ACCC Consultation on the participation of Third Party Service Providers

TrueLayer response, January 2020

Dear ACCC Committee

Thank you for the opportunity to comment on the consultation on the participation of Third Party Services Providers ("intermediaries") in the CDR regime.

We understand the concerns and questions raised in the paper and agree with the ACCC's desire to drive innovation and value for consumers in the new Australian CDR data economy, while keeping security levels high and giving people control and visibility over how their data is accessed and shared.

About TrueLayer

TrueLayer is a UK-headquartered FinTech firm, founded in 2016 and authorised by the UK's Financial Conduct Authority ("FCA"). Our platform is a prototypical intermediary: it allows clients to access their customers' banking data and initiate payments from their customers' accounts in a uniform, simple, and secure manner by integrating our Application Programming Interface ("API").

Our customers tend to be FinTechs and innovative tech companies, as well as larger financial institutions and corporations. We enable them to build novel, seamless user journeys, and to improve the efficiency of their processes (especially manual workflows dealing with financial and identity data, and payments).

Our plans for Australia

We see Australia as a key growth market for our business, and the first key market outside of Europe. We are very optimistic about the potential brought about by the incoming CDR regime, and are encouraged by the clear and visible regulatory and government support for FinTech and Regtech. TrueLayer was also one of the inaugural participants in the UK-Australia FinTech Bridge in 2018/2019, and we have participated in a number of policy discussions since.

In 2020, we intend to bring our API-based Open Banking platform to Australia and help local and international companies to build better experiences for their customers - all with the appropriate consents and data protection in place. We also hope to help Australian FinTechs and scale-ups export their products globally with our platform. From our founding day, TrueLayer has been focused on growing the global Open Banking economy, and we want to continue this work in Australia, as we have done in Europe.

We have responded in detail to the questions in the Annex to this document, however we would like to highlight upfront our key points, which are:

- We support a range of business models for intermediaries, some which require **full accreditation for intermediaries**, but also the option for intermediaries to be **unaccredited outsourced providers** to accredited persons.
- We support a **principles-based approach to sharing with non-accredited parties** (i.e. treat sharing of CDR data with non-accredited parties the same as sharing non-CDR personal sensitive information)

In addition to the matters specifically raised in this consultation, we also wish to highlight our desire for **easier and wider access to testing environments** (i.e. allow more interested parties to access the sandboxes for CDR APIs as soon as possible, and find a way to allow non-accredited parties to test APIs to enable more innovation).

Once again, TrueLayer are grateful for this opportunity to share our views with the ACCC, and look forward to contributing to Australia's growing FinTech industry.

TRUELAYER LIMITED

ANNEX - CONSULTATION PAPER QUESTIONS

Consultation questions on intermediaries

If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend to only collect CDR data, or collect and use CDR data?

TrueLayer wishes to operate in Australia in the following ways:

- Be an outsource provider to Accredited parties (we consider this is already possible under rule 1.10). TrueLayer will help accredited parties with accessing CDR APIs across multiple banks (API aggregation). This could be described as an intermediary service - we have described this role as 'outsourced technical services provider for an accredited person' (model 1 below).
- Be a CDR accredited party in our own right utilising the proposed models below, where we partner with customer-facing companies who have a 'lower tier' of accreditation (model 2 below); or with non-accredited persons (model 3 below).

In these models, with the consent and instructions of the consumer, we intend to collect and use CDR data on behalf of our clients, who will use it to provide service and build better experiences for consumers. Examples of this would be a consumer lender using the banking CDR data to assess affordability of a loan, or a new financial application using the CDR data to help tenants get their rental payments recognised as part of their credit history in some way, or a personal finance management app providing a dashboard for a consumer to keep track of their finances in one place.

Our platform allows our clients to access banking data in a secure way on an increasingly global basis. We specialise in connecting to the best banking APIs in the world and normalising the information that is provided in one easy-to-use format for our clients. As part of this, we also handle the authentication and consent journeys of the end-user (more often a consumer, although we also support corporate use cases), making it faster and simpler for companies to start providing Open-Banking-enabled features to their customers.

What value or economic efficiencies do you consider that intermediaries can bring to the CDR regime and for consumers?

Intermediaries can bring a range of values to the CDR regime, both for consumers, and for innovators who wish to bring their products to market. However, the amount of value that intermediaries can offer will be dependent on the intermediaries model adopted by the ACCC following this consultation. For example, if the ACCC opt to require both intermediaries and their clients to obtain 'unrestricted' level accreditation, this will severely limit the efficiencies and benefits of intermediaries in the CDR regime, raising significant barriers for smaller innovators. Therefore, the values we have set out below assume the adopted model will not require both intermediaries and their clients to obtain full accreditation by the ACCC.

Values of intermediaries to the CDR regime:

- **Lower barriers to entry** for companies to make use of CDR data – in particular, by intermediaries taking on the regulatory burden and associated costs of full unrestricted accreditation, smaller companies and especially startups can gain access to CDR data without the financial and regulatory burden of obtaining accreditation. This would allow innovators to access the market quicker.
- **Increased productivity in the economy** due to reduction of 'double-work' – in allowing intermediaries to build the API platforms which connect with the CDR data holders, fewer companies have to dedicate resource to building and maintaining their own connections to banks. Innovators can instead focus their efforts on creating products which benefit consumers.
- **Consolidated feedback for data holders and API standard creators** -- since intermediaries see many different use cases and clients, they can verify whether problems occur for multiple sectors and feed this back to the standards bodies and banks directly. Today in Europe, the most active participants in the Open Banking API improvement discussions are intermediaries, since their clients often don't have the resources or deep knowledge of the ecosystem to provide useful feedback.
- **Avoiding pitfalls by sharing international experiences**, especially from experienced intermediary firms such as TrueLayer who have contributed to the European Open Banking journey and have implemented many different protocols.

Value of intermediaries to consumers:

- **Higher likelihood of new competitive products** using CDR data, due to lower barriers to entry to using secure connections for accessing banking data.
- **A pathway towards fewer places to manage CDR consents**, with a possibility for intermediaries to take a more central role in helping consumers manage data sharing.
- **Higher security standards**, since intermediaries have expertise in data and cyber security, and a much larger part of their business success depends on being reliable and audited in this space.
- **Better user journeys and experiences**, since start-ups and innovators can focus on this area of value, rather than building the technical pipelines to access CDR data.

- **All of which leads to a 'flywheel effect':** better products mean higher uptake of CDR APIs which leads to continuous improvement of these APIs due to more usage, which in turn leads to better products... leading to better outcomes for consumers, faster.

How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.

Our experience in the UK open banking market has demonstrated that intermediaries can inhabit the roles of either 'outsource provider', or 'accredited provider' depending on the situation and client type.

In Australia, we believe the drawing of the regulatory perimeter (those subject to CDR rules) should be based around the parties who can be *instructed* by the consumer to collect or 'retrieve' the CDR data from the data holder. Since data cannot be 'put back' once it has been retrieved, those instructed to retrieve data must bear important responsibilities for handling and/or transmitting that data safely securely, and for obtaining the explicit consent of the consumer. In a model where those who are instructed are subject to the CDR rules, we believe regulation of intermediaries should be broadly as follows:

- **Model 1 - Intermediary acting as an outsource provider for a fully accredited party** - the intermediary is not CDR accredited, because it is an outsourced function of an accredited party (we consider this is already possible under rule 1.10). The intermediary makes the technical connections to the banks, but it is the accredited party that is instructed by the CDR consumer, and the accredited party remains fully responsible for data retrieval, storage and transmission and for all outsourced functions.
- **Model 2 - Lower tier accredited party partnering with a fully accredited intermediary** - consumer-facing service providers may have a valuable, innovative service for consumers, but not have the means to become fully accredited under the CDR. We propose that they would partner with a fully accredited 'intermediary'. The 'intermediary' in this model would bear the majority of responsibilities and liabilities for the data retrieval, storage and transmission. However, the consumer could still instruct the lower tier accredited party to access bank data (an instruction it would pass on to the intermediary acting in a fully accredited capacity). Importantly, the consumer would have the same rights when instructing a lower tier CDR party, as when instructing a fully accredited party.
- **Model 3 - Fully accredited party instructed to share data with a non-accredited party** - once the data is retrieved (with the consumers consent), we consider that the data belongs to the consumer, who should be able to decide what happens with it. We propose that a consumer should be able to instruct an intermediary acting in a fully

accredited capacity to share data with an unaccredited party. In effect, data would be leaving the CDR perimeter in this model, but the unaccredited party would need to comply with other privacy laws.

We expand and illustrate these models below:

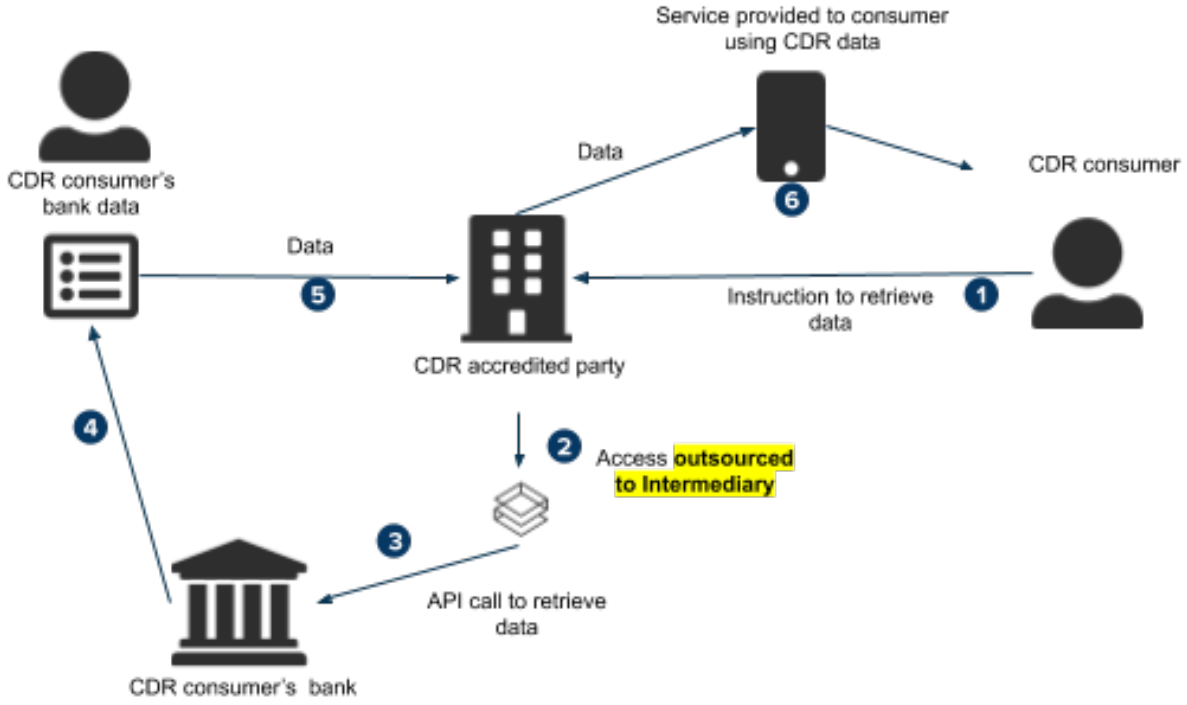
Model 1 - Outsourced Provider

For the first model, we believe the CDR regime should operate similarly to Europe, specifically the role of technical service providers such as TrueLayer. In Europe, as a pure 'outsourced provider' intermediary, we meet the needs of our more established clients, by acting as a single point of connectivity into the banks (rather than our clients having to maintain these connections themselves). Under EU rules:

- These clients must be regulated as third-party providers ("TPPs") in their own right under PSD2.
- TrueLayer uses the access certificates of its regulated clients (this is permissible under the regulations).
- Typically, TrueLayer only 'processes' data, passing it through to the accredited provider which stores the data and becomes the controller.
- The customer has a right of redress to these clients (rather than to TrueLayer).
- TrueLayer is not visible in the customer journey but the role of the intermediary is covered in the accredited provider's terms and conditions with the end customer.
- Our client is responsible for making sure outsource arrangements allow it to comply with relevant rules.
- As a technical service provider we are not directly regulated under PSD2, but must ensure our client remains compliant. We must meet GDPR rules as a data processor.

As a result, for this model to work in Australia, TrueLayer's client would need to be fully accredited by the ACCC. The intermediary would not itself need to be accredited if it was only operating under this business model.

Figure 1. Illustration of intermediaries as unaccredited outsource providers (Model 1)



An example use case of the model above would be an established large FinTech firm such as Revolut, who has the requisite funds and capabilities to apply for accreditation. Revolut, in order to enable OpenBanking services on its platform (similar to its recently launched OpenBanking features in the UK), would partner with TrueLayer for TrueLayer to aggregate and maintain access to the CDR APIs. TrueLayer would be responsible for the overheads associated with maintaining access to the CDR APIs, but would utilise Revolut's accreditation to access CDR data for its clients.

Benefits of this approach:

- Where a client wants to fully own the relationship with the customer, and provide services in its own right as an accredited provider, this model allows them to do so, without the

overheads of maintaining connectivity to multiple banks (which becomes the intermediary's role).

- The customer facing business is the accredited provider, so the customer is clear who they should contact if something goes wrong (they need not contact the intermediary). CDR complaints would be made to the accredited person, not the intermediary.

We believe that the rules as currently drafted allow for the provision of the services detailed above, in that the intermediary could act as an outsourced provider to accredited persons, providing the technical means to access CDR data on behalf of the accredited person. As such, we do not consider further amendments to the CDR regime are required in this regard.

However, while noting that intermediaries would not need accreditation in this model, the ACCC may want to ensure that there is explicit recognition of 'Outsource Providers' of this type in the regulations, so that banks would know that intermediaries have a right to access CDR data when acting 'on behalf' of accredited providers. The rules would need to allow for the outsourced provider to use the accredited persons' certificates to access CDR data on behalf of the accredited person. In this scenario, the accredited person remains fully liable for ensuring the outsourced provider's compliance with the CDR regime.

Model 2 - Lower tier accredited party partnering with a fully accredited intermediary

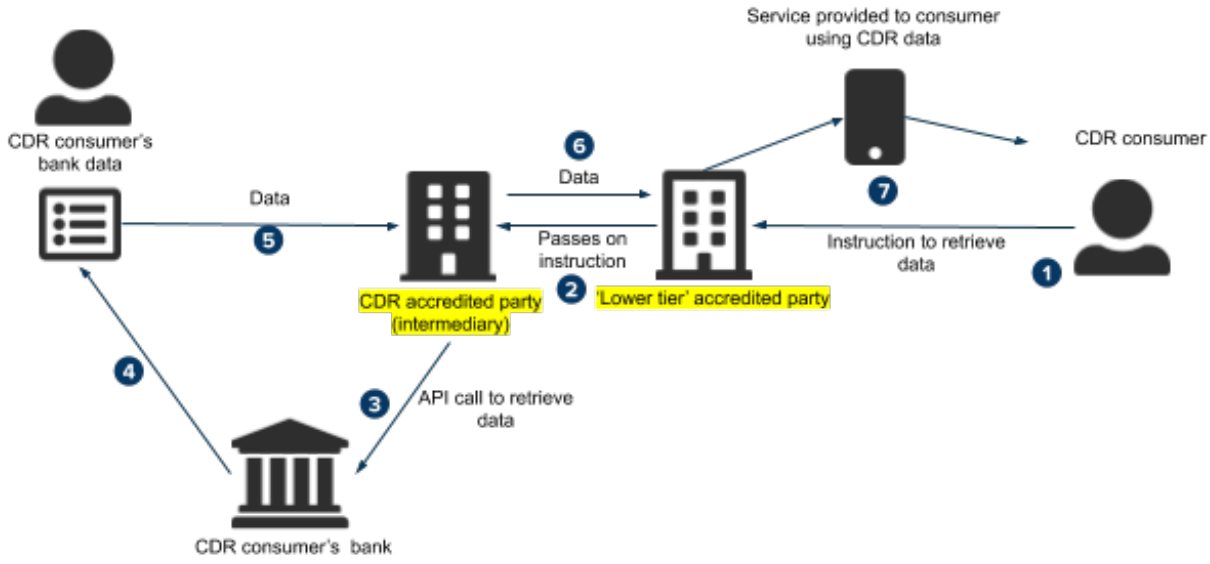
For the second proposed model, we believe that there are some parallels with the agent/principal model adopted in the EU under PSD2. In the EU, TrueLayer acts as a regulated account information service provider ("AISP") in its own right. Typically, we partner with 'agents' who provide account information services ("AIS") on behalf of TrueLayer. This model enables many innovative companies to enter the market and develop their products. It also enables companies for whom AIS is not a main activity to offer these services, without being directly regulated. In this model, under EU rules:

- TrueLayer is regulated under PSD2 for the provision of the AIS.
- TrueLayer can be the controller or processor in relation to the data, depending on how the service is provided via its agent.
- The customer has a right of redress to TrueLayer, rather than to the agent. It must be made clear to the customer who the principal is in the service i.e. TrueLayer.
- TrueLayer is responsible for ensuring its agents comply with the regulations. The agents are registered with the regulator.

However, we believe the Australian framework can improve on this model by defining a 'lower tier' of accreditation for smaller parties who are partnered with a fully accredited intermediary. The fully accredited intermediary would manage access to CDR APIs, and risks around the retrieval of data, and so would be the entity with the highest regulatory responsibilities. Therefore, the intermediary should obtain unrestricted level accreditation. The lower tier accredited party

would hold the relationship with, and the right to be instructed by, consumers, so must be subject to regulations regarding their interaction with clients and consumer consent. This would make things clearer for consumers than in the EU, where it can be confusing to have to consent to a Principal, when the service is (from the customer's perspective) being provided by the agent.

Figure 2. Illustration of a lower tier accredited party partnering with a fully accredited intermediary



An example use case of the model above is where a firm which offers accounting services wants to offer the consumer the possibility of aggregating all of their accounts in one place. These services are only a small part of the accounting firm's business model, and so obtaining unrestricted accreditation may be disproportionate to the anticipated level of use of CDR data.

Benefits of the lower tier of accreditation model:

- This model allows for a setup where the intermediary takes on the liability and obligations of full accreditation as opposed to the potential clients, who in many cases will be smaller firms, startups, or for who the data service is a small part of a larger offering, and for whom full accreditation may be prohibitive for market entry. This carves out a space in the market for innovators to provide a CDR data service before deciding whether they want unrestricted accreditation in their own right.

- This therefore decreases barriers to entry to the market, and creates more competition, which ultimately is good for consumers.
- With the intermediary's clients still subject to lower tier accreditation, consumers retain CDR rights, and can expect that their data will be managed and stored in compliance with the CDR regime. Complaints to lower tier accredited parties will also have to follow the CDR complaints process.
- The clients of the intermediaries handle the relationship with consumers, including instructions/ consents and requests to delete data. The client then passes those instructions/ consents or deletion requests to the intermediary to action.
- Since the clients remain subject to the requisite obligations of their own accreditation (unlike 'agents' in the EU, where full liability lies with the principal), they would be able to have the freedom to innovate their own products with the CDR data provided by the intermediary. This avoids the pitfalls of the agent/principal relationship in the EU, where clients are required to distribute the product of the principal with limited room for customisation.

Model 3 – Sharing data with non-accredited party

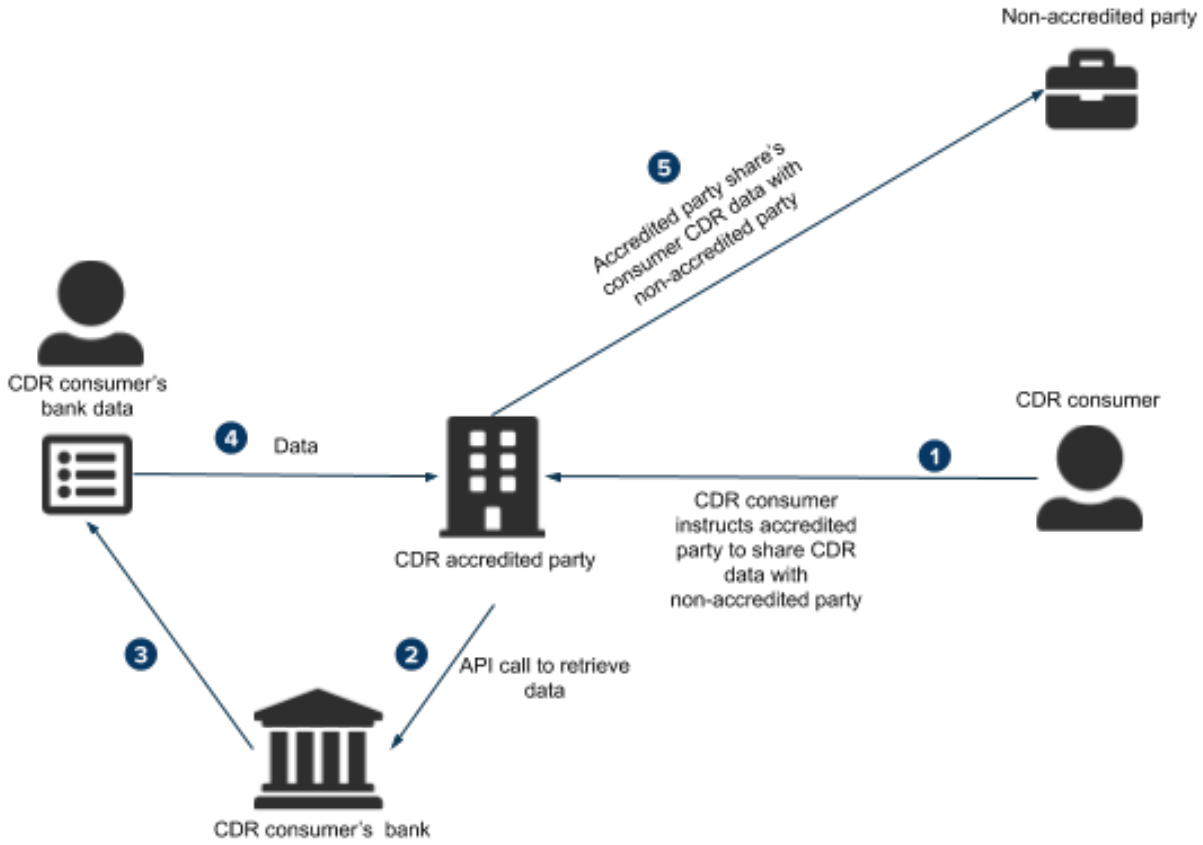
In the third model, we believe that once the CDR data has been retrieved from the source (the data holder) with the customer's explicit consent and instruction, a consumer should have the freedom to choose what happens next with their CDR data. This includes the right to instruct the accredited party to share their data with a non-accredited party.

In this model, the intermediary responsible for retrieving the CDR data would be required to have unrestricted accreditation[1], in line with our view that the retrieving party should have the highest regulatory responsibilities. However, with the explicit consent of the consumer, the accredited party would be able to assist the consumer with sharing their CDR data with an unregulated third party. CDR rules would need to be amended to permit the intermediary to disclose the CDR data to a third party, with the explicit consent of the consumer.

The differences to model 2 - 'lower tier accredited provider' - are that the consumer cannot instruct the non-accredited party to retrieve the data. The non-accredited party must pass the consumer to the accredited party in order for the consumer to instruct the accredited party to retrieve data or to pass on data it has already retrieved. Secondly, once shared with the non-accredited party, the data would be classed as having passed outside of the 'CDR perimeter'. The consumer would not have the same CDR rights in respect of the non-accredited party's use of that data. However, the non-accredited party should still have to comply with its obligations under the Privacy Act 1988, and the Australian Privacy Principles.

[1] Therefore we believe that entities with lower tier accreditation should not be able to pass CDR data to unaccredited third parties.

Figure 3. Illustration of a consumer instructing an accredited party to share data with a non-accredited party



An example use case of the model above would be an accredited intermediary such as TrueLayer, at the request of a consumer, passing CDR data to a credit-scoring company such as Experian. Experian would not itself present that data to consumers, but would use it to calculate an accurate and up to date credit score based on the users banking activity.

Benefits of allowing an accredited provider to share data with a non-accredited provider:

- Individuals with CDR data rights have the right to elect with whom they share their data.
- The intermediary remains fully accredited by the ACCC, and therefore subject to the CDR obligations, including the Privacy Safeguards.
- The intermediary is required to ensure the customer is clear about their rights once data is passed to a non-accredited party.
- The intermediary can facilitate 'data minimisation'. Having retrieved the data via API, the intermediary can assist the consumer to share only specific parts of their data with the non-accredited data (rather than sharing wholesale, as happens with screen-scraping, or sharing bank statements, for example).

- Privacy obligations imposed on companies with regards to data sharing are not unbalanced between those receiving CDR data and those that receive data from other sources, such as screen-scraping, PDF upload, or non-CDR APIs.

What obligations should apply to intermediaries if they are regulated under an accreditation model?

As noted above, we believe that intermediaries should be subject to the same obligations as other accredited persons if they wish to have unrestricted access to CDR data. This is because, in our view, the party responsible for the retrieval and transmission of CDR data should have the highest regulatory responsibilities. However, we note that in our proposed first model, intermediaries would not require accreditation when acting as an outsourced provider on behalf of an accredited third party. In that regard, the accredited third party would have to ensure the outsourced provider's compliance with the CDR regime.

We also wish to highlight that if the regulatory burden on intermediaries and their clients is too high, this may create an imbalance with other FinTech companies. In particular, intermediaries who opt to use 'screen-scraping' techniques, as opposed to CDR APIs do not have to comply with the requirements of the CDR regime, including the Privacy Safeguards. Excessive regulatory restrictions for accessing and sharing CDR data will harm the adoption of CDR APIs, and the success of Open Finance in Australia.

How should contractual obligations be regulated between accredited persons and intermediaries if they are regulated under an outsourcing model?

As noted above, if an intermediary acts as an outsourced provider to an accredited person, by providing the technical means to access CDR data APIs, we are firmly of the view that this intermediary activity should not be regulated. Rather, the fully accredited party which is outsourcing to the technical service provider should be responsible for ensuring its outsourcee enables it to be compliant. The ACCC may wish to issue some form of outsourcing guidelines (similar to those issued by the EBA in Europe) which detail how an accredited person should oversee an intermediary that is providing outsourced services to it.

Should the obligations differ depending on the nature of the service being provided by the intermediary?

Yes. We have set out our views on the obligations by service type in our answers above. Broadly speaking, we are of the view that obligations should decrease the further away a person is from retrieving the CDR data. This is because we are of the view that the data retrievers bear a large amount of responsibility for ensuring safe retrieval, storage and transmission of the data, and should be regulated accordingly. In addition, Australia already has existing privacy principles regarding the sharing of data, and we do not believe the CDR regime should create a regulatory

imbalance between those who use that regime to access data, as opposed to other methods of gathering the same information, such as screen-scraping.

How should the use of intermediaries be made transparent to consumers?

TrueLayer is in favour of ensuring that consumers understand who is accessing their CDR data and in what capacity, especially where the actors have obligations towards the consumer:

- **Model 1** - Where an intermediary is purely an outsourced provider, the role of the provider should be dealt with in the terms of service of the accredited provider. It is not necessary (and may indeed be confusing) for the consumer to be told upfront (i.e. in consent screens) about the role of an outsource provider, in the same way that it would be if banks had to explain to consumers upfront that their apps are powered by Amazon Web Services. However, the terms should explain that the outsourced provider does not store data.
- **Model 2** - Similarly, since a lower tier party would bear regulatory obligations for ensuring consumer rights, and would ultimately hold the consumers data, once it has been retrieved by the fully accredited party - the consumer should mainly be made aware upfront of what the lower tier party will use the data for, how long they will store it for, and how to request that the data is deleted. For the role of the intermediary, we suggest that lower tier parties would explain the role up front (e.g. in consent screens) in terms of a partnership. For example, “We provide this service by partnering with TrueLayer, which is fully accredited to securely retrieve your data”. The role of the fully accredited party would need to be further explained in the lower tier accredited party’s customer terms.
- **Model 3** - Where a customer wants to share their CDR data with a non-accredited party, the non-accredited party would need to pass the consumer to the accredited party, so that the accredited party could be instructed to retrieve the data, and release it to the non-accredited party. The onus would need to be on the accredited party - i.e. the intermediary to make very clear to the consumer that their data is being shared outside the protections of the CDR regime, and obtain the explicit consent of the consumer to proceed.

That being said, we wish to highlight that if the transparency requirements under the CDR are very onerous while companies who use screen-scraping based solutions can continue to build very seamless journeys, then adoption of CDR APIs may not succeed.

Complex messaging in consent journeys has also been found in the UK to reduce customer take-up, and it was only through industry feedback (such as TrueLayer’s analysis of the consent journeys of the big 9 banks in the UK) and increased regulatory pressure that the consent journeys were improved to a satisfactory level. Following the introduction of seamless consent mechanisms such as ‘app-to-app authentication’, conversion rate of Open Banking connections is now at over 70%.

How should the rules permit the disclosure of CDR data between accredited persons?

We question the need to have additional rules regarding the disclosure of CDR data between accredited persons. In this scenario both parties are subject to:

- ongoing compliance with the CDR rules to maintain their accreditation;
- the Privacy Safeguards; and
- if relevant[2], their obligations under the Privacy Act and the Australian Privacy Principles.

In all circumstances, provided that the CDR data is:

- sent via secure channels;
- only shared with the explicit consent of the consumer; and
- deleted if the customer has requested it to be;

we do not believe additional rules are warranted. This would ensure that the sharing of CDR data remains in line with the sharing of data obtained by other means, for example when using screen-scraping techniques.

As noted above in our model 1, we can see a business model where an intermediary provides outsourced technical services to an accredited person, and we believe that in this scenario the intermediary does not need to be accredited. That being said, if the intermediary is accredited (as it offers multiple services – i.e. all of our proposed business models), we do not think this warrants increasing the regulatory burden on them for sharing CDR data.

Should the creation of rules for intermediaries also facilitate lower tiers of accreditation?

Yes. We have outlined our views above with regards to offering the ability for clients of intermediaries to have the option of being subject to 'lower tier' accreditation. As noted above, we believe that regulatory obligations for the lower tier accreditation should focus on consumer facing activities, consent, and disclosures.

If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used?

The key differences between full accreditation and lower tier accreditation have been explored in the illustrations above. We believe that unrestricted accreditation should have the highest liability attached to it. The diagrams used above to explain our three proposed models detail where the liability lies in each model. We believe that if an entity is subject to lighter touch accreditation, its

[2] Subject to Section 56EC CCA

activities should be overseen by an unrestricted accredited person, as in our first model detailed above.

In sum:

Fully accredited party	Lower tier accredited party
Has unrestricted access to CDR APIs	Has indirect access to CDR APIs via fully accredited party
Compliance with all CDR rules	Compliance with CDR rules relating to obtaining customer consent/handling instructions for access/ deletion
Can be instructed directly by a consumer	Instructions are passed to a fully accredited party
Oversight of lower tier client's security and data storage obligations	Responsibility to its intermediary for compliance with CDR obligations
Ultimate liability for clients – both regulatory, and for customer redress (e.g. compensation)	Responsibility for handling consumer complaints and consumer queries
Can, at customer's instruction, share CDR data with a non-accredited party	Cannot share data with a non-accredited party

Consultation questions on permitting CDR data to be disclosed to non-accredited third parties

What are the goods and services that may be provided by a non-accredited third party which will require receiving CDR data, and how may they benefit consumers?

There are many possibilities for the types of goods and services that could benefit from CDR data, and the nature of innovation is such that we will not be able to predict every smart new way that the data might be used to benefit Australians and the economy.

In our EU experience, here are some of the innovative ways in which companies in Europe are using OpenBanking data:

- Using a tenant's transaction history to confirm that they are making rent payments regularly, and feeding this information back to credit bureaus, thereby improving access to credit and pricing, especially for younger and so-called 'thin file' consumers.
- Credit scoring companies, such as Experian.
- Making income verification smooth, by allowing lenders to access their applicant's transaction history.
- Essentially any company that, today, is using screen-scraping based access could fall into this category (or, avoid CDR API based access if it would require them to become accredited and this comes with too many hurdles).

What are the goods or services that may be provided by an accredited person who discloses CDR data to non-accredited third parties and how may they benefit consumers?

As with the above question, the goods and services that could be provided are wide. We would recommend not regulating this in a prescriptive manner attempting to be exhaustive, as this may stifle innovation. Accredited intermediaries are typical examples of this type of firm, and we discussed the benefits of intermediaries in our earlier responses. For firms such as TrueLayer, by offering a product which allows third parties to access CDR data, without having to build and maintain the technical infrastructure, the possibilities for our clients are endless. By utilising our service, they can focus their efforts on designing and building new products, for the benefit of their customers.

What types of non-accredited third parties should be permitted to receive CDR data?

We recommend an approach that is not highly prescriptive about the types of firms that can receive CDR data, but that the CDR regime should instead leverage and builds on existing, Australia-wide, data protection and privacy legislation, such as the Privacy Act and the Australia Privacy Principles.

Due to the sensitive nature of the data that is being shared, it is important that:

- the consumer knows that their data will be shared, and with whom;
- there is a process in place for the accredited person to request the deletion of any data that was shared (within the existing data protection and privacy laws); and
- the non-accredited third party adheres to Australia's existing data protection laws.

Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?

In the proposed model above, a layer of protection is being built around the 'retrieval' of CDR data. Highly regulated parties are being given the ability to retrieve the data in a safe, secure manner with regulatory oversight. The data is also being retrieved in a consistent and organised fashion - via APIs, which will allow for granular consumer control over the data, rather than the data being extracted wholesale as with screen-scraping.

Once data has been retrieved in this fashion, by regulated parties, the consumer is fully in control of their data (and should be able to use it as they see fit). Should they wish to share it with parties outside the CDR regime, the accredited party which holds the data will enable them to control what is and isn't shared.

In sum, since controls and protections exist around the retrieval of the data, much of the risk of uncontrolled and uninformed data sharing is mitigated. The party retrieving the data will also be subject to the Privacy Safeguards.

Furthermore, we note that, less secure methods of access to banking data such as screen-scraping will continue to exist without the need for accreditation (or even a simple registration), which creates an imbalanced and unfairly burdensome regulatory environment for accredited persons that will only disadvantage the uptake of CDR APIs. Data gathered through screen-scraping and other methods can be disclosed to any party, whether accredited or not.

While we have made our views clear that third parties should not need to be accredited to receive CDR data, the ACCC may want to consider a similar model to Japan if it wants oversight on the types of firms using CDR data. This would be to have a simple registration of any person that wants to receive CDR data, accessible on a public register.

As noted throughout, we are of the view that only parties that take instructions directly from the customer to retrieve data (either directly or indirectly) should be accredited.

What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?

As noted earlier in this response, we recommend an approach that is not highly prescriptive but instead leverages and builds on existing, Australia-wide, general data protection and privacy regulations. This ensures that there is no regulatory imbalance between the sharing of CDR data and other techniques such as screen scraping.

What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party?

As we have noted earlier in our response, TrueLayer is in favour of a high level of transparency with consumers, with the default situation being a requirement for explicit consent and the role of each party in the process being made clear to the consumer.