Inquiry into future directions of the Consumer Data Right

TrueLayer response, 20th May 2020

Dear Treasury

Thank you for the opportunity to comment on the potential future directions of the Consumer Data Right ("CDR"). We are excited by the potential for the CDR to become a leading framework for putting consumers in control of their data, and who can access and act on it, and look forward to the Inquiry's outcomes.

About TrueLayer

TrueLayer is a UK-headquartered firm, founded in 2016 and authorised by the UK's Financial Conduct Authority ("FCA"). Our platform 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, corporations and merchants. We enable them to build novel, seamless user journeys and products, such as receiving banks transfers for payment and account top-up. We also help them 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 our first expansion 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 policy discussions since then.

In 2020, we intend to bring our API-based Open Banking platform to Australia to help local and international companies to build better experiences for their customers - all with the appropriate consents and data protection in place. We will also 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 Finance 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 some of our key points, which are:

- **Write access, and especially payment initiation, will be transformational:** our experience in Europe shows that, once write access is in play, the possible use cases multiply. The promise of more efficient, more direct, lower cost payments provides benefits to both merchants and consumers, and can benefit the whole economy by creating efficiencies in payments in a safe and secure manner. Write access for account opening and closing will incentivise consumers to switch accounts and consider the wide variety of products in the market.
- **The CDR as Australia's equivalent to the GDPR:** currently, the Privacy Safeguards that apply to data obtained via the CDR ecosystem are in addition to the existing Australian Privacy Principles ("APPs"), which may create regulatory discrepancies and additional complexity for both consumers and industry. The CDR could become the centralised piece of legislation to govern how consumer financial data should be handled.

Finally, we understand that the Inquiry is focused on future roles that could be performed by the CDR, future outcomes which could be achieved, and what is needed for this to happen. While we have tried to not focus heavily on the current progress of the CDR and its expansion to specific new sectors, our response does refer to these areas where necessary to give context for some of our suggestions for future directions.

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

TRUELAYER LIMITED

ANNEX - INQUIRY QUESTIONS

Future directions and outcomes of the Consumer Data Right

Which future roles could be performed by the Consumer Data Right, which future outcomes could be achieved, and what is needed for this to happen?

The CDR is a strong move in favour of giving consumers more control over their data and who can access it. This means that any industry with large volumes of data in play could be targets of future iterations of the CDR, for instance social media. As was previously provided for the banking, utility, and telecom sectors, it would be paramount to provide clarity on the outcomes the CDR aims to achieve by expanding its reach. To that end, it would be useful to explore some products or services that could be offered on the back of these new datasets, but without pre-empting the creativity of the market in terms of what may be possible.

Further, as the CDR expands across multiple industries and imposes data protection rules and standards on its participants, it could take on a similar role to the GDPR in Europe, i.e. centralising all rules around how a consumer's data should be handled by a company. This would require the consolidation of the existing Privacy Principles and local state legislation into the CDR regime. However, in the long run, the benefit would be that all firms who collect, store and use consumer data would be subject to the same data standards across Australia, which will improve and enhance competition both for local companies, and incoming international firms.

The alternative approach would be to align everything under the existing Australian Privacy Principles and an updated Australian Privacy Act. As it stands, the disparity in the treatment of CDR data compared to non-CDR-sourced data could create a possibility of regulatory arbitrage which could hinder the adoption of the CDR by industry.

International Context

How can the Consumer Data Right be leveraged with international developments of similar kinds to enhance opportunities for Australian consumers, Australian businesses and the Australian economy?

An increasingly mature market for open banking services is emerging in the EU and especially the UK as a result of the Second Payment Services Directive ("PSD2"). It is clear that the ACCC has already taken learnings from experiences in this jurisdiction to aid the development of the CDR.

Further steps for the CDR

We see that in our client base already, an increasing number of firms are looking to use our platform across both Australia and Europe. To leverage this latent demand, and enhance opportunities for Australian consumers and businesses, the following further steps could be taken:

- Allow third party providers already authorised in the UK by the FCA, to passport to Australia under this authorisation, or undertake a lighter authorisation, recognising the due diligence that has already been done by UK authorities.

More than 200 open banking businesses have passed the scrutiny of the FCA to become authorised open banking providers. Allowing these firms to undergo a streamlined authorisation as accredited parties in Australia would hugely accelerate their route to market in Australia. These firms would inject competition into the Australian market, furthering innovation for the benefit of consumers and the wider economy. A reciprocal arrangement could be reached with the UK authorities.

- Bring payment initiation into the scope of CDR

While Australia's CDR sets high ambitions on the range of industries covered by it, it does not yet include write access so that third parties can initiate payments on behalf of customers. In Europe, payment initiation was introduced from the outset under PSD2, and this approach has been adopted in other jurisdictions such as Canada and Brazil. We find it present in many regions with a focus on creating higher efficiency and lower costs in the payments infrastructure of the country.

- Alignment on international standards

Secondly, the CDR regime could make its standards more accessible to international companies by accepting globally used standards. This is being discussed in a number of conversations surrounding international FinTech bridges. As a concrete example, accreditation as a CDR participant currently requires an ASAE 3150 security audit, which incurs a large expense for both national and international firms. Instead, more commonly held similar certifications may be considered by the ACCC (such as ISO 27001 which is a commonly accepted security standard in Europe).

Lessons from counterparts

The CDR regime can also learn lessons from its international counterparts. We have listed some of them below.

- Clarity for firms wishing to move towards secure methods of access via API

We believe access to financial data via APIs provides huge advantages in terms of efficiency for market participants, and user experience and security for consumers. In particular, APIs enable data minimisation, giving customers granular control over what information they are sharing, as opposed to screen scraping, where providers retrieve data in a drag-net fashion.

In the UK, the major banks who cover over 80% of accounts (the 'CMA 9') were required to provide APIs for data access. Moving the critical mass of banks onto this form of access is one of the reasons Open Banking has taken off in the UK.

On the other hand, where banks outside the CMA9 had the optionality to continue forms of screen scraping, we have seen large high street names, such as Metro Bank and the Cooperative Bank, choose to retain them over APIs, to the detriment of their customers. It is not feasible for third party providers to maintain both API and screen scraping connectors.

Additionally, PSD2 provides that banks opting to enable access via APIs are allowed to block screen scraping third party providers. This further incentivises banks and data holders to move towards the more secure method of access. The EU regulation gave clear deadlines for when screen scraping could be blocked by banks with performant APIs.

We believe the CDR regime should provide similar clarity on APIs as the preferred method of access and enable data holders who have built performant APIs to block screen scraping.

- Don't fix data standards in legislation, ensure room to manoeuvre

Finally, despite the higher clarity surrounding 'screen scraping', one learning from the EU experience was that the newly introduced APIs often did not provide the same information as informal methods. This created a disincentive for FinTechs to use the more secure method, and has required a significant amount of industry collaboration, negotiation, and regulatory involvement to bring it up to par. The CDR can avoid this by having an effective mechanism for enhancing the CDR Data Standards, including mandatory and optional fields, in a timely fashion if it emerges that the information available is not adequate to replace 'screen scraping' and other methods. In the EU, many technical API and data requirements are set in legislation, making the process for change slow and restricting innovation. Open Finance conversations are ongoing,

building on these learnings and aiming to plug unintentional 'data gaps'. We have written about these and other lessons learnt from Open Banking and PSD2 here[1].

How could the Consumer Data Right be used to overcome behavioural and regulatory barriers to safe, convenient and efficient switching between products and providers?

One of the largest barriers to switching between products and providers is customer inertia, and a lack of ability to see in practice what the benefits of switching will be. Price comparison websites have significantly improved switching across a number of industries but have yet to make a bigger impact for more significant commitments, such as home loans or investments.

The CDR could be used to develop services that make the switching options clear based on a consumer's actual circumstances and behaviours, and in the future (with write access) actually automate the switching process in a safe and secure manner. For example, an app could use CDR data combined with credit reference data to show a customer the best mortgage available to them, taking into account their monthly income and expenditures, and then allow for seamless refinancing with the new provider through an account opening API.

In providing APIs that can both open and close accounts, the CDR could enable companies to build great switching experiences, and drive innovation and competition across the market. It will also ensure that a consumer's current provider genuinely considers (on a regular basis) whether the product is the right one for them. Using APIs to enable switching ensures that customer data is being shared and stored securely between companies, the risk of manual errors is reduced, and consumers have to do less work, combating inertia.

Introducing an intermediaries regime to the CDR will also remove some of the regulatory barriers for the creation of new switching services. Some of the most innovative and consumer-friendly products (i.e. those that will harness CDR read-data to show customers the real financial benefits of switching) are often developed by innovative start-up companies. In using intermediaries, those companies will be able to avoid the significant costs associated with becoming accredited in their own rights on day one, freeing up funds to bring their products to market quicker for consumers, while still maintaining integrity and security through the intermediary's infrastructure and their ability to stand in for their smaller customers in the case of a breach (as is the case with other areas of the financial services sector where firms operate under another firm's license in a

[1] TrueLayer blog post "Three lessons for Open Finance" https://blog.truelayer.com/three-lessons-for-open-finance-7b011194da5f

principal-agent relationship). We outlined our suggestions on this topic in our response[2] to the ACCC's consultation on intermediaries.

Read access

What is the potential to develop a 'consent taxonomy', using standardised language for consents across providers and sectors?

We consider that defining the outcomes and metrics for successful consent is more important than defining the exact standard language. We believe that the ACCC and the Data Standards Body already provide guidance on what explicit consent means[3]. Beyond the standardisation of the language to describe Data Clusters, as is already provided by the Data Standards Body's CX Guidelines, additional formalisation of consent taxonomy could stifle creativity, and the ability for firms to optimise the way consent is captured as the market grows and technology develops.

However, we do believe that there may be potential to standardise both how and which specific consent data and 'metadata' is captured, and how to monitor that consumer outcomes are being met. Standardising consent data capture ensures an audit trail – allowing both for accurate tracking of consumer consents and resolving disputes. Capturing data to monitor consumer outcomes will allow the Regulator to effectively supervise accredited persons, and data holders, as well as assess trends across sectors.

How could the CDR best enable consumers to keep track of, and manage, their various consents?

We consider that the CDR has taken the right first steps towards a framework for consumers to be able to keep track of and manage their consents, through the requirement for 'CDR receipts' and the consumer dashboard required of Data Recipients and Data Holders.

An often-mentioned opportunity is a consolidated single consent dashboard, which aggregates a user's consents across a range of providers (no single provider can currently give a consumer a holistic view of their data sharing). As more sectors of the economy are covered by the CDR and its central infrastructure and accreditation system, there may be an opportunity to enable this from a technical perspective.

---

[2] TrueLayer's response to the consultation on intermediaries is accessible on the ACCC's website here: https://www.accc.gov.au/system/files/CDR%20rules%20-%20intermediaries%20consultation%20submission%20-%20TrueLayer.pdf

[3] Similar to that provided by the FCA in the UK: See section 17.55 https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

One possible solution would require all accredited persons to share CDR consent information/metadata, and to put 'consent information' on the list of designated data that needs to be made shareable, i.e. via APIs.

This would likely also require a standardised way to link consent metadata to a user identifier, to tie all the consents together.

In previous examples of companies trying to develop these kinds of tools, it so far seems that consumers do not feel enough inconvenience in managing their consents to create a viable business model for these companies. That said, the CDR could provide this opportunity quite organically, and we would be interested in the prospect of a single consent dashboard.

How could the creation of a safe and efficient ecosystem of participants and service providers be accelerated?

We firmly believe that the CDR is the safest and most efficient way to retrieve customer data, and we intend to apply for unrestricted accreditation as a data recipient. However, we expect that the CDR regime will not be as fully adopted by participants while alternative data gathering methods, such as 'screen scraping', are available to them.

In particular, there are limited incentives for firms to take steps to get accredited, and comply with the wide-ranging CDR rules, when they can obtain largely the same (and often more) data in a less secure, unaccredited manner (and therefore at a reduced cost). As a result, we believe that to accelerate the uptake of the CDR, Australia should prohibit the use of less secure methods of gathering data, including 'screen scraping', and focus on enhancing the CDR data standards rapidly should it emerge that the currently mandatory data is not adequate for use cases previously serviced by alternative data capture methods.

In addition, at present the ability to build and test APIs within the CDR regime is limited to a small number of participants. New participants will not have access to the testing environment until they become accredited, which for intermediaries is at an as yet undetermined date. We believe, to encourage firms to begin to work on APIs, that participants should be able to test APIs without full accreditation. We consider that there is minimal risk attached to this, as participants will only have access to a testing environment, and not live data. This is already permitted under PSD2 in the EU.

As we mentioned above, we also believe that the introduction of a clear intermediaries regime will greatly speed up the creation of a thriving CDR ecosystem.

Finally, to incentivise firms to move to using CDR data, Australia could consider creating a prize similar to the Nesta Open Up challenge[4]. This would encourage firms to innovate and create products that would use CDR data.

What is the scope of tiered accreditation to promote broader access without increasing risk?

As outlined in our submission to the ACCC regarding the role of intermediaries, we believe there are scenarios where requiring a business to get full accreditation to access CDR data will be prohibitive and detrimental to uptake. For example, we noted that the cost of full accreditation may be a barrier to entry for small businesses. In the FinTech industry, these small start-ups tend to be the most innovative, building applications that deliver great outcomes for consumers. However, their financial resources tend to be limited, and therefore the significant expense relating to accreditation may result in fewer new products for customers. Giving these companies an ability to prove that their products can work will allow them to raise additional funding (or sustain through revenue) and possibly obtain their own direct accreditation in due course.

We fully support the use of intermediaries and recommend the introduction of a tiered system to accreditation (including allowing intermediaries who are accredited to pass CDR data to third parties). Tiered accreditation would allow for the consumer benefits of the CDR such as liability and complaints handling to be retained, while allowing larger firms to take on the responsibilities of a fully accredited person, while bearing the greatest risk. Smaller firms could access CDR data through an intermediary (without having direct access to the APIs) with the consent of the consumer.

Tiered accreditation could also include a tier which requires registration, rather than accreditation (akin to the Japanese Open Banking regime). This means that consumers would still be able to see who is "on the radar" of the ACCC.

Are there any other areas of 'read' access that should be considered?

In addition to Banking, Utilities, and Telco, we suggest at minimum the areas of Insurance, Investments, and Superannuation be added to the scope of the CDR. The international

[4] Nesta's Open Up Challenge is a £1.5m prize fund to unlock the power of open banking for UK consumers: https://openup.challenges.org/

conversation on this topic is running under the title Open Finance, and we have provided extensive input[5] in other jurisdictions, including the UK.

Write Access

How could the Consumer Data Right best enable payment initiation?

Write access to the CDR is essential to providing a real alternative to card payments, and to increase competition in the payments sector. It is a key area of growth for our platform in Europe and we are seeing innovative use cases where merchants who previously relied on debit/credit card payments are making use of this cheaper, faster, more direct and secure alternative to enable online payments.

Figure 1: Comparison of a card scheme system vs. a payment initiation system

We believe that the CDR is an ideal place to implement payment initiation write access (as opposed to linking it directly to the NPP). The CDR should draw inspiration from global Open Banking regimes when considering payment initiation, for example considering how it has been introduced in Europe or is proposed to be introduced in Brazil.

[5] TrueLayer's response to the FCA's call for input on Open Finance is summarized in this document: https://cdn2.hubspot.net/hubfs/3954168/FCA%20Call%20for%20Input%20-%20Open%20Finance.pdf

A key point from these implementations is that payment initiation should be a stand-alone feature of an Open Finance system. I.e. it should require banks to provide the ability to initiate payments as if they were being initiated by a customer via an API call, but, crucially, be agnostic to the requester of the payment (e.g. the merchant or the technical service provider) being a member of any underlying payment scheme, or being plugged directly into the payment system and infrastructure.

In other words, we believe that payment initiation should sit on top of payment schemes such as the NPP, and interact with those systems as and when required, as opposed to being a feature that is directly linked to the underlying rails. Payment initiation services would simply stand in for the customer in instructing the credit institution to make a payment and should not tie the customer to a specific payment scheme. Payment initiation services should sit in an 'instructing' layer above the underlying inter-bank payment infrastructure.

However, when taking inspiration from global regimes, the CDR should also learn lessons from their implementations too. In particular, in Europe, payment initiation does not allow for variable recurring payments, or for refunds. Therefore, payment initiation as a product is more challenging for a merchant to adopt. While they benefit from reduced payment fees and faster settlement, they are unable to use the same method to refund the customer as and when required, which increases costs and complexity for the merchant. The CDR should therefore consider adopting write access which allows for two-way transactions.

In Brazil, the proposed Open Banking mandate also allows for customers to make variable recurring payments using payment initiation, and it has specifically altered consent and authentication rules to take into account this situation. The CDR should adopt a similar model. Without this, payment initiation would not offer a real alternative to cards.

In summary, key points to learn from other markets are:

- **Allow for two-way payments**, to enable refunds for merchants easily
- **Enable multiple payment methods**, especially recurring payments with fixed and variable amounts
- **Reduce execution risk or uncertainty**, by ensuring the payment initiation service provider can receive updates on the successful execution of the payment from the bank
- **Align and synchronize consent journeys** between read and write access so as not to require multiple disjointed authentication journeys, and to unlock the promise of lower fraud rates and better AML

- **Keep payment initiation separate from the underlying payment scheme**, and do not require the requester of the payment or the technical providers to be members of the scheme

Who should bear responsibility for payments made, and for changes made to data?

The CDR should take inspiration from global Open Banking regimes, including PSD2 in Europe. Under PSD2 the liability regime is geared so that when there is an unauthorised payment, whether it was initiated directly by the customer via their banking portal, or indirectly via a third party, the customer can always go to their bank to request a refund or recompense. This maintains simplicity and consumer protection for the customer.

The bank then has a right of redress to claim compensation from the TPP, if the issue leading to the unauthorised payment is found to have been in the sphere of control of the TPP.

This approach keeps the customer away from the complexity of liability discussions between banks and TPPs but enables banks to be put right where the unauthorised payment is not their fault.

For changes made to data, in the case where an accredited person has amended data in accordance with the instructions from the customer, it should be the customer who bears responsibility for erroneous changes. However, if the accredited person has in any way altered the amended data, or failed to carry out the amendments requested, then it should be the accredited person who is liable for the changes. Further, if the data holder fails to amend the data in accordance with the amendment request via a CDR API, then it should be the data holder who bears responsibility.

Should write access extend to the ability to change details which identify a customer (and if so, how could any associated security risks be minimised)?

We believe that write access should extend to the ability to change customer identification details, as it is in the interest of consumers to find efficient and secure ways for them to update their details if required. This is also especially important if the CDR expands write access into more use cases, such as account opening and closing, or switching. Where write access is used to change identifying details, we would recommend that changing such details requires additional consent and authentication from the customer, for example two factor authentication.

We believe that the CDR controls for the security risks. The current rules already require directly accredited participants to adhere to strict security and data standards, and this should be no

different in respect of write access. The rules should perhaps address what level of checks and controls an accredited person should have in place for updating customer identification details, including by leveraging existing customer due diligence requirements for know-your-customer and anti-money laundering.

Linkages and interoperability with existing frameworks and infrastructure

How could the Consumer Data Right, were it expanded to enable write access, relate to or interact with existing and future payments systems and infrastructure, such as the New Payments Platform (NPP), Bulk Electronic Clearing System, and EFTPOS?

In our view, write access to the CDR should be a stand-alone feature (given its various potential uses) which is separate to existing payments infrastructures. However, it should be able to interact with those systems as required.

For example, if write access is used for payment initiation, it should be able to 'plug-in' to the NPP and allow the payments that have been initiated by the customer to be conducted across the NPP. For many firms, accessing the NPP can be expensive, with significant regulatory requirements attached to it. This can be a barrier to market entry, and limit competition and innovation. Allowing for write access CDR data to plug into NPP (without requiring direct participation) will remove some of those barriers and bring faster payments to a wider set of companies across Australia, ultimately benefiting end users.

We believe that one of the benefits of Open Banking, and specifically payment initiation, which could be achieved through write access CDR, is the ability to move away from card payments and the associated costs. This benefits both the consumer and the merchant, who will avoid the high costs of debit and credit card transactions. As a result, we do not see any direct need to write access CDR to integrate with EFTPOS (even though it charges lower fees than schemes such as Visa and Mastercard). Write access CDR can, for example, be tied to an app on a customer's phone, eradicating the need for carrying a payment card.

Are there any accreditation frameworks that focus on data risk management which should be recognised within the CDR?

As noted above, we believe that the CDR should leverage other international authorisation and accreditation frameworks, and standards which are required to have been met in those jurisdictions. This will drive international expansion, foster innovation and provide a better end

experience for consumers. It might also remove some of the accreditation costs which pose a barrier to smaller start up's or sole traders. For example, consideration should be given to:

- Accepting ISO27001 certification within the accreditation regime of the ACCC (or alternatively being standard agnostic).
- "Passporting" of an equivalent license from other regions (e.g. for read access to CDR data, considering firms that have been granted licenses as Account Information Services Providers in the UK and Europe).
- Taking into account a firm's regulatory status as supporting evidence of a company's fit for purpose status, providing the ACCC have a right to consult international regulators.

Consumer protection

How can it be ensured that, as the Consumer Data Right develops, it does so in a manner that is ethical and fair, as well as inclusive of the needs and choices of all consumers?

We believe there are a number of steps which could be taken to ensure that the rights of the consumer are taken into account when developing the CDR:

- Consistently reviewing the CDR standards against alternative data gathering methods, ensuring that the CDR does not prohibit or restrict a consumer's right to (sharing) their data. In addition, thought should be given to prohibiting other less secure data gathering methods such as 'screen scraping', so that all companies offer consumers the same quality of data protection;
- Taking into account feedback and views from all relevant parties. To do this, the CDR should give all parts of the ecosystem a low-barrier way of providing feedback. For consumers, appropriate engagement mechanisms such as social media campaigns, surveys, video education and focus groups could be used, both to ensure that consumers know their rights, but also to understand their needs and perspectives; and
- Having a customer-facing website which is easy to understand - one example to review could be the UK's Open Banking portal: https://www.openbanking.org.uk/

What could be ways to encourage socially beneficial uses for the Consumer Data Right?

We believe there are many ways in which developers can use CDR data for social good, and we are already seeing examples of this in practice with our European based customers. For example, some are developing apps that use consumers' financial data to 'round-up' spends, donating the rounded-up amount to charity.

Others have developed apps that harness payment initiation to allow charities to benefit from removing the cost of credit card fees (for instance, https://donate.truelayer.com/ allows charities to get direct donations into their bank account at no cost during the COVID-19 pandemic). In addition, we see clients who help financially challenged customers improve their credit score or get access to financial products they might otherwise have been barred from.

To encourage socially beneficial uses of CDR data, it would be useful first to identify objectives (similar to the UN's development goals) which outline what ethical and fair means in the context of the CDR. For those that demonstrably contribute to these objectives, there could then be reward support, for example tax benefits or national recognition.