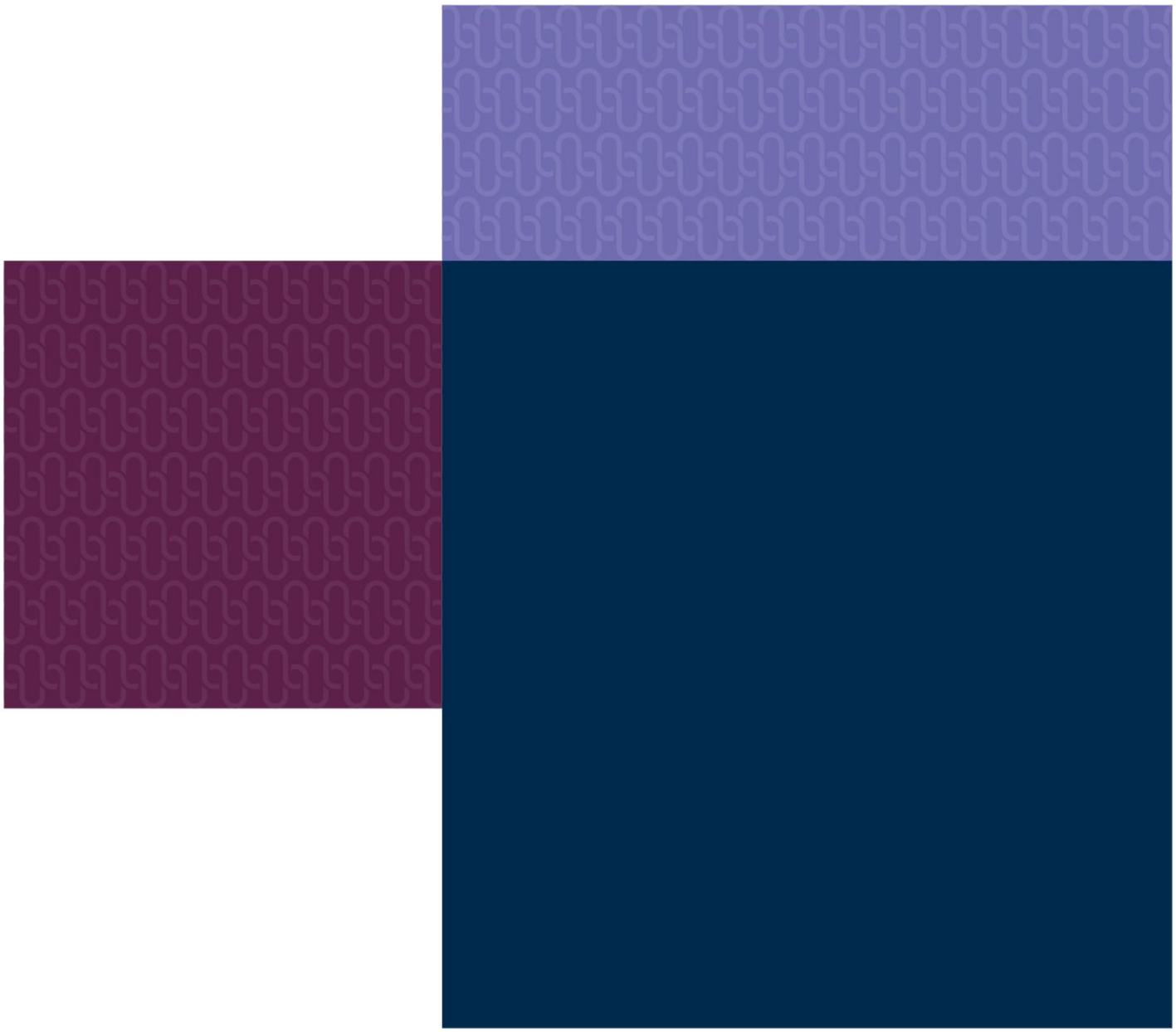
BANK OF ENGLAND

Fintech

Open data for SME finance

What we proposed and what we have learnt

March 2020



Contents

Contents **2**

1. Introduction **3**

2. How open data could help address the SME funding gap **4**

2.1. Changes taking place in the economy 4
2.2. The economics of data 5
2.3. The state of SME lending in the UK 6
2.4. The economics of the SME lending market 9
2.5. Recent and forthcoming initiatives to support SME finance 10
2.6. A proposal for an Open Data Platform 11
2.7. What the Open Data Platform would look like in practice 12

3. Policy issues and design considerations **15**

3.1. Policy issues 15
3.2. Design considerations 17

4. Engagement with industry and authorities **19**

4.1. The benefits of data portability 19
4.2. The need for the right technology and standards 19
4.3. The case for additional data 19
4.4. Views of public authorities 20
4.5. Plans for implementation 20
4.6. Summary 20

5. Lessons from around the world **21**

5.1. China 21
5.2. India 22
5.3. Estonia 23
5.4. Australia 23

6. Technical considerations **25**

6.1. Conceptual architecture 25
6.2. Principles for the architecture and technology 25
6.3. Design choices 26
6.4. Other governance considerations 28

1. Introduction

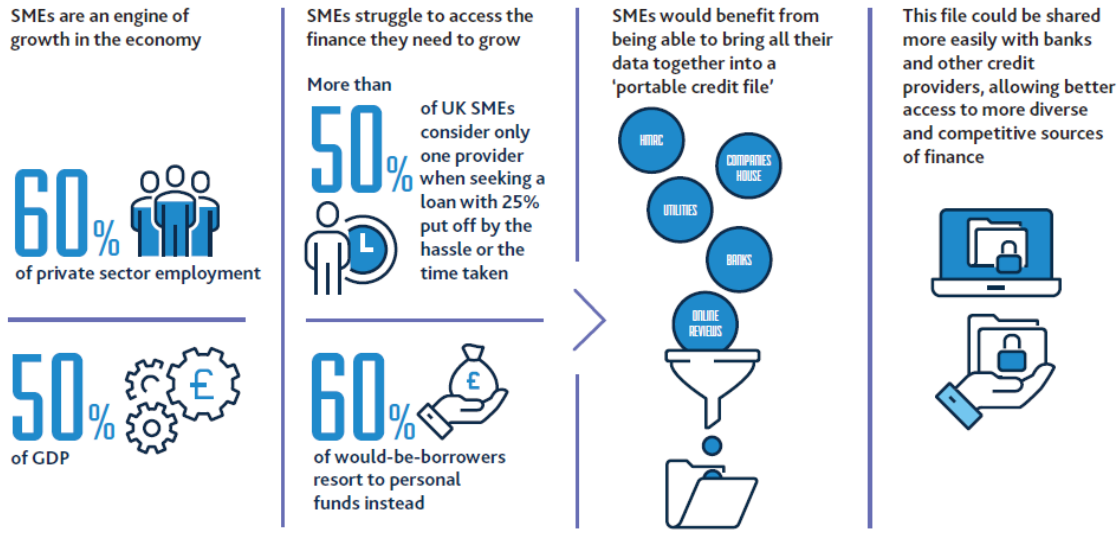
In 2018, the Governors of the Bank of England commissioned an independent review on the Future of Finance, how it might respond to long-term trends shaping the economy, and how the Bank should evolve to support it. That Future of Finance Report, along with the Bank's response, was published in June 2019.[1]

The reports described how the economy is becoming increasingly digital, with every transaction adding to an ever-longer trail of data. And they explained how the financial system is beginning to harness that data, using the latest technology to deliver more tailored services and keener pricing.

The Bank's response identified five priority areas where it could have greatest impact. One of these was to help develop an open platform to boost access to finance for small businesses up and down the country. Inspired by Open Banking, it proposed a vision for how open data across the whole economy could ease frictions in the financial system, in particular to help close the £22bn funding gap for small and medium-sized enterprises (SMEs) across the UK.

This paper explains the proposal in more detail, and provides an update on what we have learnt from our research and industry engagement to date. It will guide the Bank's ongoing engagement with public authorities, including as an input to the Government's Smart Data Review and Digital Markets Taskforce, as well as the Financial Conduct Authority's (FCA) Open Finance initiative. In particular, this paper will form part of the Bank's input to the Government summit announced in the 2020 Budget, looking at what further data needs to be made accessible to make it faster and easier for SMEs to shop around for credit.[2]

Figure 1: How an open data platform could deliver a portable credit file for SMEs



Source: Bank of England; BVA BDRC Continental *SME Finance Monitor;* Competition and Markets Authority *Retail Banking Market Investigation*

[1] *Future of finance: review on the outlook for the financial system and what it means for the Bank of England* (June 2019) and *New economy, new finance, new Bank: the Bank of England's response to the van Steenis review on the future of finance* (June 2019).
[2] *Budget 2020*, 11 March 2020.

2. How open data could help address the SME funding gap

2.1. Changes taking place in the economy

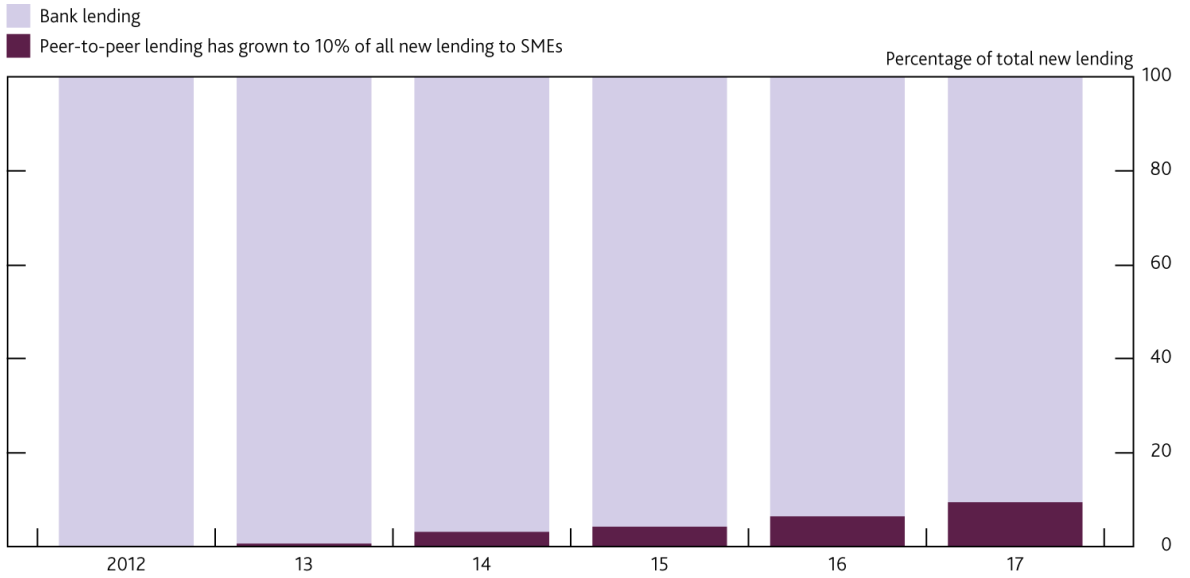
The economy is becoming increasingly digital and the financial system needs to adapt to these changing demands.

The nature of commerce is changing as new technologies shape a new economy.[3] An increasing amount of activity is taking place online as platforms enable direct connections between people and businesses globally. These online interactions are generating vast quantities of data that are being used to improve and personalise products and services.

Online platforms have enabled a sharing economy, facilitating a shift away from asset ownership amongst some cohorts of the economy. The decline in asset ownership reduces the ability for these groups to access certain financial services, such as secured lending, given the lack of collateral they can provide. And, as the economy has become increasingly capital light, flexible and dynamic, the financial system has become more reliant on the value of intangible assets.

The nature of work is changing too. In the UK, one in ten people worked in the "gig" economy over the past year, and nearly one in six British workers were self-employed.[4] Work through platforms is often characterised by variable incomes, which means those workers are less likely to be deemed creditworthy by traditional finance and lending models.

Chart 1: Peer-to-peer lending to SMEs has grown



Source: Cambridge Centre for Alternative Finance and UK Finance

[3] *Enable, empower, ensure: a new finance for the new economy*, Mark Carney (June 2019).
[4] *Platform work in the UK*, University of Hertfordshire survey and ONS *employment and labour market statistics*.

New financial services business models have emerged in response to this new economy. Alternative lenders, including peer-to-peer models, have grown rapidly since 2012 to service unmet demand **(Chart 1)**. Fintechs around the world are finding ways to streamline on-boarding and verification of individuals and small businesses through new sources of data. Others are combining data with advanced analytical techniques to enrich credit scoring and open up lending to previously underserved parts of the economy.

2.2. The economics of data

Data has unique properties that suggest it should be accessed in the digital economy rather than owned.

As economic activity moves online, it produces an increasingly long trail of data. Firms in all sectors of the economy are starting to realise the value of this data. The largest technology firms are already demonstrating the value of gathering and analysing data at scale to understand macro trends and predict demand. Innovative businesses are using novel sources and big data to understand customers better and deliver more tailored and more keenly-priced products and services.

In an economic model, data would be considered a factor of production. Analysis of that data forms part of the production function, in which businesses combine their land, capital, labour and data resources to produce the goods and services that consumers demand. Data helps firms understand their customers and their own production process. And just as technology innovations can generate gains in productivity, advances in data analytics can improve the quality and efficiency of their production process. Data therefore has private value to a business.

But data has a unique feature that sets it apart from the other factors of production: the use of data by one party does not make it less usable by others. Economists would say that data is *non-rivalrous*, much like street-lighting or radio waves.

As a result, that same data also has value beyond the private interests of a single business. Because data can be replicated, it can also be combined with other data at relatively low cost. That combination of datasets can deliver additional insights and is one reason why many of the largest technology companies have grown in value so rapidly in recent years. It also explains the emergence of a growing market for personal data, in which buyers pay for and use data to enhance the marketing of products and services. And it explains why governments around the world have sought to regulate the collection and use of personal data to protect the rights of individuals, including through regulations such as GDPR in the EU.[5]

The non-rivalrous nature of data has implications for how it should be used in the economy. It suggests that, although data can be proprietary, its value to the economy is maximised when it can be shared and combined with other data cheaply and easily. That in itself increases the importance of protecting the interests of individuals in the economy and leads to a model where data might be accessed with the right permission, rather than owned.[6] This is consistent with regulations such as GDPR, which focus on transparency and control of data, rather than rights of ownership. Private companies could compete on the *analysis* of data rather than the quantity of data they can collect.

Advances in technology have made this new model of data portability economically viable. Increased computing power and speed of communication have made it cheap enough and fast enough for data to be accessed remotely in the cloud. The economics now favour rapid transmission of data rather than local storage. This will help the digital economy of the future to embrace the portability of data instead of local ownership and storage.

---

[5] *The General Data Protection Regulation.*

[6] *The Economics and implications of data: an integrated perspective*, IMF Departmental Paper no. 19/16.

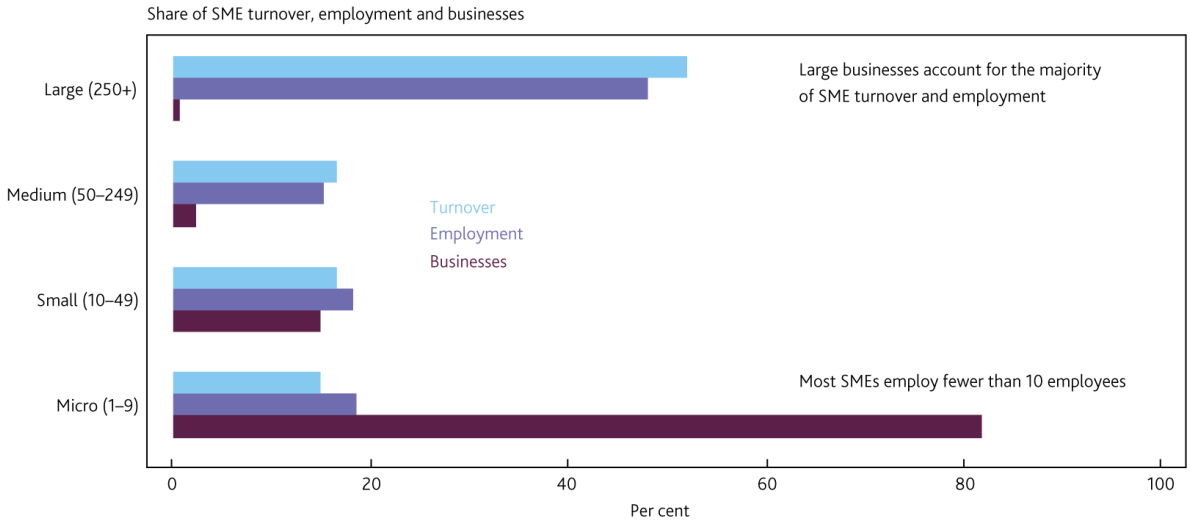
2.3. The state of SME lending in the UK

SMEs are an engine of growth, but accessing the right finance can be difficult, particularly for fast-growing businesses outside of London and the South East.

There are 5.9 million small and medium-sized enterprises (SMEs) in the UK.[7] They are an engine of growth, employing 60% of the private sector workforce and contributing 50% of UK GDP.[8]

SMEs are usually defined as private businesses with fewer than 250 employees or an annual turnover of less than £25m, but they are a heterogeneous group.[9] The large majority have fewer than 10 employees and together account for less than a fifth of all SME employment (19%) and turnover (15%) **(Chart 2)**. And there are a small number of larger SMEs with over 250 employees, which account for around half of all SME employment and turnover. There is significant regional variation too. For example, in the South West SMEs account for 73% of employment and 58% of turnover, significantly higher than the UK average.

Chart 2: SMEs are a heterogeneous group

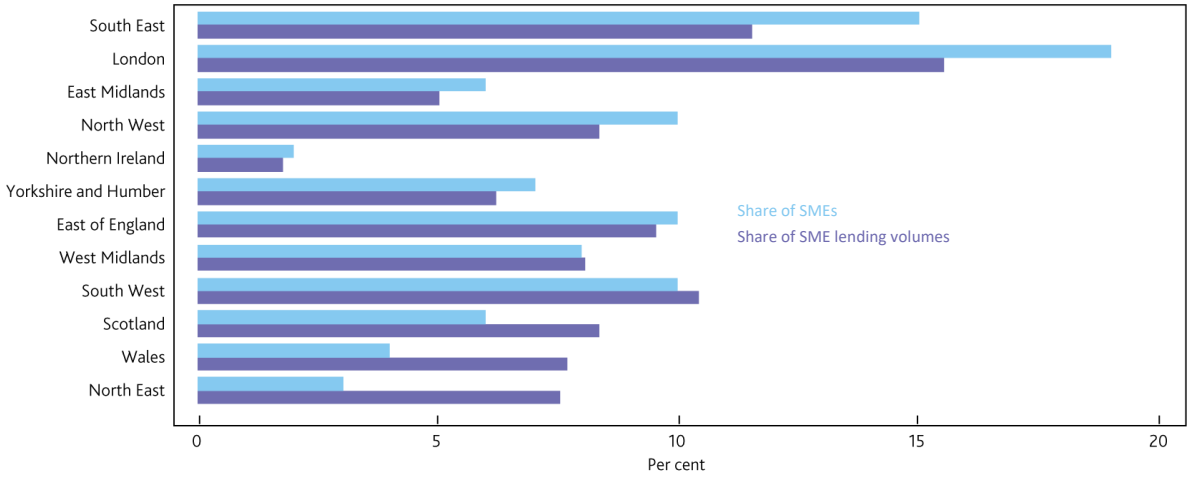


Sources: BEIS, Business population (2018)

The demand for finance tends to vary by firm size, growth and maturity. But there also appears to be some regional variation in the supply of finance. For example, the data suggests that SMEs in London, South East, North West, Yorkshire and Humber, and East Midlands are less likely to receive a loan than the rest of the country **(Chart 3**). In London, equity finance appears to make up the difference, but this concentration of equity finance and angel investors suggests a lack of diversity in financing options elsewhere **(Chart 4)**.

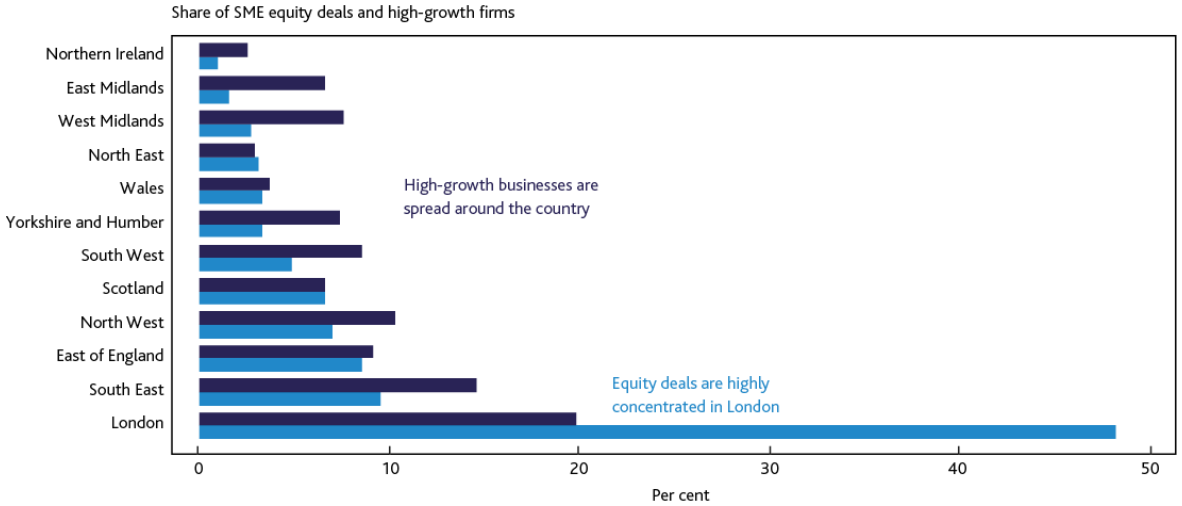
[7] *Business population estimates 2019*, BEIS.
[8] *Federation of Small Businesses* and *European Commission SBA Fact Sheet 2018*.
[9] *Small Business Finance report 2019*, British Business Bank.

Chart 3 Some regions receive fewer SME loans



Source: UK Finance, SME Update Q2 2018; BEIS, Business Population Estimates 2018

Chart 4 The availability of equity finance is highly concentrated in London

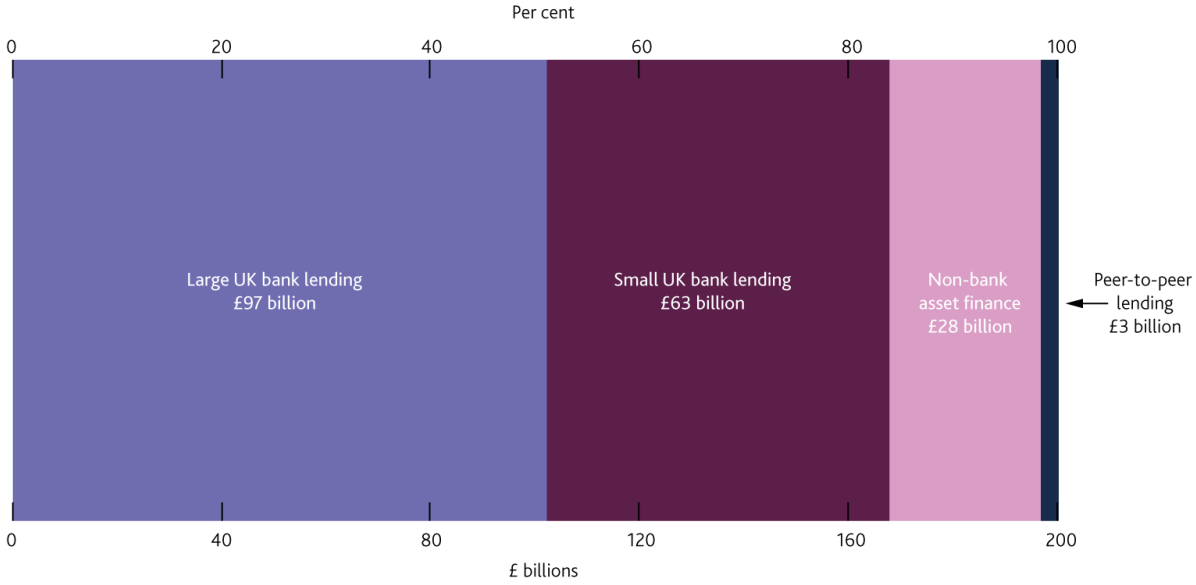


Source: British Business Bank analysis of Beauhurst data and ONS

In aggregate, bank lending makes up 85% of the stock of outstanding debt for SMEs **(Figure 2)**. When SMEs do seek loans, the majority consider only one bank – usually their current account provider. And the chances of being rejected are over 50% higher when applying to a new provider.[10] This helps to explain why the majority of the lending to date has been provided by larger banks. But as experienced in the 2008 financial crisis, this reliance on existing bank relationships and an inability to shop around creates a risk to the supply of credit during a downturn. A lack of diversity amongst lenders can further amplify the business cycle if traditional lenders behave in similar ways.

[10] BVA BDRC, *SME Finance Monitor 2018 Q4.*

Figure 2 Bank lending makes up 85% of outstanding debt for SMEs

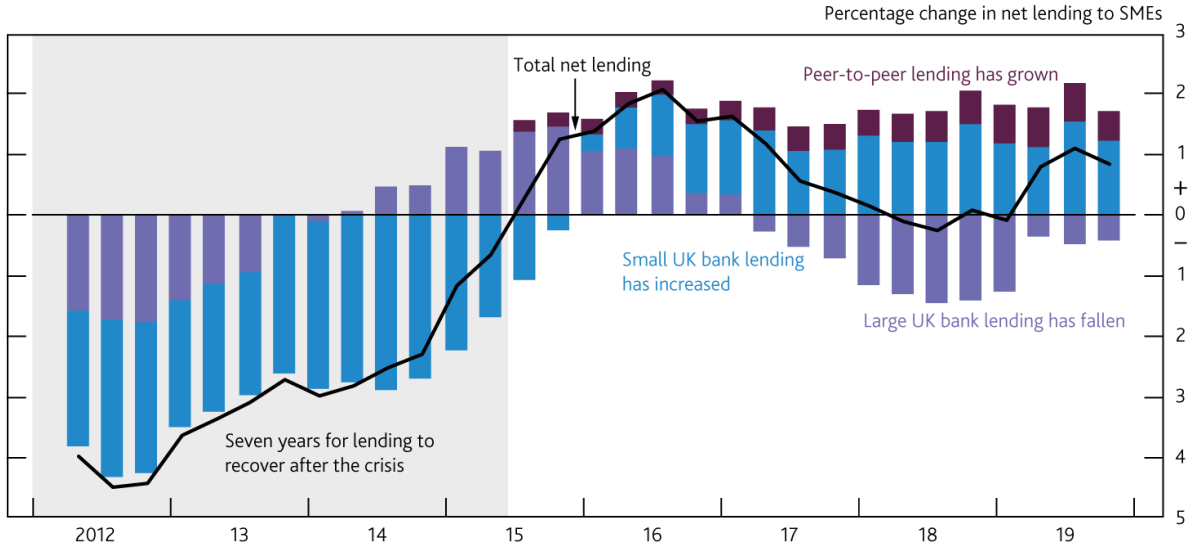


Sources: Bank of England, ONS, Peer-to-Peer Finance Association and Bank calculations

The flow of lending tells a different story. It took seven years for net bank lending to SMEs to recover from the shock of the financial crisis **(Chart 5)**. Research has found that firms borrowing from weaker banks struggled to access credit and invest during the crisis. This is consistent with the fact that in past downturns, the supply of bank credit to SMEs has tended to tighten faster than credit to larger companies. During the financial crisis, SMEs also faced higher interest rates, shortened maturities and increased requests for collateral relative to larger businesses.[11]

Since 2017, however, all of the net growth in SME lending has come from smaller banks or from alternative sources such as peer-to-peer (P2P) lending **(Chart 5)**. A diversity of lenders with different business models is important to ensure SME lending is resilient to a downturn or financial sector shock in future.

Chart 5 It took seven years for lending to SMEs to recover from the financial crisis



Source: Bank of England, Peer-to-Peer Finance Association and Bank calculations.

[11] OECD, *Financing SMEs and entrepreneurs 2012.*

2.4. The economics of the SME lending market

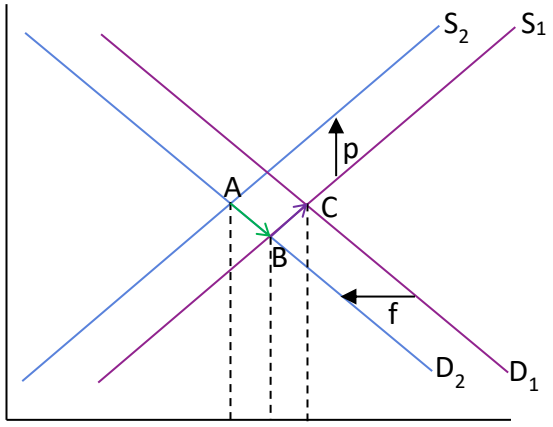
Making information easier to share could boost both the supply of, and demand for, credit, increasing SME lending without increasing risks in the system.

Many small businesses struggle to access the finance they need. Survey evidence suggests that only 36% of SMEs make use of external finance. More than 50% of SMEs consider only one provider when seeking a loan and 25% of SMEs are put off from shopping around by the hassle or time taken. This results in six in ten of those who would like to borrow resorting to personal funds instead. And 70% of SMEs would rather grow more slowly than borrow.[12] The evidence suggests there is a market failure, because of two information asymmetries.

The first information asymmetry: lender vs borrower

The first information asymmetry exists because the borrower knows more about their business prospects than a potential lender, making the loan a risky proposition. This is true for any loan and explains why a lender requires information on the business to understand the business model and assess the risk before extending a loan. But the information asymmetry is particularly acute in SME lending, where business models are very heterogeneous and often unproven – especially if they are start-ups or innovators. Additionally, small firms are often young and don't have a long credit history; and there is a higher rate of failure. For all these reasons, SME lending is a particularly risky business, and lenders demand a larger premium to compensate for these risks. Relative to an efficient market equilibrium, this constrains the supply of credit from S_1 to S_2 in **Figure 3**. In this kind of market, information is extremely valuable.

Figure 3 Supply and Demand in the SME lending market



The second information asymmetry: incumbent vs competitor

The second information asymmetry arises because the existing bank account provider for the SME can better observe cash flows, balances and existing loan performance. It therefore has an informational advantage over other potential lenders. In order to compare prices from any other lenders, the SME needs to share this and other information to demonstrate that they are creditworthy. But this is often a very manual and paper-heavy process, which varies considerably between lenders. Important regulation, such as Anti-Money Laundering

[12] CMA *Retail Banking Market Investigation 2016* and *BDRC SME Finance Monitor Q4 2018*.

(AML), and the associated Know Your Customer/Business (KYC/KYB) processes, impose additional requirements. That all contributes to a lengthy on-boarding process, which can take up to six weeks just to get a quote. Most small businesses need access to finance on a much shorter timeline, especially those that are young and fast-growing. The busy owners of small businesses are put off by the long and cumbersome on-boarding process and cannot afford the time to shop around. Many choose not to borrow at all. Relative to the efficient market equilibrium, these frictions constrain the demand for credit from D_1 to D_2 in **Figure 3** and reduce the allocative efficiency of the market.[13] Making information easier to share in this market could address a considerable deadweight loss.

Relative to the efficient market equilibrium *C*, the risk premium *p* caused by the first information asymmetry constrains the supply of credit to S_2. Additionally, the hassle and time taken to apply reduces the demand for credit by *f* to D_2.

Giving lenders better information on borrowers should improve credit decisions and reduce the probability of default. It reduces the risk premium *p*, increasing the supply of credit (in part through the entry of new lenders) at any given price, moving us along the demand curve towards point *B*. The price of credit is lower for everyone, and some previously under-served borrowers can now access the finance they need.

Making it easier for SMEs to apply for loans reduces the friction *f* and increases the demand for loans at any given price. This moves us along the new supply curve S_1 towards point *C*, bringing in previously excluded borrowers into the market. The marginal borrower is charged a higher price, reflecting the additional risk, but because of the supply-side reform, this might still be below its previous level at *A*. Although this is unlikely to eliminate all efficiencies and reach point *C*, it has the potential to increase the flow of responsible lending to SMEs without taking unnecessary risks that would make the system more vulnerable in a downturn.

2.5. Recent and forthcoming initiatives to support SME finance

Most policy interventions have focused on the supply of SME lending, rather than demand

Her Majesty's Treasury (HMT) have launched significant supply-side initiatives over the past decade to support SME lending, including the Commercial Credit Data Sharing Scheme (2015) and the Bank Referral Scheme (2016). But surveys by the Competition and Markets Authority (CMA) and the Business Development Research Consultants (BDRC) suggest that SMEs are still tied to the provider of their business current account. This is in part because these initiatives do not fully address the barriers to shopping around, nor do they tackle the entrenched advantages enjoyed by existing providers.[14]

More recent initiatives have started to address the demand side frictions by enabling data portability. Open Banking is changing how the UK financial system uses data. It allows data to move securely around the financial system in a standardised way through secure Application Programming Interfaces (APIs).[15] This enables SMEs to share the transaction data in their bank accounts, which should reduce the informational advantage of the bank account provider and make it easier for non-bank lenders to compete with banks.

---

[13] Because this process has relatively high fixed costs, it is less of an issue for larger corporates, where the value of the loan makes it worthwhile.

[14] CMA *Retail Banking Market Investigation 2016* and *BDRC SME Finance Monitor Q4 2018*.

[15] Open Banking Implementation Entity.

Following the successful implementation of Open Banking, the Department for Business, Energy and Industrial Strategy (BEIS) Smart Data Review explained that it would seek to follow up with other initiatives, which would link together to enable a smarter data economy.[16] The next stage of the Review is exploring how best to enable data portability in the telecommunications and energy sectors. And the FCA's Open Finance initiative is exploring how best to enable data portability in the financial sector, focused around savings, insurance, mortgages, investments, pensions and consumer credit.[17]

While these are positive steps towards creating a digital economy, they do not yet address the long, manual and paper-heavy on-boarding process that presents a friction to shopping around for finance for most SMEs. And they do not yet address the challenge of the thin credit files of young and successful SMEs seeking finance to support their growth.

2.6. A proposal for an Open Data Platform

Permissioned data sharing standards could deliver an Open Data Platform and a "portable credit file" that makes it easier for SMEs to apply for credit and improves transparency for lenders.

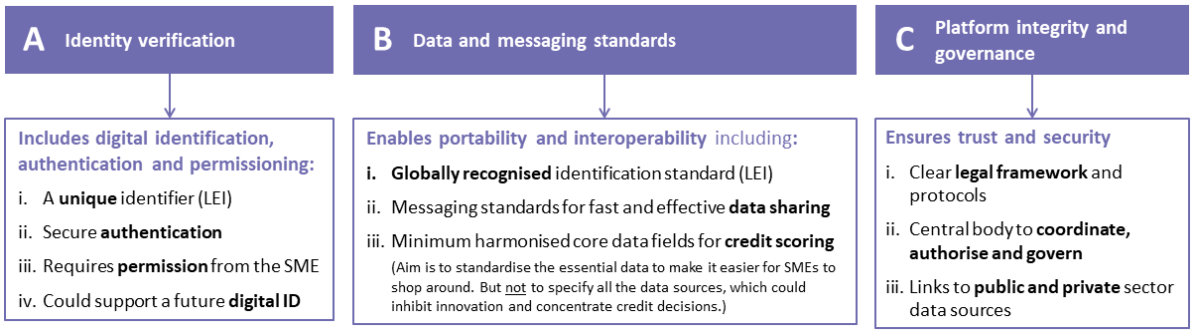
Open Banking has successfully demonstrated that with the right permissions, sensitive financial data can be shared securely with third-party providers using APIs. At the same time, fintechs have demonstrated their ability to use real-time data from online market places, for example, to expand the information set and make better and more inclusive short-term lending decisions.

Recognising the potential that a connected, "smart" data economy could have, the Bank explored what it could mean for SMEs in the financial system of the future. If the same, permissioned data sharing standards were rolled out across the economy on an Open Data Platform, small businesses would be able to harness the power of their data to access the finance they need to grow. With the touch of a button, an SME could permission the movement of their data from multiple places, to a potential new lender, creating a virtual and portable credit file.[18]

The Open Data Platform has three essential building blocks **(Figure 4)**:

A. **Identity verification,** including digital identification, authentication and permissioning
B. **Data and messaging standards,** enabling portability and interoperability
C. **Platform integrity and governance**, ensuring trust and security

Figure 4 Building blocks of the Open Data Platform



[16] *Smart Data: Putting consumers in control of their data and enabling innovation.*
[17] *FCA Call for Input: Open Finance.*
[18] *Openness and integration – the new finance and new economy in a global context*, speech by Dave Ramsden.

A. Identity verification, including digital identification, authentication and permissioning

The ability to identify a business quickly, easily and digitally enables a more seamless user experience as they move around the financial system. The Legal Entity Identifier (LEI) is likely to play an important role: as a 20-digit alphanumeric code, it can offer a unique identifier to every one of the 6 million SMEs in the UK, and as a globally recognised standard, it is built to support cross-border identification for trade finance.[19]

Once the entity is identified, it can be digitally authenticated in order to validate instructions, like a digital signature. That authentication could be delegated to a person's mobile device, for example, to enable one-touch permissioning.

B. Data and messaging standards, enabling portability and interoperability across different providers

Standardising the format of core data fields makes it easier to interpret the data held by different institutions in different systems. And standardising the messaging protocol through APIs makes it easier to request and receive the desired data quickly and effectively. Together, these help make the existing, separate systems interoperable, enabling businesses to pull their data together from many different institutions with a single application.

C. Governance and integrity of the platform

In order to maintain trust and security, there must be a robust process to authorise participants on the platform and world-class encryption to protect against cyber-threats. The platform would also require a clear legal framework to set and maintain a dispute resolution mechanism.

An Open Data Platform that gave businesses the ability to compile their data instantly, from public and private sources, in a safe and permissioned manner, would unlock a truly smart data economy. And because it would rely on moving data between the owners, rather than replicating it or storing it in all in a single location, it has the potential to be secure, trusted and cost-effective.

In this way, the proposal is a targeted application of the BEIS Smart Data and FCA Open Finance initiatives applied to the specific frictions in SME finance. It is a natural extension of Open Banking and Her Majesty's Revenue and Customs' (HMRC) Making Tax Digital; and fully aligned with GDPR, as well as the conclusions of Professor Furman's Digital Competition Expert Panel Report on how to extract value from data, promote competition and give consumers control of their data.[20,21] It goes further by proposing a standardised approach for all sectors in the economy and by including both public and private data sources to enhance the information set a lender can access on a prospective borrower.

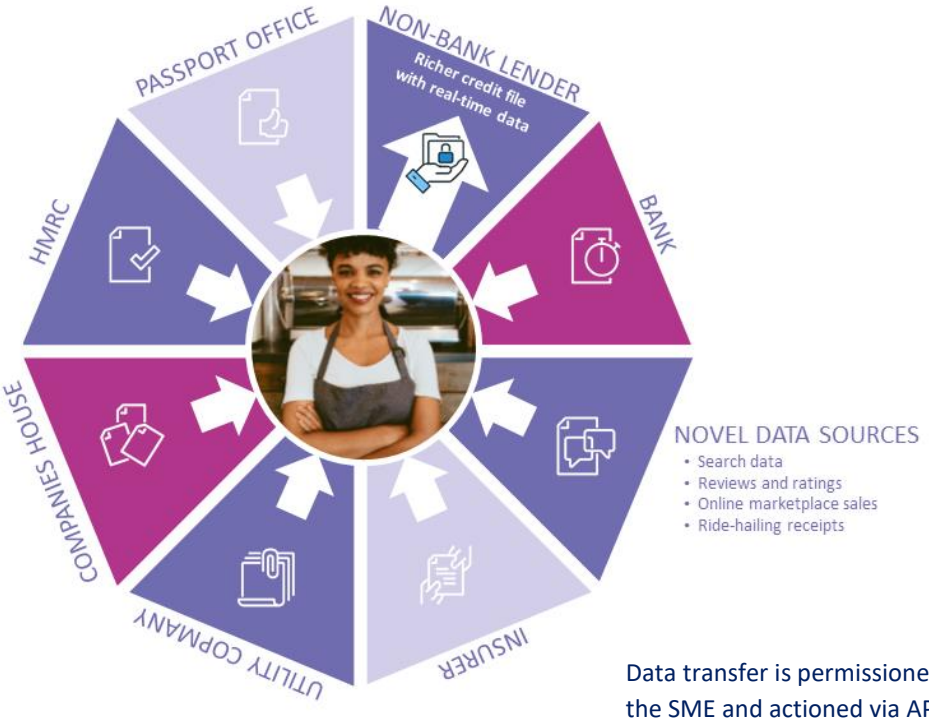
2.7. What the Open Data Platform would look like in practice

The Open Data Platform would, in practice, be a decentralised network of data providers, using a standardised set of APIs to move data around the financial system instantly, at the request of the SME **(Figure 5)**. No data would move without the permission of the SME, there would be no central data repository or physical credit file, and there would be no central infrastructure to build. Like the internet, the protocols and standards would enable interoperability and provide a platform for firms to innovate upon.

---

[19] *Setting standards*, remarks at the ISO20022 Conference by Dave Ramsden.
[20] *HMRC Making Tax Digital*.
[21] Report of the Digital Competition Expert Panel, *Unlocking Digital Competition*, March 2019.

Figure 5 A stylised diagram of the Open Data Platform applied to the SME finance use-case



At the touch of a button, the SME would permission an API call to a handful of data providers with whom it already has a relationship (such as its bank, its utility company and its insurance company) to instantly share specified data fields with a third-party (such as a non-bank business lender). The data transfer would be encrypted end-to-end and would provide access for a specified (minimal) period of time. If the third party needs access again, they can request it easily and the SME can authorise the request effortlessly with their fingerprint, for example, or a glance at their smartphone.

Expanding the sources of data that lenders could access, such as data held at insurance and utilities companies, as well as search, ratings and social media data could help to build richer credit files. Linking public sources such as the Passport Office, Driver and Vehicle Licensing Agency, HMRC and Companies House could improve the underwriting process for a loan by reducing the inefficiencies involved in identity verification. Opening access to all this data using common messaging and data standards could eliminate a significant barrier to entry and open up the market to greater competition.

Moving data around using a system of APIs like this would also reduce the cost of AML checks. Banks say the burden of compliance is one of their biggest costs, so an efficiency saving like this would give incumbent lenders a clear and immediate incentive to take part and help make it a success.

Shortening the on-boarding process and allowing customers to share their credit files with different providers should enhance choice and competition in the market.

Crucially, this model would also allow innovative firms to use new data for credit risk assessment. Today's cutting-edge fintechs are using real-time payments and transaction data to enhance their credit-scoring. Lenders in future might be able to use online search and ratings data, or real-time shipment and satellite imagery data and envision many other ways to build a richer and truer picture of the borrower's ability to repay.

The same platform also has the potential to deliver a "personal financial passport" for individuals. By enabling individuals to pull together their data from different sources, it would empower consumers to harness the full

value of their data. Adoption would put into practice the recommendations from the Digital Competition Expert Panel Report. This data mobility would allow consumers to move their personal information from one platform to another, to avoid lock-in and open the door to new services.

The Bank can leverage its role at the heart of the UK financial system to support change. It strongly supports the principles of 'Open Finance' and can draw on experience in promoting data standards to help catalyse an open platform to boost access to finance for small businesses and enhance choice for households. Success will require a joint effort from both the public and private sector, including the Bank's continued support.

3. Policy issues and design considerations

The previous chapter explained how permissioned data portability could support SME finance. This chapter discusses the wider potential benefits for the Government's and the Bank of England's objectives, including economic policy, innovation, inclusion, financial stability and competition. It also considers a number of other issues, including privacy, cyber-security and governance, and how they might be addressed in the design of the platform.

3.1. Policy issues

Open data for SME finance could support the wider objectives of the Government and the Bank of England

Government Economic Policy

The Government's economic objectives focus on boosting growth and employment. There is also an added emphasis on opportunities to boost growth and "level up" the UK economy by focusing efforts outside of London and the South East. The Government is also keen to demonstrate the UK's leadership on the global stage and ability to attract investment and trade from beyond the EU. That includes leveraging the UK's role as a global financial centre as well as a global centre for fintech innovation.

Chapter 2.3 highlighted the regional differences in SME finance and, in particular, the lack of equity finance available to fast-growing SMEs outside of London and the South East. By boosting access to debt finance for SMEs across the UK, the Open Data Platform should go some way towards closing the gap between London and the rest of the UK. And by supporting an increase in responsible lending to young and fast-growing SMEs, it should contribute to increased productivity and growth, particularly outside of London.

Open Banking has established the UK as a world leader in enabling permissioned data portability in the banking sector and a number of countries around the world have been watching developments closely. By taking that principle further and delivering a decentralised system of permissioned data portability in an advanced economy, the Open Data Platform would further reinforce the UK's position as a global leader.

The Open Data Platform would serve as a platform for innovation. By formalising a set of standards that become widely used, it might offer a high return on investment, attracting innovative start-ups to develop new use cases. It will help to enhance the UK's reputation as a global centre for fintech innovation and thereby enhance the UK's ability to attract the best talent from around the world.

Inclusion

Survey evidence suggests that a large number of SMEs are financially excluded in some form or other. In particular, 25% of SMEs are put off from shopping around for a loan because of the hassle or time taken. This means 6 out of 10 would-be-borrowers choose to resort to personal funds instead. Meanwhile, 70% of SMEs state that they would rather grow more slowly than borrow. These statistics suggest that the SME lending market is failing to meet the needs of some businesses. And the problem may be even more pronounced at

the smallest end of the scale, where young and small firms also face a higher probability of being declined loans, most likely because of thin credit histories.[22]

This problem appears to be getting worse, as an increasingly large number of SMEs are reliant on the value of intangible rather than tangible assets. The shift towards online business means there is less need for commercial property – even large companies now share office space flexibly – meaning businesses have less collateral to offer a prospective lender. Additionally, as the value of a business is more closely tied to the customer base and the network they have built, it can be harder to value. Businesses can reach scale faster because they are less constrained by geography and word of mouth travels faster and further than ever before.

All of these things mean that it can be harder to determine the creditworthiness of a young, asset-light and fast-growing company using traditional methods. But additional data can help, especially to determine the value of intangible assets. For example, the ability to track the frequency with which customers return to a website can help measure brand affinity and therefore value of the customer base. Being able to track the customer ratings of a business in real-time can provide greater transparency to a lender and might enable smaller and shorter duration loans as a business builds up its reputation and credit history.

In this way, an Open Data Platform can help young or fast-growing businesses, those with thin credit files, or those reliant on intangible assets to access finance and thereby support greater financial inclusion. These types of businesses are often serviced by equity finance, angel investors or venture capital. But the lack of such options outside of London (Chart 4, Chapter 2.4) may be limiting the growth of these businesses. By making more data available to bank and non-bank lenders, the Open Data Platform could help fill a gap in the market and support lending to businesses outside of London and help level up the UK economy.

Financial stability and competition

The Bank of England has an objective to protect and enhance the stability of the UK financial system. It defines financial stability as the consistent supply of the three vital services that the real economy demands from the financial system: the mechanism for paying for goods and services; intermediating between borrowers and savers; and insuring and dispersing risk. One of the key features of the 2008 financial crisis in the UK was a marked decline in the availability of credit, with SMEs facing tighter credit conditions than larger firms.[23, 24] In particular, as illustrated in Chart 5 (Chapter 2.4), the UK banking sector largely pulled out of lending to SMEs. In other words, in the immediate wake of the crisis, the financial system failed to intermediate effectively between savers and borrowers.

One of the reasons for that was that the provision of finance to SMEs was highly concentrated among a small number of banks, with very similar business models. UK banks are much better capitalised now than they were in 2008. But financial systems that lack diversity have been shown to be less resilient to shocks. For example, during the financial crisis the US financial system was able to continue serving the real economy, even as its banks cut lending to repair their balance sheets. Because it had much deeper capital markets, non-bank finance was able to step in when banks pulled away.[25]

The Open Data Platform is designed to address one of the key barriers to entry in the SME lending market. And in doing so, should open up the market to greater competition from new banks and non-bank lenders. The SME lending market is heterogeneous and there is a considerable spectrum of risk profiles. To serve the full spectrum will almost certainly require a range of different providers with different business models and

---

[22] CMA *Retail Banking Market Investigation 2016* and *BDRC SME Finance Monitor Q4 2018*.
[23] *The Banks that said No: Banking Relationships, Credit Supply and Productivity in the United Kingdom*, Franklin, Rostom and Thwaites (2015).
[24] OECD, *Financing SMEs and entrepreneurs 2012.*
[25] Bank of England FS Paper No. 33, *A European Capital Markets Union: implications for growth and stability*, February 2015.

different risk appetites. Support for a diversity of lending models will help reduce the likelihood of a shock hampering the market for SME lending.

Through the Prudential Regulation Authority (PRA), and in support of its financial stability objective, the Bank of England has an objective to promote the safety and soundness of the firms it regulates. As part of its supervision of banks, building societies and credit unions, the PRA monitors the risks that firms are exposed to, including through their loan books. Because the Open Data Platform proposal is designed to enhance the information available to lenders, it should support responsible lending. And by enhancing risk models, it should support increased lending volumes without reducing the quality of the loan book, as described in Chapter 2.4.

The PRA also has a secondary objective to facilitate effective competition, where possible. Lowering the barriers to entry and levelling the playing field for non-traditional or non-bank lenders will help ensure traditional lenders price competitively and innovate to improve the services they can offer their customers.

3.2. Design considerations

There are also a number of issues raised by the Open Data Platform that can be addressed in its design

Privacy

In June 2019, the Digital Competition Expert Panel published a report on how to extract value from data, promote competition and give consumers control of their information. It emphasised the importance of data portability to empower consumers and giving users control to ensure trust. The proposed system of APIs in the Open Data Platform would be fully aligned with these principles.

SMEs vary in complexity and in size. At the smallest end of the scale, micro-SMEs and sole traders behave more like individuals. So a widespread system of data portability must meet the standards expected by consumers and must be built on trust. This section discusses the policy requirements to build that trust.

Consumers increasingly want to make use of their data. They want systems to be connected, when it makes their lives easier and delivers value to them. But they are nervous about data on them being used or shared between third parties without their knowledge. And they are nervous about any one entity (public or private) having too much information on them.

The General Data Protection Regulation (GDPR) gives individuals certain rights over their data and is aimed at giving them greater control and trust in the use of their data. Importantly, it gives them the right to know how their data is being used (transparency) and the right to "receive their data in a structured, commonly used and readable format" (portability).[26]

The following features will be important to consider as part of the design:

- **Permissioned:** individuals should have complete control of their data. Every movement of data must be permissioned by the individual. And an individual should easily be able to review the permissions they have provided and revoke them at any time.
- **Transparent:** the Open Data Platform must be transparent. Every permission, data request and movement should be visible to the individual and summarised in an easy-to-read dashboard.
- **Time-limited:** access to data should be for a limited period of time. Every data request should make clear how long the data is needed for. Any data request should be for a minimum feasible time period, on the understanding that access may be requested at regular intervals.

[26] *GDPR Article 12* and *GDPR Article 20*.

- **Specific use:** access to data should be for a specific use. Every data request should make clear what the data is being used for.

Cyber-security

Achieving the highest standards of cyber-security in the financial system is crucial for operational resilience and consumer trust. This is especially true as data becomes increasingly easy to access remotely. If successful, the proposed Open Data Platform might reach a scale that makes it systemically important, so the design must address cyber-security head on. The following features will be important to consider as part of the design:

- **No central repository:** At a national scale, creating a central repository of sensitive personal and financial data would present a significant target for cyber-crime. A system of APIs to move data between the different participants around the system would therefore have design advantages.
- **Minimal data storage:** Data providers around the financial system have a responsibility to safeguard appropriately the data they hold on individuals and businesses. A principle of minimal data storage should minimise the risk of data breaches, by avoiding replication of sensitive data around the system, and by avoiding single points of failure in large data aggregators. Consistent with that principle, data that moves via APIs should be used and then deleted as soon as the permission expires.
- **End-to-end encryption:** The standardised APIs will themselves create a point of failure and will require the highest levels of cyber-security. As part of that, data moving around the system should be encrypted from end-to-end, using public key infrastructure. This will minimise the risk of data packets being intercepted mid-transfer or missing their intended recipient.

Governance

The final layer to build trust in the system will be appropriate governance arrangements. This will give individuals assurance that participants in the system adhere to the relevant privacy and cyber-security standards and confidence in the ability to resolve any issues that might arise. The following features will be important to consider as part of the design:

- **Authorisation:** A system that opens up sensitive financial data left open and unregulated would risk being misused. Individuals would expect participants in the Open Data Platform to be vetted and authorised to ensure they meet the highest standards of data privacy and cyber-security.
- **Oversight:** Individuals would expect a degree of oversight and expect appropriate sanctions to ensure authorised participants adhere to the rules.
- **Liability model:** There needs to be clear responsibility for loss of data. The non-storage approach should reduce the risks, but participants should not be dis-incentivised from sharing data for fear of being penalised.

4. Engagement with industry and authorities

The publication of the Future of Finance Report in June 2019 provided a helpful milestone for further engagement with and opportunities to learn from relevant stakeholders. In the nine months since publication, the Bank of England has discussed the Open Data Platform with other central banks, think tanks, public authorities and a wide range of private institutions, including: bank and non-bank lenders, data providers, credit reference agencies, fintechs, larger technology companies, accounting software providers and insurers. This chapter summarises the key messages from those discussions.

4.1. The benefits of data portability

Firms in the private sector were universally positive about permissioned data portability. Interestingly, they all believed they had something to gain from a fully-connected system. The fintechs saw an opportunity to get access to more data. The incumbent banks recognised the cost-savings they could make by streamlining their highly manual and paper-heavy AML compliance processes, which they regard as one of their biggest costs. Many others felt that giving households and businesses greater control of their data was an inevitable consequence of GDPR.

4.2. The need for the right technology and standards

A number of stakeholders said that these movements of data already take place, to varying degrees. For example, there is already an API to access the Passport Office, DVLA and Companies House. And some fintechs have gained a competitive advantage relative to incumbent banks, by using these APIs to speed up the on-boarding process. Some told us that they are now able to on-board, approve and provide loans to SMEs in a matter of days, and sometimes even minutes. But the quality and nature of these APIs varies considerably, so fintechs face a high fixed cost every time they want to connect to a new data provider. That investment can be prohibitively expensive to repeat, so there was widespread agreement on the importance of standards: a uniform approach to writing those APIs and the guidelines that accompany them would deliver efficiency gains. As one fintech described it, “standards like those in Open Banking tip the scales just enough to make innovation worthwhile”.

4.3. The case for additional data

When asked what additional data would be most valuable, lenders (perhaps unsurprisingly) prioritised access to government-verified data, including passport and tax data, such as tax returns, with the permission of the SME. This was seen to reduce significantly the likelihood of falsified applications, simultaneously reducing fraud and credit risk. Lenders also highlighted the importance of information on company directors, particularly at the smaller end of the scale, where the financial performance of the business is highly correlated with the behaviour of its directors. And in light of the increasingly capital-light business models they see, some lenders also spoke of the increasing value of any data that could help value intangible assets, including brand affinity on social media, and even footfall using satellite imagery. One non-bank lender made a strong case for two-tiered access to data at Companies House, so that authorised participants (including lenders) could access key data on company directors, including date of birth and address; while keeping those fields hidden from the public register.

4.4. Views of public authorities

The public authorities, especially HMT, BEIS and FCA, noted that much of this work was already in train, but acknowledged that it was happening sector by sector. The authorities agreed on the importance of sectoral initiatives being coordinated and modular. If all the open data initiatives use the same messaging, security and privacy standards, they could be combined over time in a modular fashion to build a complete system of data portability.

Our discussions also highlighted other ways to simplify our proposal. For example, HMRC's Making Tax Digital Initiative will soon require SMEs to submit their accounts via accounting software packages using HMRC's new API.[27] Given the role they are starting to play, accounting software providers could serve as the gateway to that data, without any change at HMRC. This might avoid the need for legislation and could save a considerable amount of time and money.

4.5. Plans for implementation

Despite the support for the concept, many stakeholders were sceptical about implementation. Some were nervous about crowding out private innovation and emphasised the value of providing the core standards at the centre, but allowing others to innovate upon that platform. Others highlighted the importance of using the standards that already exist, from Open Banking and beyond, to make the platform easy to integrate with and maximise adoption. Some lenders also warned from their experience that that the user-experience would need to be seamless to engage with time-constrained business owners. They would be unlikely to engage until they need access to finance, particularly those with relatively less technological and financial expertise, so it would require minimal effort on SMEs' part.

4.6. Summary

The consensus seemed to be that the Open Data Platform proposal was achievable, subject to agreeing a universal set of standards and standardising some of the data fields. And the fact that some of these data flows were already taking place showed that it was both valuable and technically feasible.

[27] *HMRC Making Tax Digital*.

5. Lessons from around the world

This section summarises the most relevant examples of data portability from around the world and the lessons for the UK.

5.1. China

What has China done?

China has successfully utilised data and technology to widen access to finance for SMEs. Through their platforms, SMEs can access loans immediately, using real-time data from within the platform and beyond. The ecosystem gathers data from hundreds of millions of real-name registered users and millions of small businesses, which buy and sell on online marketplaces. This alternative approach to traditional credit scores can improve access to finance for those who have traditionally had limited credit history.[28]

What is unique about this approach?

The ecosystem in China includes information on both social aspects, similar to a social media platform, and credit aspects, similar to a conventional bank on its platform. It adds payments history and links with public agencies, financial institutions, and merchants to obtain more alternative data that can more accurately reflect consumers' creditworthiness. A holistic credit score is built based on users' personal characteristics, fulfilment capacity behaviour and preferences, and even interpersonal relationships. Comprehensive use of such data may not yet be acceptable elsewhere.

What can we learn from it?

The China model benefits from its scale and access to data. To replicate this system in the UK would be difficult because of the already established networks, the lack of a nationally recognised identification scheme, and the fact that data is safeguarded. But it demonstrates the value of bringing together digital identity verification, data and messaging standards, and a platform ecosystem.

The use of LEIs could replicate the benefits of a digital identity by enabling fast, accurate and unique identification of businesses, both domestically and globally. China benefits from the scale and reach of its platforms, built on the same standards. In the UK, the use of data and messaging standards should similarly enable portability of data and interoperability across the economy. China's platforms use access to government data to support credit scoring. Although the approach would need to be different in the UK, it demonstrates the benefit of providing access to government data, with the right permissions, security and governance.

---

[28] *Does China's bet on big data for credit scoring work?* Financial Times December 20, 2018.

5.2. India

What has India done?

India has pioneered the provision of financial and social services digitally through the 'India Stack', a series of layered applications, covering biometric identification, the Unified Payments Infrastructure (UPI) and data portability.[29] The India stack is designed to create a digital single market and foster widespread data sharing.

What is unique about this approach?

The India Stack provides a range of services, including the foundational Aadhaar system of digital ID. Aadhaar is a unique biometric ID given to each individual. More than 99% of the adult population, amounting to more than 1.2 billion unique users, is enrolled in the programme, launched by the government in 2010.[30] Each Aadhaar account is linked to a verifiable 12-digit number that serves as a unique identifier, facilitating digital,online applications that require identity verification (including payments, buying a phone or opening a bank account).

Additional applications include the 'DigiLocker' – a system of cloud storage which provides each citizen with one gigabyte of storage and currently holds over 3.5 billion (primarily government) documents.[31] It also provides for the ability to provide electronic signature, leveraging the Aadhaar ID.

The predominant financial applications of the India Stack are the UPI and the national financial inclusion programme. UPI is a platform that allows any two entities to execute a payments transaction, over a range of payments rails, and by exchanging only a limited set of information. It uses a set of APIs to execute the authentication, authorisation and value transfer functions of payments.

What can we learn from it?

India's experience highlights that authorities can deliver projects to improve the data ecosystem rapidly and at scale, if they can ensure public and private sector support. The high enrolment in Aadhaar reflects the use of government policy to promote the scheme, particularly the decision to require Aadhaar for access to government welfare schemes and subsidies, as well as strong take-up from the corporate sector, particularly financial institutions.

The India Stack highlights the benefits that come from integrating digital services across a range of functions (eg identity, signature and payment). It also demonstrates the value of ensuring a high-quality underlying digital data ecosystem, as a precursor to building further applications with increasing sophistication. In this respect, there are parallels to the UK, where the positive experience with Open Banking lays the groundwork for more sophisticated applications.

Finally, India's experience showcases the importance of leveraging the technical design of underlying infrastructure as a policy tool. For example, UPI has been designed to work with different technologies and to accommodate different levels of technical sophistication. It can be used in Unstructured Supplementary Service Data (USSD)-based applications (ie non-smart phones) and it can generate Aadhaar-linked QR codes, allowing customers to use their smartphone for Aadhaar-enabled transactions. This provides for a more inclusive system where users of all income levels can benefit from the system.

Similarly, privacy-enhancing measures can be built into an identification system, as design features. For example, when a service provider sends an authentication request to Aadhaar, the purpose of the authentication is not revealed; authorities can only track when someone uses their Aadhaar number, not

[29] *IndiaStack*.
[30] *Aadhaar dashboard*.
[31] *DigiLocker National Statistics*.

where or why. In addition, the system can verify identity using a temporary number linked to Aadhaar. This process of masking the underlying ID number reduces the potential for data brokers to create individual user profiles by collecting and merging user information from disparate databases. This is not a panacea for privacy concerns (Aadhaar has been criticised by privacy advocates) but does highlight the importance of technical design for embedding policy choices.

5.3. Estonia

What has Estonia done?

e-Estonia is the Estonian government's programme to digitalise the provision of state services. A key feature of e-Estonia is the provision of government-issued digital IDs to Estonian citizens, which provide ID holders with digital access to all of Estonia's e-services. Digital IDs are attached to physical ID cards, which have an embedded chip and use public-key encryption to ensure the safety of users.

e-Estonia prevents duplication of data: government systems are not allowed to store the same information in more than one place. This distribution of data is designed to provide improved data protection because there is no single place where all the information about someone is held. In order to support the sharing of data, Estonia operates a secure data-sharing network called the 'X-Road'. This is a distributed data exchange layer, which directs queries between separate computer systems. Each data owner determines what information is available and who has access to it, and this is then shared via the X-Road.

What is unique about this approach?

The e-Estonia system has a penetration rate of close to 99% of the population, because it is tied to Estonia's mandatory national ID scheme.[32] This means that Estonia operates one of the most comprehensive national digital networks in the world, with 99% of public services available online. The only e-services not available are marriage, divorce and real estate transactions.

What can we learn from it?

e-Estonia shows us that it is possible to achieve a wide-spread digitalisation of public services. A study of Estonia's e-government services found that e-services saved users time and made dealing with government more accessible.[33]

Importantly, the X-Road demonstrates how a very thin layer of infrastructure can enable a distributed system to work together effectively. In addition, the X-Road creates a joined-up system, meaning it is easier for a citizen to update their details on all systems simultaneously.

Information about the data stored is both transparent and accessible. Citizens control their underlying data and access to it. There is an open register showing the profile of the information that is held in each government system, what reason it is held for, and who it can be accessed by. This is likely to have helped promote trust in the system within the Estonian population.

5.4. Australia

What has Australia done?

Australia introduced its Consumer Data Right (CDR) into law in August 2019. The CDR mandates that banks and financial institutions make it easy and practical for consumers to share their data with third parties. Banks and financial institutions are required to share product and customer data with customers and, with the consent of the customer, banks are required to share that data with accredited third-parties. The application of the CDR to the banking sector is referred to as Open Banking.

---

[32] *e-Estonia*.

[33] *Impact assessment of the e-government services,* Praxis (2013).

Initially, only Australia's biggest four banks will be required to provide access to financial product and customer data. The reach of the CDR is intended to increase over time, and by July 2020 it is anticipated that the CDR laws will apply across the banking sector. Next, the laws will apply to the energy and telecommunications sectors, before being rolled-out across the economy on a sector-by-sector basis.

What is unique about this approach?

The Open Banking initiative in Australia was delivered as part of the Consumer Rights Law, which has a much wider vision for open data. That vision covers a range of sectors, giving customers access to a much wider variety of data.

In addition, the coverage is wider than in the UK. Smaller institutions in Australia licensed as Authorised Deposit Takers are also required to comply. This is in contrast to the UK, where the CMA order only applied to the nine largest institutions.

What can we learn from it?

Inclusion – the Australian system illustrates that it is possible to include smaller institutions in an Open Banking platform. The expectation is that it will help increase competition by allowing smaller institutions to access larger amounts of data that currently give larger banks a competitive advantage.[34]

Coherent vision - the Australian government has set out a clear timetable for the implementation of the CDR. This increases certainty in the industry, and allows firms to direct investment accordingly.

Clear system of penalties - Penalties of up to AUD$420,000 for individuals (or AUD$2.1 million for businesses) may be imposed for misleading conduct relating to the transfer of CDR data or breaches of the new Privacy Safeguards.[35]

[34] *Australia Enters the Era of Open Banking: Consumer Data Rights Bill of 2019*, Iron Mountain.
[35] *Australian Consumer Data Right law: what you need to know*, Dentons.

6. Technical considerations

This chapter discusses the design choices and standards required to deliver a world-class Open Data Platform to boost access to SME finance.

6.1. Conceptual architecture

Conceptually, the Open Data Platform architecture comprises four components:

- **Data owner** - who has control over setting, maintaining, revoking and reviewing specific permissions on how their data is shared by *data providers* on their behalf and how it is processed by *data processors*.
- **Data providers** - public and private sector data sources. These data providers will be authorised and permissioned to share data when explicitly permitted by the *data owner* to share with an authorised *data processor*.
- **Data processors** - authorised and vetted third parties could interact directly (via their own channels) or indirectly (via a cloud-based accounting platform) with prospective loan applicants. Third parties would be able to request and process data securely, and build a core credit file with additional data from public and private sector *data providers*, based on permissions explicitly set by the *data owner*.
- **Governance** - orchestrates the authorisation and authentication flows as well as possible API endpoint integrations. This may need to be overseen by a public body, which would also be responsible for non-technology aspects such as authorising and vetting third-party participants, implementing standards and guidelines, including around cyber-security, and enforcing a code of conduct.

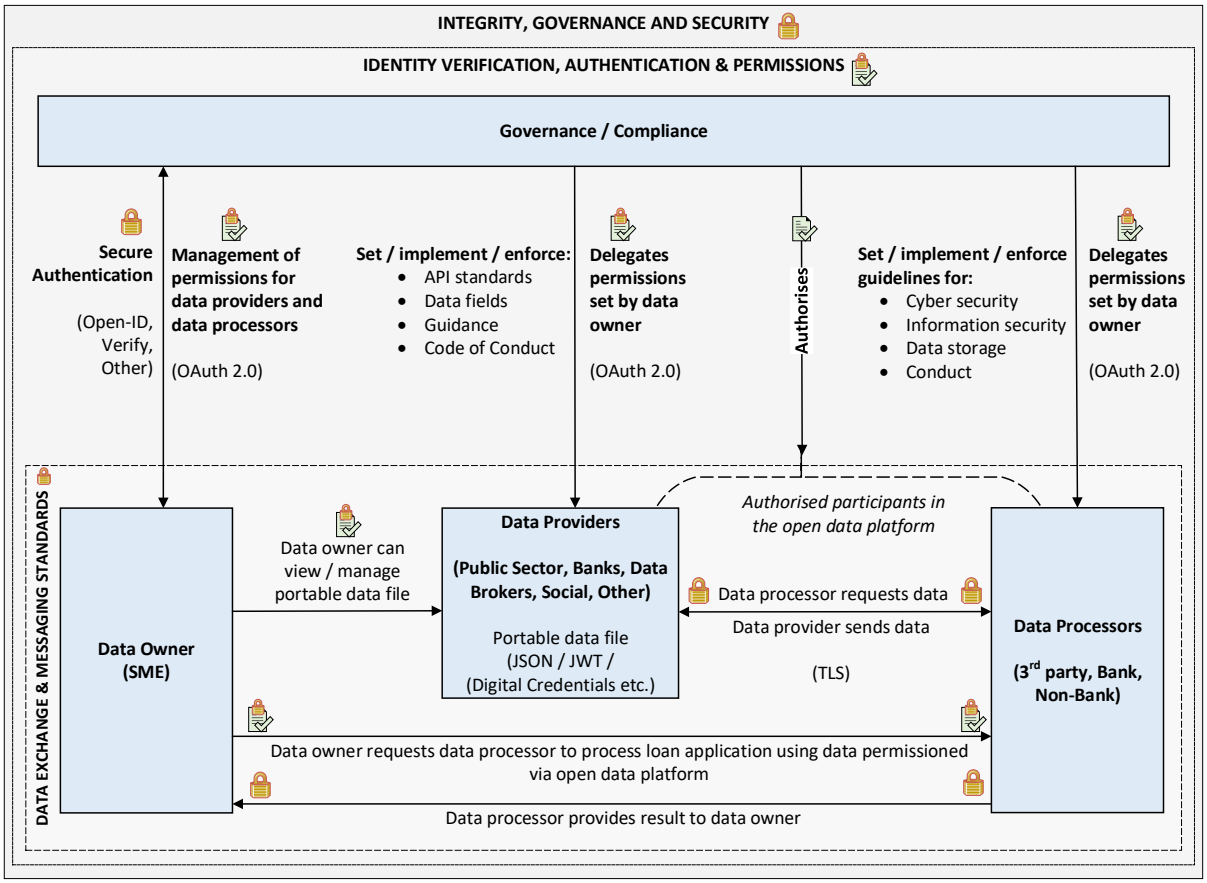
The interaction between these components is set out in **Figure 6** (next page).

6.2. Principles for the architecture and technology

In designing this Open Data Platform, there are a number of principles that guide our proposed architecture and technology:

1. Public-private collaboration – recognise and maximise the relative strengths of the public and private sector. Public authorities can help provide a degree of credibility and set standards for private companies to innovate upon. This should minimise the risk of crowding out innovation by keeping governance and standards to the minimum required to ensure credibility, utility and operational resilience. And it should seek to harness rather than replace the role provided by individual institutions in the system today.
2. Ensure trust, while supporting innovation – the standards that are put in place must be best-in-class to ensure operational and cyber-resilience and they must prioritise the interests of end-users to ensure data protection.
3. Leverage existing technology – to minimise the burden on industry and make use of existing investments in technology infrastructure and standards, where possible. For example, many of the Open Banking API standards could be rolled out more widely, maximising the value of related technology investments by fintechs and banks.

Figure 6 A representation of the components and flows in the Open Data Platform



4. Open and competitive – use best-in-class and open technologies and standards that enable private companies to compete on level terms, like the early standards deployed with the internet, rather than picking proprietary technologies and standards that create winners and losers.

6.3. Design choices

These principles lead to a distributed model, with minimal central governance. This maximises the role of existing nodes in the financial system, while minimising overheads and bureaucracy. It also leads towards a model of minimal data-storage, such that existing data providers maintain responsibility for the data they hold, and data processors do not store multiple copies of data around the system. Such a model enhances cyber-resilience since there is no central data repository and because it minimises the impact of a cyber or data breach at any given node in the financial system.

Similar to Open Banking, the Open Data Platform would involve users sharing their data via APIs with third parties. This section covers some technical requirements to ensure confidence and trust in the platform. In any data exchange, there are three key elements to consider:

A. Identity verification, authentication and permissioning
B. Data exchange and messaging standards, enabling portability and interoperability
C. Integrity, governance and security, ensuring trust

A. Identity verification, authentication and permissioning

The SME needs a way to grant permissions to (public and private sector) data controllers to share their data with third parties. These data controllers need a way to confirm that an SME has granted permission for data to be shared, processed and for what period of time. The data controllers also require assurance and

verification that third parties can be trusted with personal data they are permitted to share. Third parties require confirmation of what they are permitted to use and process, for whom and for how long. Each of these groups require a standardised means to:

- Authenticate that the parties sharing and requesting data *are* who they claim to be;
- Confirm permissions for what can be accessed by whom and for how long.

Both public and private sector data controllers and third parties require a secure and standardised way to request and exchange data for platform users. Both groups are required to protect any data exchanged, processed or stored from loss.

OAuth 2.0
OAuth 2.0 is the leading industry standard and widely used to provide a secure method for verifying digital identities. Further, it provides a formal structure for obtaining, and securely transferring, consumer permissions between entities. OAuth is commonly used for permitting websites to share data with one another.

OAuth 2.0 uses the concept of tokens that can be passed between parties during a transaction for authentication purposes, enabling users to allow third parties to act on their behalf. These tokens could leverage the JSON Web Token (JWT) standard providing an optionally validated and/or encrypted container format that is used to securely transfer information between two parties.

OAuth 2.0 is just a framework and therefore, for financial data use cases, secure implementation of OAuth must be considered by deploying two supporting standards in conjunction.

OpenID Connect
OpenID Connect (OIDC) is a standard built on top of OAuth to provide delegated authentication. OIDC enables a relying party to defer to an identity provider to authenticate users, just as some BigTechs or the Government's Verify system do today. The relying party does not have to be concerned with managing usernames and passwords, instead they trust the identity provider to do that. The identity provider then returns an ID token that the relying party can use to assert a user's identity. It is assumed the identity provider is enabling strong and secure authentication by default.

The OIDC specification defines an element called the claims request parameter, which can be used to request that specific items and their properties, including authorisation, are returned in the ID token. The request parameter also allows users to sign the request, which ensures they can detect if it has been tampered with.

B. Data exchange and messaging standards

Systems and data sources could interface and exchange data via APIs. These APIs could follow the same style and approach taken by Open Banking, leveraging existing APIs for transactions or accounts, for example. Open Banking evolved these APIs iteratively, addressing issues found or introducing necessary features in each new version. The latest version 3.1 of the Open Banking APIs are a much more robust set than those published 18 months ago. Any additional open data initiatives should seek to leverage the gains made there. Core credit data would be comprised of a standardised set of data fields. Specifics of this set of data could be defined by the private sector solely or in collaboration with public sector bodies. Non-core data would not be standardised and instead would be data source specific.

C. Integrity, governance and security

Financial API
The Financial API Specification (FAPI) is a draft standard for configuring financial API security solutions which makes extensive use of OIDC. It defines recommended flows, configuration parameters, and signing and encryption algorithms for implementations of OAuth and OIDC to enhance security and mitigate known risks and attacks. It also adds additional security controls around all data requests and responses.

The FAPI enhances OAuth applications for financial data by providing security even if some attacks on the flows are successful, for example if an attacker manages to phish an access token or intercept requests and responses of a secure message flow. To achieve such protections, the FAPI incorporates several new security mechanisms which aim to increase the security of the protocol. As with any nascent standard, edge cases may reveal areas of improvement when those aims are not met.

All three standards (OAuth 2.0, OIDC and FAPI) are open source and do not therefore favour any proprietary interests. The combination of the three standards should meet the authorisation and authentication needs of the Open Data Platform. But there are additional workflow standards that could further mitigate risks. For example, Open Banking uses a two-stage request mechanism where a payment or account request is first staged before being authorised. This allows a bank to present the information request to the user at the time of consent so they clearly understand what it is they are agreeing to.

JSON Web Token

The purpose of a JSON Web Token (JWT) is to enable the receiving party to trust that the data received was unaltered during transport. It is self-contained, meaning that it can neatly encompass identifying information about a user, what a user can access, an expiration date, a signature for content validation and importantly any other information.

For example, a token can also embed a combination of identifiers such as the Legal Entity Identifier (LEI), Unique Taxpayer Reference (UTR), Companies House Number or VAT number. It could also contain some data elements of a core credit file.

JWT is a designed for lightweight transmission of certain data. It does not encrypt that data, therefore encryption standards should be deployed to secure tokens or data shared with third parties in transit.

Transport Layer Security

Transport Layer Security (TLS) is used to encrypt requests and responses between third parties and banks using certificates. TLS is used in every browser worldwide to provide secure browsing functionality. API endpoints can be secured with TLS. Another alternative could be RSA cryptography which deploys public and private keys. The public key can be shared with everyone, whereas the private key must be kept secret. Both the public and the private keys can encrypt a message, with one key used to encrypt a message and the opposite key used to decrypt it.

6.4. Other governance considerations

An Open Data Platform (like Open Banking) will require regulators, government institutes, security firms and data source providers to evaluate and assess criteria for trusted status. Similarly, to ensure the objectives of such a platform are achieved and accessible to all, enforcement of guidelines for user experience and a code of conduct should also be established.

Participants would be expected to implement strong user authentication, using multi-factor authentication at minimum as well as security controls to protect confidentiality and integrity of user's security credentials.

Any governance body overseeing the platform should strongly support adoption of, and compliance with, strong information security management frameworks such as ISO27001 or the National Institute of Standards and Technology cyber-security framework, including requirements for auditing compliance.

The body could convene industry groups, including participants, to support sharing of threat intelligence, developing standards, supporting engagement and communications as well as a developer community. The network platform must be secured and subject to regular security (and cyber-penetration) testing, to identify any vulnerabilities and mitigating actions.