which helps to explain the success of each ecosystem.

Each example requires a degree of interoperability and/or common standards in order for the product to be valuable to consumers, and delivered by the ecosystem.

Where trade-offs exist within the system, and where there is a greater need for continuous optimisation, a separate entity tends to be established. In the example of iDEAL, or Digital IDs, these entities are commercial bodies which fulfil key economic roles described above (in this section).

Commercially motivated coordinating bodies are likely to ensure incentives are aligned, and attempt to promote optimal investment and innovation decisions by the various parties. Where continuous optimisation of a product is less relevant, industry coordination around standards can be achieved without the coordination of a commercial entity (e.g. for communications or video-game -console case studies). In any case, a prerequisite for a successful ecosystem is the need for incentives to be aligned to allow for the necessary coordination of industry standards.

These common themes are also highly relevant when we consider the economic characteristics present in the Open Banking ecosystem, and the related key roles required in order for Open Banking as a product to be successful. They will also inform an assessment of the most appropriate model for taking Open Banking forward, to which we now turn.

5 Possible models

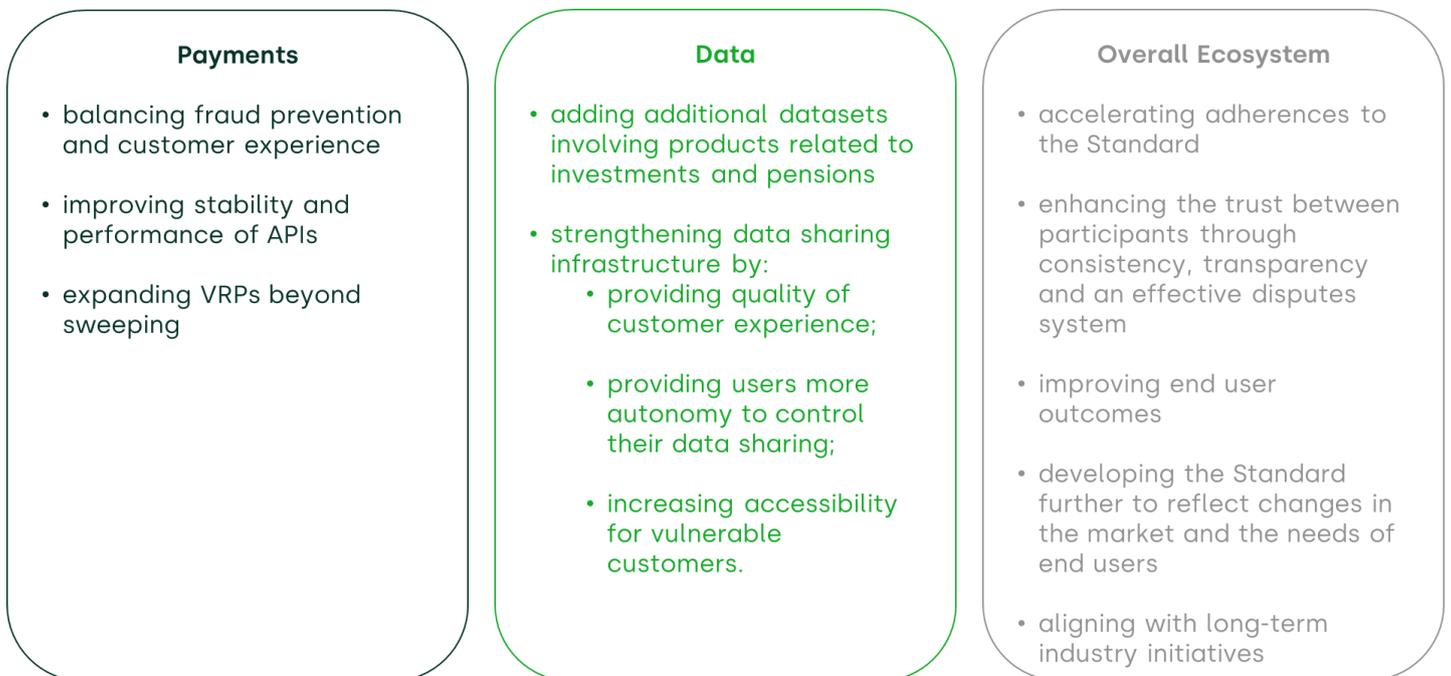
In this section we consider what are the possible models that could be applied to any extension of Open Banking beyond the current boundaries of the mandate. We first outline the key principles that should be considered in terms of any extension of Open Banking and then consider the models that could be applied.

In considering how to expand Open Banking, one should be aware that the competitive and technological landscape, and as a result consumer expectations, have changed since Open Banking was introduced almost a decade ago. Technological change means that Big Tech markets have been brought into a position which is adjacent to various consumer financial markets, in particular on the payments side. This has two implications: First, there is the potential for further Big Tech entry into financial services in general and payments in particular; second, consumers have become used to the streamlined user-friendly experience offered by Big Tech financial services (e.g., Apple Pay) and will expect similar streamlined offerings from Open Banking.

5.1 Key principles underlying possible alternative models

The Future Development of Open Banking report, published in February 2023, provided helpful insight to stakeholders' key priorities for future improvements, in areas including payments, data and the overall ecosystem. Specifically, the report identified the following thematic priorities for each area of Open Banking:

Figure 5.1: Open Banking Report thematic priorities



Source: Open Banking Strategic Working Group report for the Joint Regulatory Oversight Committee (2023), 'The Future Development of Open Banking in the UK', *Final Report*, Executive Summary.

What is missing is a clear plan as to how these objectives should be achieved. In section 3, we identified three main challenges of the current system. A lack of incentives, an absence of alignment, misallocation of liabilities and a lack of any mechanism to internalise trade-offs.⁷³

The overall effect in the wider economy would then be to reduce transaction costs. Lower transaction costs can promote competition as it becomes easier for consumers and SMEs to shop around and so raise consumer welfare.

An evolution of Open Banking to meet these challenges will be needed if the UK is to develop an Open Banking sector that reaches its potential. This could include an Open Banking payments option that, from merchants' perspective, competes with existing payment methods such as card payments or direct debits, and from consumers' perspective, would be at least as convenient. It could also mean data sharing that would help to reduce the frictions that are encountered in everyday life when a consumer is asked to prove their eligibility for a product or some other characteristic. This would offer a stepping stone to broadening the current Open Banking ecosystem to a wider Smart Data ecosystem.

The overall effect in the wider economy would then be to reduce transaction costs. Lower transaction costs can promote competition as it becomes easier for consumers and SMEs to shop around and so raise consumer welfare.

In terms of solutions, there are broadly three possible routes forward and different routes may be optimal for different use cases depending on which of the features outlined above are most pertinent in a particular use case. Two of these have already been discussed and this report introduces a third option.

5.2 Expansion of the Open Banking mandate—coordination without incentives

One option for the evolution of Open Banking might be to continue mandating the ASPSPs to provide (for free) better and wider APIs. However, as discussed in section 3, in the absence of commercial incentives that provide revenue-generating opportunities, ASPSPs will have no reason to go beyond the minimum standards. Furthermore, other ASPSPs may have been discouraged by the costs that were incurred by the CMA9 in developing their APIs. It may also have discouraged other financial providers not covered by the current mandate from innovating to begin the process of providing Open Finance.

Therefore, the only paths to increased innovation or improvement of the current regulator-mandated API design is either through:

- a more innovative use of the current APIs by TPPs and other users;

⁷³ There is also a need to bear in mind how policy developments in other areas might affect the Open Banking ecosystem. In the UK, the government has set up a Smart Data working group to maximise the potential of Smart Data initiatives. Any Smart Data Right for consumers and SMEs needs to be carefully designed and set a minimum scope for 'free' access. This would create space for commercial innovation to deliver more value to end customers.

- increasing the regulatory minimum.⁷⁴

The first may yield some benefits initially, but there will be diminishing returns over time, as the level of innovation possible within the constraints of the current Open Banking model is limited.

The latter is not likely to drive consumer-centred innovation in a dynamic environment. First, regulatory mandates may incorrectly predict which areas to include and exclude from scope. For example, under the current Open Banking model, ASPSPs were mandated to provide solutions for use cases such as setting up standing orders, but which have not been useful in practice.

Second, regulation may also distort the market in other ways, such as preventing dynamic market-led responses by ASPSPs and TPPs in a fast-moving industry. By the time new proposed regulatory standards are approved, the needs of the market may have evolved. In order for Open Banking to be competitive with existing payment methods, it must be able to be dynamic and responsive to market demands.

Third, innovation in terms of making online interaction easier is a constant process of trial and error where new (and old) hypotheses constantly have to be tested (and re-tested). This is something that firms with a profit motive will tend to do better than regulators.

However, this option does provide for coordination as all ASPSPs would be making the same API features available, so all products offered over Open Banking would have near universal reach. This may therefore be a reasonable option for use cases where universal availability is the most pertinent product characteristic, while commercial incentives and dynamic innovation are less important.

5.3 Voluntary Premium APIs—*incentives without coordination*

Hoping to expand Open Banking through a system of voluntary premium APIs, offering broader access than the APIs within the mandate, represents a continuation of business as usual. ASPSPs are able to do this today (and were able to do it before the mandate came about).

Clearly, commercial incentives are present for the development of premium APIs, for which ASPSPs may charge a fee. However, the strength of those incentives may be muted as a result of a lack of alignment in the perceived value of some premium APIs amongst ASPSPs. Above we highlighted how some products need to have (near) universal availability in order to be successful. For example, a non-sweeping VRP payment product or a digital ID product that would confirm customer characteristics at the point of sale (e.g. age verification) would need to be an option for a large majority of potential consumers in order for a merchant to be interested in using it. Such products are unlikely to be attractive if only a small minority of customers even has the potential to use them.

⁷⁴ For example, we understand that TPPs are arguing for greater 'write' access under Open Finance. This would include the ability to open and close accounts on consumers' behalf, and to change address etc. If free access was extended to these use case that would potentially force ASPSPs to change their commercial models.

Even if multiple banks were to develop such products independently in response to the incentives provided by premium APIs, there may still be coordination issues that would hinder the roll out and adoption of such products. Without coordination, such APIs may all work in different ways and have different protocols. Any FinTech writing an application to use those APIs in order to provide a service to consumers would—in effect—have to write a different application for each bank in order to work through the idiosyncratic protocols of each bank's API (this could work with a single front-end from the consumer's perspective).

However, even if it is possible to develop the same overarching product for all consumers, some banks may innovate differently and include different features. In that situation, it may prove impossible for a FinTech to construct a simple, streamlined, single product offering with a single front-end for all users independent of their ASPSP.

One possible outcome, should development of the Open Banking ecosystem be left to premium APIs, is that a large (potentially) online merchant may have the incentive and ability to partner with a small number of banks to create an Open Banking non-sweeping VRP payment product.

Premium APIs may provide (and have provided) sufficient incentives for banks to develop some Open Banking products. For example, NatWest has produced a customer attribute sharing premium API for identity services. However a lack of coordination has hindered their growth.

One possible outcome, should development of the Open Banking ecosystem be left to premium APIs, is that a large (potentially) online merchant may have the incentive and ability to partner with a small number of banks to create an Open Banking non-sweeping VRP payment product. Other ASPSPs may then join for fear of losing customers. The result would be that the design and rules of the system would be driven by large retailers and large banks, potentially, to the disadvantage of smaller companies and smaller stakeholders in the Open Banking ecosystem.

5.4 The potential for a three- or five-party system

It is possible to combine commercial incentives with coordination, and so achieve take-up for a product that requires (near) universal availability, and ensure that ASPSPs and TPPs have incentives to produce the best products they can and internalise the trade-offs inherent in Open Banking. Commercial incentives can be provided by ensuring that ASPSPs are paid when their APIs are called, but some overarching entity coordinates the standards used by these APIs. An overarching entity could similarly ensure that products requiring universal availability are developed by all ASPSPs.

This is how the three- and five-party systems that have successfully developed credit-transfer based payment methods and digital ID verification systems have been set up and operated in Europe (see section 4), as well as traditional payment card schemes.⁷⁵

⁷⁵ What we are referring to here as a five-party system is normally referred to as a four-party system. We are referring to it as a five-party system here as we wish to highlight the role of the party that is in the position of a card scheme, coordinating the card services.

In a three-party system (e.g., American Express), the product owner will charge merchants a fee for using its payment services, and may offer incentives to the consumer (e.g. cashback or air miles) to get them to use the payment method they have been given access to.⁷⁶ In a five-party system, a central coordinating party (such as a card scheme) will operate in much the same way, but typically reaches merchants through acquirers, and consumers through issuers. The rules stipulate that an interchange fee must then be paid from the acquirer to the issuer. This interchange fee effectively compensates the issuer for some of the costs and risks they take on in the payments system through their relationship with the consumer.

Within such a model, almost all of the roles outlined in section 4.2 in terms of setting standards, oversight, providing incentives, conducting cost–benefit analyses over investment decisions, day-to-day product management and longer-term optimisation of design, are conducted by the scheme. Within a five-party system, some elements of these roles might be delegated. For example, the day-to-day management of customer relationships and some investment decisions are delegated to acquirers and issuers.

Within the Open Banking ecosystem, there are many products (and possible products) and it is not necessarily the case that the same parties should fulfil the same roles for all products. Products may need to be treated on a case-by-case basis, and it is beyond the scope of this report to assess which model is most appropriate for each product. However, one distinction we do draw concerns the distinction between questions of oversight *within* particular products, and oversight of the *Open Banking ecosystem as a whole*.

- Oversight of particular products in terms of standard setting for APIs, and the provision of incentives, etc., might be best left to commercial entities that will have incentives to maximise take-up.
- Oversight of the Open Banking ecosystem as a whole might be best managed by a regulator to ensure stakeholders have incentives to provide new products, and to provide for some basic levels of consumer protection that are typically provided elsewhere in the financial ecosystem.

We note that these proposals may see firms being subject to two sets of regulations, in terms of overarching commercial entities setting regulations to make specific products work and ensure efficient interoperability between the different providers, as well as regulations from a public body managing the ecosystem. However, it is also the case that this works well in other environments—for example acquirers and issuers within the existing five-party payment systems must observe the rules of the systems within which they operate, and are also subject to broader regulation by public authorities.

An overarching commercial entity may be best placed to set standards and provide incentives for other participants *within* particular products because they will have an incentive to make the choices that promote take-up. The higher the rate of take-up of the

⁷⁶ Note that many 3 party services now use independent acquirers—so might now be considered 4 party systems.

product, the higher such an entity's profits will be. A commercial entity is also likely to be more agile in the sense of being able to respond more quickly to changing incentives, changing the protocols APIs must fulfil as well as other standards where required. They can also respond quickly to customer feedback on the user interface.

The constitution of such a commercial entity is something that might vary according to need within the Open Banking use case under consideration. One option might be that it could be a joint venture between banks and other stakeholders. This has been a solution in some of the case studies we have seen (e.g. Currence, itsme, BankID, MitID). An alternative would be that a completely new commercial entity be established. Consideration would need to be given early on to the competition law implications surrounding the way in which the commercial entity is constituted and makes decisions. Otherwise the legal risk may become an obstacle to such a commercial entity being established.

In terms of the ecosystem as a whole, the oversight role may be best played by a specialised regulator. Such a regulator will need to be capable of taking a wider view and considering input from all stakeholders in the industry as to potential use cases that might add consumer value and what might be holding the ecosystem back from providing such use cases. The role of the regulator should not be to directly oversee the provision of Open Banking use cases and products, but rather to examine what the road blocks to the provision of such use cases might be and seek to unblock them by ensuring that the relevant stakeholders have appropriate incentives.

Such a solution might be most appropriate in a dynamic environment where commercial incentives and universal availability are both important; and where it is possible to ameliorate any potential competition concerns that arise from the necessary cooperation between ASPSPs and TPPs.

5.5 Conclusions

It is important to note that Open Banking may not be the right solution for every issue in retail financial services, nor should replacing retail finance with Open Banking be the goal of the industry or regulators.

The introduction of Open Banking in the UK has had some early successes. Particularly in terms of rapidly mandating and setting standards for ASPSP's APIs used by TPPs to access the banking infrastructure. However, there is room for improvement.

The CMA's Order has effectively divided the UK Open Banking ecosystem in two.⁷⁷ In the area covered by the Order where the UK's main ASPSPs are required to provide free access via APIs, there is coordination, but a lack of commercial incentives. This is suitable for

⁷⁷ Note that there is actually a third area of the ecosystem as well, which is the free payment account access that must be provided by non CMA9 banks under PSD2. However we focus on the two areas above to illustrate the point about incentives and coordination.

Open Banking use cases where universal reach is important, but commercial incentives matter less.

In the area outside the Order (and not covered by PSD2), there are commercial incentives, but a lack of coordination is likely preventing the realisation of certain Open Banking use cases, in particular those that require universal availability. This would be suitable for use cases where commercial incentives and dynamic innovation are important, but universal availability is less of a concern.

This report suggests adding a third option in multi-party systems with commercial governance that could provide commercial incentives sufficient to get all the relevant parties on board and align incentives to internalise trade-offs. This option would be suitable where commercial incentives and universal availability are both important, and where potential competition concerns arising from cooperation across different firms can be ameliorated.

This report suggests adding a third option in multi-party systems with commercial governance that could provide commercial incentives sufficient to get all the relevant parties on board and align incentives to internalise trade-offs. This option would be suitable where commercial incentives and universal availability are both important, and where potential competition concerns arising from cooperation across different firms can be ameliorated.

Developing products to meet use cases within the Open Banking ecosystem will involve paying close attention to which of the characteristics of Open Banking products are most important and carefully considering which of the three options for provision above is most appropriate in terms of being able to provide sufficient incentives for rapid development and adoption.

The future regulatory framework should prioritise the below.

- Removing potential roadblocks to the development of new services, recognising that these new services must be delivered by multiple parties, and that their development will be costly for all—so they should all be entitled to monetise these new products and services.
- Coordinating the development of new products where an industry-wide cost-benefit analysis demonstrates that there is a clear net benefit to such a product, but its development is subject to common action problems as the product requires universal availability to be successful. In such circumstances, regulators should consider carefully which of the models of provision outlined above is most likely to promote uptake given the balance of product characteristics within the use case.
- Any Smart Data right for consumers and SMEs, and Open Finance regulation, must be carefully designed to balance a 'free' access right with scope for commercial innovation to deliver more value to end customers.

The result of applying the correct framework to the correct Open Banking use cases should be faster roll out and adoption of Open Banking. This should not be considered a goal in itself, and—as discussed above—there is a need to consider carefully whether Open Banking is the 'correct' answer to the question raised by each potential use case.

Contact

Andrew Mell
Technical Adviser
+44 (0) 20 7776 6644
andrew.mell@oxera.com

oxera.com

