Your response

Question	Your response
Question 1: Do you agree with our assessment of the challenges that people and SMEs face when engaging with the market, which Open Communications might help to address? Please explain and provide evidence.	Confidential? – N
The Open Banking Implementation Entity (OBIE) is very supportive of Ofcom's proposals for Open Communications. It shares the same objectives as Open Banking, putting customers in control of their data and delivers on GDPR's right to data access and portability. This has the great potential to increase competition, deliver innovation and drive positive outcomes for consumers and SMEs.	

The challenges outlined in the paper are similar to those identified in retail banking. A lack of customer engagement and understanding leads to an inactive and stagnant market, thereby creating a void in competitive behaviour and innovation. The ability to view all accounts in one place plays a key role in supporting financial capability, enabling customers to make better decisions based on a more informed understanding of their own needs.

Open Communications can help customers by making consumption and contract data available through machine readable and open standards-based APIs. With improved price and service quality transparency, customer can access better deals and generate more competition in the market. Customer interests will ultimately be better protected as customer understanding is key to a more active and engaged market.

Open Banking has been an excellent example of a regulatory initiative that allows new commercial activity to evolve on top of standardised, collaborative infrastructure – in our case the interbank payment systems - and act in a complementary way. Open Banking standards enable open access to the underlying infrastructure and provide the basis upon which innovation can flourish. This leads to a greater choice and range of products for end users, from more mainstream services to niche products to serve particular consumer and small business needs. This access enables increased participation from a range of participants; ensures ongoing stability and resilience for its users; encourages greater innovation and competition; enhances adaptability and security; and provides an overlay to the current infrastructure that will benefit customers. Open Communications has the potential to provide the same for the telecoms and pay TV markets.

The success of this regulatory approach can be seen in the growth of Open Banking. The number of users of Open Banking-enabled products now exceeds two million, doubling in just over six months, despite disruption caused by COVID-19. As of September 2020, there were 90 regulated entities with at least one proposition live with customers.

Research sponsored by Nesta Challenges' *Open Up 2020 Challenge* shows a sharp increase in the use of money management apps during the pandemic, of which 45% were 25-34-year-olds. According to the survey of 2,000 UK adults in early July 2020, one in five started using online banking apps during lockdown and 54% now use them regularly. Open Banking innovations have delivered a clear benefit to users at a time when needs have demanded them.

More generally, Open Banking has given consumers and SMEs more power and control over their financial affairs. Users of Open Banking services can now securely share their data with third parties, enabling them to have a single view of their finances, which means easier budgeting and being able to more effectively shop around for the best suited products and services.

Open Communications has the potential to provide customers with the same level of benefits, power and control with their telecoms and pay TV contracts.

Question 2: Is there additional evidence of problems that people and SMEs face when engaging with the market that you would expect Open Communications to help address? Please explain and provide evidence.	Confidential? – N

Over 40 million consumers and small businesses use banking apps – and thereby know how to access and authenticate themselves to their banking providers – but we would expect this figure

to be significantly lower within the communications sector. This means they will be less likely to then be checking on their levels of usage, available deals and switching opportunities.

Implementing a harmonised and standardised authentication process will help with this barrier. Having a common approach, common interface and common protections mean there is a greater opportunity to build familiarity and trust with customers, both of which are crucial to mass adoption and reducing the risk of fraud or poor outcomes. Having a single authentication approach also means users would not have to go through the inconvenience of signing up to new services and then having to remember credentials for each of these new services.

Developing a form of dashboard similar to that used in Open Banking could enable customers to more easily keep track of aspects of their communications contracts like the amount of data being used and being clear on what consents they've given to Third Party Providers (TPPs).

Developing an overarching regulatory framework for sharing in-scope data (and clearly defining what constitutes in-scope data) would significantly help with current gaps in data provision.

Question 3: Do you agree with our view of the benefits for people and businesses that Open Communications could generate?	Confidential? – N

The communications sector has the advantage of a stronger starting point than banking as more customers are already better engaged in comparing and switching services. Access to more and better data could enable third parties to take advantage of this engagement by offering improved and new services.

Open Banking should be seen as a key enabler in delivering Open Communications and generating the benefits Ofcom has identified. By building on its foundations, the implementation costs for industry can be reduced and the likelihood of customer uptake increased. As the first of its kind in the world, Open Banking had to start from scratch and learn lessons along the way on the best approaches to take. We can pass on all these learnings to ensure that the benefits Open Communications is capable of delivering can be realised in the cheapest, quickest and most efficient ways.

The four use cases outlined in the consultation paper – improved product comparison, account aggregation, account management, and managing costs for financially vulnerable customers - fit with Open Banking experience. The key to successfully implementing them and seeing customers actively using the new services and products is getting the frameworks, standards, conformance and performance right, and getting them harmonised. The risk otherwise is that customer experience is patchy and detrimental to trust and the take-up of Open Communications-enabled services.

Additional use cases and benefits will also emerge as the design and implementation of Open Communications progresses that can't even be imagined right now, such is the strength of innovation by a plethora of competing providers. Setting up the legal and technology frameworks will provide the basis upon which innovative, talented companies can develop new customer propositions.

It is not just customers who would benefit from a harmonised Open Communications implementation. It is important to recognise the benefits it would also deliver to data providers,

third parties, and policy makers and regulators. It has the capacity to correct market inefficiencies and a lack of transparency, and also helps to lower barriers to entry for newer service providers, leading to greater competition.

- **Customers** – harmonisation provides a common approach, common interface and common protections. The more commonality, both in terms of data security and user experience that exists between and across sectors, the more opportunity there is to build familiarity and trust, both of which are crucial to mass adoption. Harmonisation also reduces the risk of fraud or poor outcomes.
- **Data providers** – it streamlines implementation thereby reducing risk and cost. A range of vendors and technical service providers (TSPs) now also exist to support data providers.
- **Third parties** – it lowers the barriers to entry thereby promoting competition and innovation.
- **Policy makers and regulators** – it maximises the likelihood of consumer adoption, thereby achieving intended policy outcomes. A single regulatory framework is also easier to supervise.

All this ultimately benefits the customer as the market will become more buoyant with an ever greater choice of providers, services and products becoming available.

Based on our learnings from delivering Open Banking, we believe that the expected benefits of Open Communications can be maximised from the outset by:

- Ensuring harmonisation and minimal implementation burden by adopting best practices observed from Open Banking;
- Working to implement a consistent and convenient user experience; and
- Setting out a regulatory framework with distinct parameters and clarity on expectations and outcomes, all designed based on close engagement with industry.

Customers don't need to know about Open Communications to benefit from the changes it brings as it should just exist behind the scenes as a technology and legal framework. However, we do believe that a customer-facing element such as some form of a "trustmark" could give customers the confidence that they are using properly regulated services and products. The primary aim should be ensuring a simple customer journey; a key lesson from Open Banking during the early part of implementation is that poor customer experience presents a significant barrier for customer adoption.

We note the mention in the consultation document of screen-scraping being used by a small number of account comparison third parties to avoid users 'dropping out' if they are asked to input too much data[1]. Screen-scrapping is not recommended as a process for enabling customers to share their data with third parties due to its inherent security and liability flaws. Implementing financial grade API security – already used in Open Banking – together with strong customer authentication – also already used in Open Banking - would not only be safer, it would be easier for people to use. When implemented well, APIs also provide a much higher level of performance and availability.

Question 4: Do you agree with our assessment of how Open Communications could enable services that benefit people in vulnerable circumstances? Are there other ways it could benefit people in vulnerable circumstances?	Confidential? – N

[1] Para 4.14

Vulnerable customers are typically the most disadvantaged group that we see across different markets and therefore potentially have the most to gain from Open Communications. Building the framework creates the basis upon which niche and targeted services and products can be built by providers, better servicing those in vulnerable circumstances.

Open Banking experience has shown that initiatives to spur innovation for vulnerable customers (e.g. Nesta Challenges' *Open Up Challenge 2020* and Nationwide's *Open Banking for Good*) have proven themselves effective at stimulating the market. Examples include debt advice charities using Open Banking to better manage their clients and FinTechs using Open Banking to help carers and families watch over vulnerable relatives; there is no reason why similar services tailored to the telecoms market could not be equally as successful.

Many vulnerable consumers may access Open Communications capabilities through intermediaries (such as charities, powers of attorney, carers etc.). Kalgera has launched a mobile and web app that analyses past and present financial behaviour to identify risks and trigger personalised alerts for nominated trusted parties without the vulnerable customer having to compromise their account details or ability to move money. Further consideration should be given to differing levels of access provision to nominated parties and to direct access to third parties.

Simple, consistent and familiar processes will always help those more vulnerable and increase the likelihood of customers engaging with the market and shopping around rather than hiding from it. It is also much easier for trusted third parties and intermediaries to help vulnerable individuals when the correct protocols and data sharing frameworks are in place, with appropriate and consistent customer protections. Introducing Open Communications branding or logos would further add to the levels of confidence for people to use services and prevent customers getting caught out by scams. Thought should also be given to a form of "trustmark" as part of wider Smart Data considerations to further build customer trust in and recognition of data sharing initiatives.

The consultation document highlights in several places the potential of combining Open Communications and Open Banking information to enable third parties to better help vulnerable customers to manage communications expenditure alongside other outgoings. This would be a significant benefit for all customers but if it is to be realised then a harmonised implementation approach with Open Banking (and all other Smart Data initiatives) is of critical importance.

Question 5: Are there any risks that we have not identified that could reduce the overall benefits of Open Communications? Please provide evidence, where possible.

Confidential? – N

The primary focus of Open Communications, or any Smart Data initiative, should be on delivering a first-rate customer experience and all the benefits it would bring to customers, providers and competition; the biggest risk would therefore be not delivering it.

There is also significant risk attached to not implementing it in the most effective way as a fragmented or uncoordinated approach would create its own risks, ultimately damaging the reputation of the initiative and potentially the reputations of data sharing in other markets, such as Open Banking.

- **Not harmonising standards** could lead to a patchwork delivery, inconsistent experiences, duplication of efforts, and increased costs and implementation time.
- **Not harmonising the liability framework** could lead to customer confusion and detriment, and providers not knowing their own liabilities.

- **Not reusing Open Banking assets**, for example the Directory, certificate issuance and the Dispute Management System could lead to duplicated infrastructure and unnecessary extra cost.
- **Not using a consistent authentication approach** would require customers to sign up, create, and remember multiple sets of credentials to authenticate themselves. There are several options to consider when designing Open Communications including using an existing mechanism such as Gov.verify (only 4.7m users and far fewer use it regularly), engaging with the banking industry to reuse the authentication mechanism used by Open Banking, which would mean an addressable population of the 40+ million consumers and small businesses that already use mobile and/or online banking, or leveraging the experience and skills of the telecoms industry in authentication solutions. However, work and thinking in the area of identity assurance more generally continues to mature. Future solutions may offer a good, cross-sector customer experience that development of Open Communications should consider.

In addition, not making Open Communications a mandatory requirement on incumbent providers would not be conducive to enabling customers to exercise their basic right to access their data and share it with chosen authorised third parties without contract and without discrimination.

There is always a risk that customers will choose not to use Open Communications services and consequently not benefit from its positive outcomes, but they are already likely to be opting out of data sharing so it would not cause any material disadvantage. Designing Open Communications in a way that puts customer trust and control at the heart of the architecture will help build confidence that their data is protected and will only be used for the specific purposes for which they have given their consent, thereby increasing customer willingness to participate.

Particular features that help in this regard are ensuring customers are provided with a clear and simple consent process that is transparent regarding how their data will be used, and how that consent can be revoked. The regulation of TPPs is also important to build customer trust; a regulated status should include the conditions that they hold themselves to high standards of data protection, and have robust security protocols and a good data governance process in place. This mitigates the risk of increased fraud. Data providers should be liable for incorrect data as this mitigates the risk of incorrect or incomplete data being shared with a TPP resulting in poor advice being given to customers.

Encouraging competition at the same time as preventing anti-competitive behaviour is key to any data sharing initiative. Competition may be enhanced by making those organisations that obtain data subject to a reciprocity requirement. This is a complex subject and one that requires detailed consideration by a range of stakeholders. There are broadly three types of reciprocity: data provider to data provider (where a receiver of data should probably be required to make data of the same category available to the provider), data provider to third party (where there may be merit but further thought is required) and data provider to big tech firm acting as a third party (where the nature of the data may be different, and should be considered in-scope of Smart Data considerations).

Competition risk could arise in how Open Communications is implemented, where firms might not allow equal access to TPPs. It is important that TPPs can compete and will innovate to find the best products for customers, and customers should be able to find it easy to try a few different TPPs to assess their recommendations. Domination of the market by only a few large TPPs would weaken competition and potentially stifle innovation, putting some at a competitive disadvantage. This would be exacerbated if Open Communications is not based on compulsion. To avoid this risk

the barriers to entry need to be kept low so that TPPs can compete on the strength of the insight they provide. The ability to use Premium APIs should also be considered from the outset to enable TPPs to better compete and to encourage cooperation from the banks with the sector.

Question 6: Do you agree with the core principles that we have identified for the design of Open Communications?	Confidential? – N

The identified core principles set out[2] are sensible and in line with Open Banking foundations. Ofcom's fourth core principle - "Users should be in control of the data they share" – is aligned with OBIE's belief that the primary objective of any Smart Data initiative should be to empower consumers and small businesses to exercise their basic right to access their data and share it with their chosen authorised third parties without contract and without discrimination. This leads to increased engagement, better service, more innovation and increased competition.

Based on our experience and learnings, we would recommend some additional overarching principles:

1. **Harmonising the way Open Communications works**

This would benefit customers, data providers, third parties, and policy makers and regulators. Commonality across user experience and data security encourages familiarity and trust, reduces cost and risk, lowers barriers to entry, and makes it easier to supervise. Not adopting this principle could lead to users being faced with a bewildering array of access procedures, consent flows, liability frameworks and dispute processes. Experience would suggest that customers and providers will simply not engage and intended policy outcomes will not be achieved.

2. **Minimising the implementation burden on industry**

Harmonising Open Communications by building upon Open Banking foundations would minimise the burden of implementation on the industry. The OBIE created and continues to maintain several assets, in particular the Open Banking standards, the Trust Framework, and the Dispute Management System, which could be repurposed for Open Communications and remove the cost of creating duplicate infrastructure. Firms seeking to minimise the implementation burden of Open Communications will be able to adopt best practices observed from Open Banking at the outset and will also benefit from better access to experienced talent and increasingly sophisticated suppliers. Importantly, a range of vendors and technical service providers (TSPs) now exist to support data providers constrained by legacy platforms. These TSPs can configure and host all the functionality from the incumbents' core mainframe systems through to the API front-end, thereby minimising expensive upgrades or platform changes.

3. **Recognising the benefits of central ecosystem support**

The OBIE was set up as a central, co-ordinating body to produce standards, support implementation and monitor activity. Implementation support lowers the cost of implementation for both data providers and third parties and improves consistency across the ecosystem. The OBIE monitors the ecosystem, runs a Conformance Certification Service and helps banks and TPPs test their implementations and resolve issues. We would strongly recommend a similar body is put in place for the implementation and ongoing monitoring of Open Communications.

4. **Recognising the benefits of a common authentication approach**

[2] Table 3, p.41

Having a common approach, common interface and common protections mean there is a greater opportunity to build familiarity and trust with customers. Having a common authentication approach would greatly simplify customer engagement and reduce unnecessary friction; it also means users would not have to go through the inconvenience of signing up to new services and then having to remember credentials for each of these new services.

5. Mandating Open Communications by law

The primary objective of any Smart Data initiative should be to empower consumers and small businesses to exercise their basic right to access their data and share it with their chosen authorised third parties without contract and without discrimination. We believe, therefore, that it is reasonable and required that Open Communications be a mandatory requirement for incumbent providers. There is a role for voluntary industry initiatives, however the learning from the Midata experience (discussed in more detail below) is that mandatory powers are critical. Without compulsion it is difficult to achieve consensus and programs will likely under deliver or become delayed. Deadlines should also not be set at the pace of the slowest incumbents. In addition, where Smart Data initiatives rely exclusively on proprietary APIs and market coordination is absent, there is an inherent risk of unfair price discrimination to access data.

6. Ensuring equitable funding arrangements.

Open Banking has been funded by the largest providers of personal and business current accounts in Great Britain and Northern Ireland (known collectively as the CMA9) according to their market share. However, an industry levy across all incumbents based on size may be a better approach for Open Communications as it is more representative. Third party providers should also, as a matter of principle, contribute to funding, but at a lower level commensurate with their size. Proxies could include revenues, customer base, active sectors, level of accreditation, etc. Ofcom could explore using the levy that it currently charges to its relevant regulated entities as a potential mechanism for collecting the funding required for Open Communications. Caution should be exercised to ensure absolute levels for smaller players are manageable as third parties are crucial to bringing innovation and competition to the sectors.

A key principle that our experience has taught us is that future data sharing initiatives like Open Communications should set out at the start where regulation should finish and the market should be able to take over to achieve a desired outcome. Regulators and regulation work best when they can create the right environment, conditions and framework for the market to innovate and compete – both kickstarting the industry into action where it hasn't occurred voluntarily and enabling disrupters to enter the market and cause a new sense of competition themselves.

The intention with Open Banking was to get the standards right and then allow the market to take over and deliver the products and services. As the first of its kind in the world, it has been a learning exercise knowing how far to take the standards development and serves as a case study of how to best make this regulatory approach its most effective. Development of the standards ended up going further than first expected as they included determining minimum customer experience standards, when it became apparent that it was not appropriate to leave this completely in the competitive space. Future regulatory initiatives should be clear from the outset on what is mandatory and what is voluntary.

Another key learning is around the governance set-up of any vehicle delivering regulatory change, to allow the right mix of regulatory requirements and commercial incentives to provide the best outcome for end users. Opportunities for incumbents to generate new revenue streams to offset some of the costs of implementation will tend to be welcomed. In Open Banking, this has meant having a baseline set of mandatory requirements under the CMA Order and the Payment Services

Regulations (PSRs), with additional non-mandatory Premium APIs that can be leveraged by banks commercially. As well as enabling the recovery of initial costs, Premium APIs have the indirect benefit of increasing API performance and co-operation with TPPs. Examples of Premium APIs in the Open Banking market are those that enable delegated authentication to simplify the customer experience, those that provide additional attributes such as payer address, and those that deliver higher performance standards than required by the PSRs.

OBIE also views making certain standards obligatory as being critical to success. Where data providers have significant flexibility in design, our experience has been this could result in inconsistent implementation and poor customer journeys which will subsequently need to be reworked. Additionally, where implementation has been voluntary, progress has been slow due to difficulties being experienced in reaching agreement on common standards and implementation approaches.

In the context of Open Banking, feedback from some of the CMA9 is that a mandatory approach has actually had considerable benefits in enabling better coordination and sensible prioritisation to reduce cost. It has also ensured that the project requirements were developed in a highly collaborative way that facilitated manageable implementation. This enabled efficiency and reduced risk to operational resilience.

It is notable that in its response to the Canadian Department of Finance's Consultation Paper, HSBC compared the UK regulatory-led mandatory approach to Open Banking with a US market-driven approach and concludes: "The UK approach provides the government with control of decisions in areas such as the launch date of the regime, the identification of participating banks and the authorization requirements of TPPs. In contrast, the US approach leaves these decisions in the hands of individual banks, which has led to significantly slower progress in the adoption of Open Banking in the United States and more limited customer engagement. The UK approach would appear to reduce the risk of internal inconsistencies. To take an example, a US customer seeking to access their banking information with a TPP could find that one of their US banks has signed a contractual agreement with that TPP, while their second bank has not. As such, the expected benefits of open banking would be reduced".[3]

It is worth highlighting Midata as an example of how compulsion is often required to achieve the desired policy outcomes. Launched in 2011, Midata was a voluntary programme promoted by the Government in partnership with the energy, banking, telecoms and retail sectors and was intended to give consumers greater access to their transaction data. Banks voluntarily supported the initiative by providing downloadable account transaction data in a standardised file format but there was less willingness by the incumbents in the other industry sectors. Despite claims that Midata would "change personal banking forever", it never achieved widespread adoption, largely because of the poor user experience. However, the learning from Midata was a step in the evolution of Open Banking, with a recognition of the importance of implementation.

Question 7: On what kinds of communications providers do you consider that any obligation to provide customer and data should sit?	Confidential? – N

Open Banking was mandated by the CMA on the nine largest providers of personal and business current accounts in Great Britain and Northern Ireland according to market share. These nine providers have also had to share the cost of implementation. This approach has been criticised as

[3] https://www.canada.ca/content/dam/fin/consultations/2019/ob-bo/ob-bo-38.pdf

a point of principle by the mandated institutions, with concerns largely directed at the non-mandated incumbents.

A broader coverage of providers would be strongly beneficial to achieving the objectives of Open Communications but we understand the concerns about placing burdens on smaller providers and the risk that costs are disproportionate to the benefits of Open Communications. Under Open Banking we have found that an innovative group of vendors and TPPs have emerged that can supply off-the-shelf solutions. These organisations would be well placed to serve Open Communications participants to ease the technical and financial burdens of implementing the initiative and helping to lower the barriers to entry.

Further measures to ease delivery for participants can also be taken, such as ensuring a fair and appropriate funding mechanism is put in place, the data sharing requirements are proportionate, and adding revenue-generating extras like Premium APIs help to offset the implementation costs and provide additional commercial opportunities.

We would also recommend a phased roll-out and suggest that a manageable group of the largest providers should be encouraged to launch APIs together. Insisting that all providers launch simultaneously would be disadvantageous in that it would seriously hinder implementation timelines, which would be constrained by the pace of the slowest providers. This requirement should be factored into the proposed timing of roll-out. Selecting large providers ensures that TPPs have access to a wide pool of accounts, which they need for their services to be meaningful.

Question 8: Do you agree with our initial views on how to approach key issues for the design and operation of Open Communications? Do you have comments to make on other implementation issues?	Confidential? – N

Open Banking offers the basis for other data sharing initiatives to build upon. We strongly believe that adopting Open Banking approaches and assets would benefit all parties by leading to a lower cost and less risky implementation, a faster speed to market, and greater customer adoption.

Harmonising standards benefits all stakeholders. For incumbents and TPPs it streamlines implementation and reduces costs; for consumers it provides a common approach, common interface and common protections; and for policy makers and regulators, it maximises adoption and is easier to regulate. The Government and sector regulators should be aiming for harmonisation and consistency in design and operation across all Smart Data initiatives.

There are a number of other design principles based on our experience, which we believe would help create a consistent approach and experience and ease the path to full implementation:

- **Trustee approach** – the Implementation Trustee played a key role in defining the minimum viable proposition without the need to wait for agreement on all aspects of the implementation approach, leading to a quicker to market delivery.
- **Compulsion** – there is a role for voluntary industry initiatives; however, as already explained the learning from Midata is that mandatory powers are critical for achieving desired policy outcomes.
- **Funding** – getting the right approach to splitting the cost of implementation is important. An industry levy may be a better mechanism than the Open Banking approach of being funded by the nine largest incumbents.
- **Infrastructure** – this should be shared across sectors to reduce costs and time to market.

- **Liability framework** – should be consistent to engender consumer trust and ensure consistent consumer protection.
- **Data models** – there are many components to a standard; data models sit on top of the security protocols and trust frameworks and are relatively simple to create and should be sector specific.
- **Security protocols** – a security standard is crucial to customer trust and should be common across all Smart Data initiatives. There should be a common approach to consent and authentication.
- **Authentication** – there should be a common approach for a consistent and common user experience.
- **Implementation support** – this is a critical aspect as standards on their own are not sufficient. Implementation support improves consistency across an ecosystem and lowers the costs of implementation for incumbents and third parties.
- **TPP accreditation** – this is crucial to consumer trust and protection and the criteria should be standardised across initiatives. A lower level of accreditation than that used in Open Banking might be better suited for non-financial data, but requirements should be based on common components and be incremental.
- **Reciprocity** – this has not been mandated under PSD2 for Open Banking but the one-way flow is sometimes criticised; it would be worth considering mandating recipients of data to also make data available.
- **Trustmark** – this could support customer confidence in using Open Communications and other Smart Data initiatives.

Authentication

It is important that consent by customers to share their data is explicit and informed. It is crucial that customers can actively choose not only with whom their data is shared, but also how it will be used to engender trust, confidence and use of Open Communications services and products. Open Banking developed consent standards and dashboards to give customers this control and confidence and we would recommend that Open Communications follows the same approach.

Having a common approach, common interface and common protections mean there is a greater opportunity to build familiarity and trust with customers, both of which are crucial to mass adoption and reducing the risk of fraud or poor outcomes. Having a common authentication approach would greatly simplify customer engagement and reduce unnecessary friction; it also means users would not have to go through the inconvenience of signing up to new services and then having to remember credentials for each of these new services.

There are several options to consider when designing Open Communications including using an existing mechanism such as Gov.verify, engaging with the banking industry to reuse the authentication mechanism used by Open Banking, which would mean an addressable population of over forty million consumers and small businesses that already use mobile and/or online banking, or leveraging the experience and skills of the telecoms industry in authentication solutions.

Open Communications has the benefit of having telecommunications providers being at the heart of authentication solutions already. Customers are very familiar with the common authentication method of One Time Password (OTP) by SMS being used across multiple platforms, with work continuing on more secure versions. This industry experience will give the development of Open Communications an advantage in considering its authentication framework.

Repurposing the authentication and consent method pioneered by Open Banking is a clear and strong option for consideration. There are over forty million UK consumers and small businesses already very familiar with bank authentication, which underpins the Open Banking consent model and means that they can already choose to access Open Banking services without needing additional onboarding or passwords. Using the Open Banking consent model would therefore mean that Open Communications would be also be immediately accessible by these forty million plus customers.

However, work and thinking in the area of identity assurance more generally continues to mature. Future solutions may offer a good, cross-sector customer experience that development of Open Communications should consider, reducing customer friction even further.

Whichever method of authentication and consent is pursued, the principles of harmonisation, consistency and a simple, frictionless customer experience should remain the same. Cross-sector engagement is key to ensure that all Smart Data initiatives can work together to provide most benefit to customers. The objectives should be to find a way of enabling third parties to authenticate so that customers don't need to undergo redirection, which adds friction to the customer experience, and enable long-lived consents so that customers aren't forced to re-authorise on a regular basis.

Asking customers to re-authorise their consent is an important prompt to use when they appear to have disengaged from the service or product in use and plays to the overall principle that transparency and informed consent are key. However, regularly requiring customers to undergo this process when they are happy and actively using Open Communications services can cause unnecessary irritation and risk putting customers off further use.

Leveraging existing Open Banking assets and services

OBIE developed and maintains a number of assets and services; we believe that leveraging them for Open Communications will be of enormous benefit to participants and customers and has the potential to underpin a harmonised cross-sector approach.

This approach would lead to lower implementation costs as the majority of work is reusable (other than the data models), faster time to market and lower risk. It seems unnecessary for other sectors to go through same process, spending time and money reinventing what already exists. Significant investment was made in building the Directory and Dispute Management System, both of which are largely reusable. Additionally, if TPP accreditation is standardised then an ecosystem of TPPs will already be available to work with the standards to aid the telecoms sector with their implementation.

We set out these assets and services below.

Figure 1

Standards

A report published in July 2019 concluded that the Open Banking standards were world leading and noted that they are being adopted globally not only in relation to financial data but also in relation to cross-sector data.[4] These findings led the Open Data Institute (one of the co-authors of the report) to conclude "The Open Banking model is an appropriate model to use for other sectors such as energy and telecoms…. Improved data portability through secure APIs is a structure that could work for more than just retail banking. Energy, telecommunications, and other sectors could benefit from understanding the journey of Open Banking and its potential to help make data work for everyone".[5]

- *Technical standards*

Open Banking allows bank customers to access account information, including their account balance, historical transactions and regular payments, with TPPs on an ongoing basis. It uses standardised APIs to do this, so that each bank provides this information to third parties in an identical way. The Open Banking standards and support infrastructure are available to all banks, not just those mandated under the Order, under an Open Licence. Security considerations were central to the architecture of Open Banking and therefore a distributed open API model was chosen over a

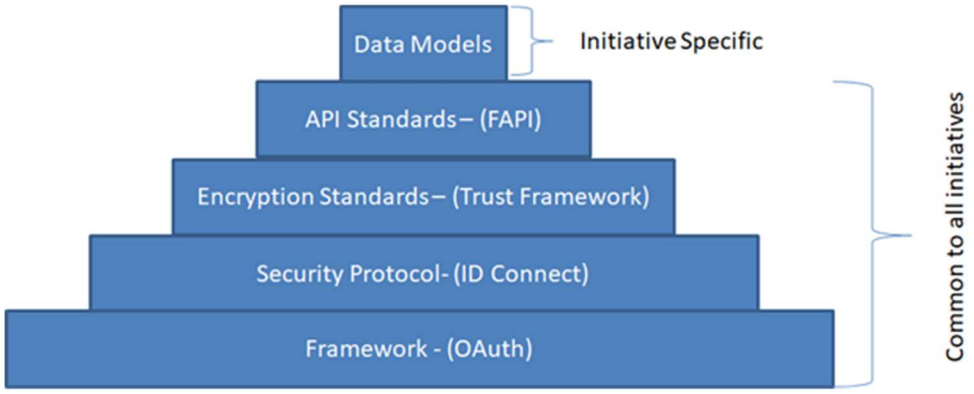
[4] Fingleton Associates/ODI - *Open Banking, Preparing for lift off* (July 2019) https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf

[5] https://theodi.org/article/how-far-open-banking-has-come-our-five-takeaways

centralised proprietary model in order to avoid having a single point of failure. Critically, the Open Banking API standards sit on top of a trust framework (that ensures only authorised entities are able to participate in the ecosystem) and an authentication mechanism (that allows customers to identify themselves in a safe and secure manner). These components are the building blocks of enabling customers to share data in a safe and secure way and can be harmonised across multiple sectors to reduce risk and provide a harmonised approach that drives cross-sector consistency.

The technical standards comprise a hierarchy as set out in figure 2.

Figure 2



The majority of the components are common to all initiatives apart from the data models. The data models contain the specific data items to be transferred for each sector. Harmonisation should occur in the components that are responsible for security, identify and authentication.

Open Banking standards are tightly defined. Some standards are not tightly defined and therefore resemble frameworks rather than standards and lead to implementation variances. Open Banking has developed a suite of conformance tools that can assess algorithmically whether standards have been implemented correctly.

It should be noted that the Open Banking standards are open licence to maximise participant adoption.

- *User Experience Standards*

Open Banking recognised that technical API standards alone are not sufficient for delivering a good user experience, which in itself is critical to adoption. We have therefore built supporting non-technical standards in the form of user experience standards (to harmonise and remove friction from the customer experience) and performance standards (to ensure the APIs perform to a minimum level of performance). This is a clear learning from Open Banking that is of key relevance for other Smart Data initiatives, including Open Communications.

Other important lessons have been learned in the initial implementation where some of the authentication processes were unexpectedly laborious for customers and this poor customer experience presented a significant barrier for customer adoption. In order to create a smoother authentication journey, the OBIE developed and mandated user experience standards, which were called the “Customer Experience Guidelines” (CEG) over the course of 2018. The publication of these standards in September 2018 also mandated full support for mobile, where customers are redirected to their banking app (rather than their browser) to approve new consents. These new

guidelines deliver a less complicated, one step journey that is intuitive to end users. This is a model that should be used as a template for Open Communications.

A common, consistent user experience will be reassuring to customers. A common experience minimises customer confusion and improves adoption of any data sharing initiative. The alternative is that customers will have to learn to interact in numerous different ways with each Smart Data initiatives. This harmonisation is essential as otherwise incumbent providers in each sector will inevitably take different approaches.

Customer authentication is a key requirement in any data sharing implementation. The protocol for authorisation and authentication must balance a customer-friendly user experience with security considerations. The Open Banking approach involves third parties redirecting the user of their application to the user's bank's website so that they can authorise the transfer of information. This approach is very secure and also supports a smooth customer experience.

If Open Communications did choose to leverage the existing Open Banking authentication infrastructure, it would enable the customer to authenticate without needing to remember new usernames and passwords. The principal benefit of doing so is that it provides immediate access to over forty million people who use mobile or online banking in the UK and crucially these mobile banking customers use their mobile banking apps over 30 times per month, giving them a high-quality authentication mechanism with which they are already fully familiar. It should be noted that simply using the bank authentication mechanism does not mean the bank accesses the customer data. It will be important to open up the market for authentication services to providers other than just banks.

- *Operational Guidelines*

Open Banking also developed standards covering availability, performance and testing to ensure incumbents have target service levels therefore enabling TPPs to reliably offer services to consumers and small businesses. These standards can become part of the regulatory monitoring of the implementation of the standards.

Directory

The CMA Order required the creation of a "whitelist" of authorised TPPs that could be securely identified by the banks. This whitelist, now known as the Open Banking Directory, was built so that the CMA9 and other banks could identify and trust the TPP seeking to access its APIs and confirm that the TPP has the appropriate regulatory permissions. The Directory also allows TPPs to easily locate and connect to banks also enrolled in Open Banking. The Directory was a material cost to build for the Open Banking initiative. The Directory is a flexible asset and has been repurposed to support the Confirmation of Payee service, which is not directly related to Open Banking but shares the basic requirement of an ecosystem requiring a whitelist. This is an essential requirement for all other sectors.

User dispute mechanism

The CMA required the OBIE to create a customer redress mechanism to manage consumer complaints and ensure that their complaint was appropriately dealt with between the bank and the TPP. Open Banking has developed a Dispute Management System which enables multiple third parties to resolve disputes between themselves, speeding up resolution.

Implementation Support

Open Banking is a "many-to-many" network, with many TPPs connecting to many banks. Connecting to such a network can be a complex task for both data providers and TPPs. Open Banking provides support by helping banks find TPPs with whom to test their implementations (and vice versa) and helping resolve issues identified by participants. A co-ordinated approach to this would drive efficiency, enable the learnings in one sector to be exchanged effectively to another and streamline the implementation process for participants.

Monitoring Function

Open Banking has a monitoring function ensuring that the CMA9 meet their obligations under the CMA Order. This includes timely conformance with technical standards and compliance with the User Experience Standards and Operational Guidelines. The Trustee has powers, delegated by the CMA, to impose remedial actions on the CMA9 as necessary.

We would strongly recommend that these assets and services are leveraged for Open Communications for the benefit of all participants and users.

Question 9: Do you agree with our view of the data that Open Communications should make available to third parties? Is there data about accessibility needs or vulnerable circumstances that people would benefit from being able to share with third parties?	Confidential? – N

Open Communications should be covered by an overarching regulatory framework for sharing in-scope data. This framework should address the regulated roles and customer protections necessary for the purposes of sharing data and build upon GDPR. Data providers should be responsible for the factual accuracy of the data provided but not carry any contingent liability for the data beyond that. We believe that only authorised firms should act as receiving parties. This is essential to safeguarding trust in the ecosystem for both end users and data providers.

The customer's right to data portability and the right to withdraw consent under GDPR is critical but is insufficient on its own to give consumers and businesses the tools that they need to actively manage their data. They should also be able to determine what data elements they choose to enable TPPs to access, to whom that access is granted, for what period, for what purpose(s), as well as the ability to revoke consent. Open Communications would provide the mechanism to securely transfer their data, where they choose to do so, increasing their ability to leverage their personal data.

To ensure customers are fully aware of how the data they choose to share will be used and have confidence that this will be the case, it is essential to provide them with a clear and simple consent process in which there is transparency regarding this point.

In-scope data should be consistent with the portability requirements of GDPR (i.e. include all data provided by the customer to the data provider as well as all data derived from activity with the data provider). It should also include any data reasonably required for the Open Communications APIs to technically function (e.g. metadata such as transaction IDs). Out-of-scope data should include data that is proprietary to the data provider (e.g. enhanced algorithms).

It is important that there are market incentives for incumbents. It should not be mandatory for all data elements to be provided for free to customers and TPPs. For example, it may be appropriate that charges could be levied for the use of derived data or data that has been validated by the incumbent, where they have added value to the underlying customer data held. For these additional services, it will be useful to utilise the same standards uniformly across the market, but for data providers to contract privately with TPPs wishing to use the service. We have termed these services Premium APIs. As well enabling recovery of initial costs, Premium APIs have the indirect benefit of providing commercial incentives for increasing regulatory API performance and co-operation with TPPs.

Open Communications should be rolled-out in steps to start delivering customer benefits as early as possible. The simpler aspects of basic read-only data such as product and service quality data should be made available first to allow for simple product comparison. Taking a staggered approach will also allow time to ensure that the data is top quality and that performance is high, which are both critical to customer confidence and adoption.

Question 10: What are your views on the appropriate arrangements for determining liability and redress in disputes between customers, providers and / or third parties?	Confidential? – N

The CMA required the OBIE to create a customer redress mechanism to manage consumer complaints and ensure that their complaint was appropriately dealt with between bank and TPP. Open Banking developed a Dispute Management System which enables multiple parties to resolve disputes between themselves, speeding up resolution and, as discussed in our response to question 8, we believe this could be reused by Open Communications. Having a harmonised liability framework would help to engender consumer trust and ensure consistent consumer protection.

Under the legal framework of the Payment Services Regulations (PSRs), providers are required to hold professional indemnity insurance (or other comparable guarantee) to cover their liabilities that arise under the Regulations. Ofcom may wish to consider whether something similar may be required to offer further protection under Open Communications.

Open Communications should include an overarching regulatory framework for sharing in-scope data to address the regulated roles and customer protections necessary for the purposes of sharing data safely, building upon GDPR. Data providers should be responsible for the factual accuracy of the data provided but not carry any contingent liability for the data beyond that. GDPR does not provide a framework for customer redress, which is why ensuring a suitable mechanism is in place is so important. Under the Revised Open Banking Roadmap, we are currently consulting on whether it would be helpful to develop a voluntary code in addition to statutory provisions.

We currently have work underway to assess appropriate protections for customers with regards to Open Banking-enabled payments. Whilst not directly relevant to Open Communications we would be happy to share findings with Ofcom once concluded in case there are any useful learnings to consider.

Question 11: Do you agree that we have identified the main sources of costs for implementing Open Communications for both providers and	Confidential? – N

services that use Open Communications data? Are there any sources of costs that we have missed?	
Question 12: What factors will drive the overall scale of costs to in-scope communication providers and to third parties? How might this level of cost vary depending on whether providers serve residential and / or business customers?	Confidential? – N

As the first of its kind in the world, it is tempting to look at Open Banking as a benchmark for costing Open Communications. We would strongly argue against this for several reasons. There is undoubtably a huge amount to learn and reuse from Open Banking, as we have set out in this response, but it's important to recognise the differences between the Open Banking implementation and that of Open Communications.

Technical differences

- Implementing the payment initiation standards has been one of the most complex parts of Open Banking and therefore costly. This wouldn't be needed in Open Communications.
- Open Banking is more complicated than Open Communications because transaction data updates frequently and for some use cases real-time information is required. Daily updates would keep costs down, although we appreciate that this would need to be a consideration for aspects such as data usage during the design stage.
- Payment initiation functionality requires the highest levels of security, fraud protection, performance and resilience. Open Communications is generally only likely to require 'read-only' access, which doesn't need such a stringent framework.
- Open Communications can build on our existing standards and assets rather than starting from scratch as was the case for Open Banking.

Banks' implementation approach

- The implementation efforts of banks in Open Banking have varied significantly, leading to individual costs being widely spread on the cost spectrum to implement the same aspects.
- Those who experienced the highest costs tended to focus on delivering a minimally compliant product only, then frequently suffered higher costs as a result of proprietary build, over-tailoring products and a poor choice of suppliers. This undoubtably resulted in complexity, delays and re-work.
- The highest costs frequently included the cost of making upgrades to or creating core technology assets that they would otherwise have had to do irrespective of Open Banking obligations. These are also assets that have multiple purposes across the bank.
- Those participants that adopted an agile, purpose-driven approach meant a quicker, cheaper and higher quality implementation.
- Banks that had invested in modern cloud-based platforms or data lakes or outsourced their front-end to technical service providers were also able to implement more quickly, cheaply and to a higher quality. This has also made their systems more sustainable and more likely to provide a higher performance and availability.

Firms under Open Communications will benefit from adopting Open Banking best practices from the outset and from better access to experienced and increasingly sophisticated suppliers. TSPs also now exist to support data providers who may be constrained by legacy platforms, which can minimise the cost and burden of expensive upgrades or platform changes.

It should also be made clear to incumbents that there are revenue-generating opportunities that can come out of Open Communications, which can also offset the delivery costs. Not all data elements should be provided for free, and participants should be free to pursue additional charged-for services (through Premium APIs). We have also found that Premium APIs bring an indirect benefit of increasing API performance and co-operation with TPPs.	
Question 13: If relevant, please estimate and describe, as far as possible, the costs to your organisation of implementing and running Open Communications.	Confidential? – N
OBIE is not providing a response to this question.	
Question 14: If relevant, would your organisation consider using Open Communications data as a third party to offer new services or enhance existing ones?	Confidential? – N
OBIE is not providing a response to this question.	