Westpac New Zealand Limited

Submission to Ministry of Business, Innovation and Employment
on
Open banking regulations and standards under the Customer and Product Data Bill

10 October 2024

1. INTRODUCTION

1.1 This submission to the Ministry of Business Innovation and Employment (**MBIE**) is made on behalf of Westpac New Zealand Limited (**Westpac**) in respect of *Open banking regulations and standards under the Customer and Product Data Bill* (**Consultation Document**). Thank you for the opportunity to provide feedback on the proposals.

1.2 Westpac's contact for this submission is provided separately.

1.3 Westpac refers to and supports the submission's made in the NZBA submission but would like to take this opportunity to focus on a number of key areas of concern to Westpac which are likely to:

a) put **customers** and their data at **increased risk** and **undermine trust and confidence** in the CDR Regime; and

b) **inhibit growth** and **innovation** in the **open banking ecosystem.**

1.4 Westpac continues to be concerned with the potential interplay of two regulatory regimes targeting open banking and in particular is concerned with apparent **inconsistencies** between the proposals under the Consultation Document and the Commerce Commission's recent recommendation to the Minister to designate the interbank network under the Retail Payment System Act (**Network Designation**). Westpac urges MBIE and the Commerce Commission to provide clarity as to their proposed respective roles and responsibilities as a matter of priority.

2. KEY SUBMISSIONS

Inconsistent treatment of intermediaries and Fourth Parties exposes consumers to risk

2.1 Westpac has significant concerns in respect of the Bill's differential treatment of intermediaries who initiate actions on behalf of another party (**Fourth Party**) and believes that this has significant potential to expose customers to unnecessary risk of harm and undermine trust and confidence in the Consumer Data Right (**CDR**) regime.

2.2 In this regard it is important to bear in mind that unlike many overseas jurisdictions, New Zealand does not have a broad financial licencing regime for providing financial services. Accordingly, many Fourth Parties may not be subject to any regulation or oversight by a regulator outside of the CDR regime and this introduces a level of risk to the open banking ecosystem which could undermine consumer trust and confidence.

a) Fourth Parties should be subject to the same accreditation requirements as intermediaries

2.3 The discussion paper proposes that where data is requested, or actions are initiated by an intermediary on behalf of a Fourth Party, only the intermediary needs to be accredited and not the Fourth Party who is the ultimate recipient of the data or party initiating the action. We do not believe that this is appropriate and have significant concerns with this proposal's potential to undermine trust and confidence in the CDR regime. This is also wholly inconsistent with Minister Bayly's desire "*to ensure that standards are set so that customers can be sure that their data is safe, and the parties*

that are accessing it are accredited as trustworthy, competent, and secure." (as stated in the foreword to the Consultation Document.)

2.4 Based on our understanding of the market, we believe it is likely that a significant number (if not a majority) of entities will choose to access customer data through an intermediary rather than doing so directly[1], meaning that *most customers* will face Fourth Parties rather than intermediaries. The reason for this is because of the efficiencies gained in indirect access through an intermediary rather than having to maintain separate connections with all Banks.

2.5 Notwithstanding the indirect access to customer data, Fourth Parties will be the ultimate recipients of customer data and will be the main entities with whom most customers will have their relationship with. In order for customers to have trust and confidence in the CDR regime, they will need to have confidence that the entities they are dealing with and to whom they are entrusting their data are trustworthy and have appropriate security measures in place.

2.6 For the above reasons, it is essential that Fourth Parties should be subject to the same accreditation requirements as intermediaries.

b) Relying on customer consent places vulnerable customers at risk

2.7 The Consultation Document proposes that risks around Fourth Parties will be managed through customer consent and application of the Privacy Act 2020 (**Privacy Act**). However, we have concerns that this approach will expose customers and their data to unnecessary risk of harm, in particular, when this is viewed against a backdrop of increased prevalence and sophistication of frauds and scams.

2.8 Reliance on consent alone implies a significant level of sophistication on the part of customers who will need to have a detailed understanding of the risks involved in sharing their data and the security and trustworthiness of the entity with which they will be sharing their data. This level of sophistication cannot be assumed for all customers and in particular for certain vulnerable customer groups in the current environment.

2.9 Therefore, in the absence of the trust implied by an external accreditation by a government body, customers may either be unwilling to share their data or share their data in a way that is not in their best interests. It is unclear whether a consent model can be designed that will appropriately address these concerns and whether customers will properly understand they may be sharing data with a Fourth Party who has not been accredited. As noted, this is particularly the case for vulnerable customers and in an environment when sophisticated frauds and scams are increasing, and customers are at increasing risk of having their data misused.

2.10 We strongly recommend that MBIE engage in customer testing to understand customer's expectations as to how their data will be treated in the CDR regime and what level of protections they would expect to apply.

c) Reliance on the Privacy Act for Fourth Parties is insufficient

[1] As an example we understand one existing intermediary currently has integrations in place with more than 50 Fourth Parties https://static.akahu.io/submissions/Akahu%20submissions%20-%20Customer%20and%20Product%20Data%20Bill.pdf

2.11 Similarly, we do not believe that reliance on the Privacy Act alone for Fourth Parties will be sufficient in protecting customers or their data. The Privacy Act is an effective principles-based regime that has been adaptable to be used in a number of different scenarios, however it has never been tested in the context of a widescale data sharing ecosystem, in particular, where that data is highly sensitive financial data.

2.12 The CDR regime is intended to design an economy wide data sharing ecosystem in which data that is currently held by data holders is shared on a potentially wide scale that could include pooling of data from multiple sources and other large scale high-risk uses of data such as the creation of data warehouses that are not currently contemplated by the Privacy Act. In this context it is important that there are appropriate safeguards in place for all those who are in receipt of customer data and not simply the initial requestor of the data.

2.13 MBIE has already recognised that the Privacy Act alone is not sufficient to govern the use of data under the CDR regime by requiring that accredited requesters need to go through an accreditation process and are subject to additional obligations that do not apply to parties who receive data under the Privacy Act. It is unclear why the Privacy Act is considered sufficient for dealing with Fourth Parties (whom most customers will have a relationship with) but it is not considered sufficient for dealing with accredited requestors who receive data directly. In practice this means that the *same* set of data will be subject to two separate regimes:

a) the initial data sharing will be subject to the consent requirements and other obligations under the Bill; and

b) once the data has been passed onto a Fourth Party the same data will be subject to the Privacy Act alone.

d) Most customers will not have access to a dispute resolution scheme

2.14 The Bill requires that accredited requestors are a member of a financial services dispute resolution scheme but this obligation will not apply to Fourth Parties who will be the main users of customer data and with whom most customers will have their relationship. This means that where customer complaints arise, these customers have no regulated forum to resolve their complaints and would have to rely on the Disputes Tribunal or the courts process which are costly and difficult to navigate.

Accreditation criteria should take into account use cases to protect customers from high-risk use cases

2.15 We are concerned that there does not appear to be any consideration of use cases in determining whether an applicant should become an accredited requestor. We believe that how customer data will be used is a critical consideration in determining whether an applicant should be accredited. There are a number of potentially high-risk use cases for customer data such as datamining or lead generation, which we do not believe should be permitted for use for data shared under the CDR regime.

2.16 Equally, with payments there is a risk that bad actors with fraudulent business practices or other high-risk industries could be allowed to participate in the payment system putting customers at risk. In this regard we reference, the body set up by UK Finance made up of Banks and FinTechs to develop draft rules for commercial Variable Recurring Payments (i.e. retail payments) in the context of Open Banking. The draft rules explicitly contemplate the risks of bad actors entering the system and

establish an onboarding process to address that risk as well as a staged roll-out of commercial payments with only low risk use cases initially in scope[2].

2.17 It is common practice for Banks to undertake due diligence on customers or other entities they do business with, in order to ensure Banks meet their regulatory obligations. This will include obtaining information on the nature of the business and the types of activities it intends to undertake. Accordingly, businesses should be accustomed to providing information about their business activities and we do not consider it to be an onerous obligation for potential accredited requestors to be required to provide information on their intended use cases as part of the accreditation process.

Liability – potential gaps should be addressed to ensure integrity of the ecosystem

2.18 The Consultation Paper proposes that where an accredited requestor requests an unauthorised payment, liability should sit with the accredited requestor. We support this approach. However, we note that there are a number of other areas of potential liability which we believe need to be addressed. A clear liability regime that ensures that consumers are protected and know who will be held accountable when something goes wrong will be one of the key enablers of trust in the open banking eco-system. We therefore ask MBIE to address the following:

a) accredited requestors should be liable where a request is made for payment to an incorrect bank account or for an incorrect amount;

b) ensure consistency of approach with the Anti-Scam Centre where an authorised payment made by a customer has been made as a result of a fraud or scam;

c) a party should be liable for damage to another party's systems as a result of accessing or using the APIs; and

d) clarifying that Banks are not liable for the use of data by accredited requestors or Fourth Parties once it has left their systems and that liability for any misuse of data sits with the party who has control of the data.

Restrictions on fees will inhibit growth and innovation in API infrastructure

2.19 Westpac is committed to enabling a thriving and successful open banking ecosystem and will continue to commit significant resources to enable and support an open banking ecosystem to meet the evolving needs of both its fintech partners and its customers.

2.20 A thriving open banking ecosystem relies on incentives for growth and innovation for all participants in the market that are based on sustainable and equitable commercial models for those participants.

2.21 Westpac strongly believes that restrictions on pricing for requests made under the Bill will disincentivise continued investment and enhancement in open banking infrastructure inhibiting future growth and innovation which would support a thriving open banking ecosystem (noting EFTPOS as an example of a free payment service which has resulted in lack of investment and innovation).

2.22 Significant investment has been made in API infrastructure within Westpac. This involves not only investment in the development and provision of APIs but also ongoing costs associated with the

[2] https://www.ukfinance.org.uk/news-and-insight/press-release/uk-finance-publishes-report-facilitate-commercial-variable-recurring

provision of wrap around support services to third parties, ongoing monitoring of third parties as well as compliance, risk and product governance to ensure safe and efficient access to customer data. This is critical in ensuring that customers and their data is safe and protected and to promote and maintain trust and confidence in open banking.

2.23 To date, Westpac and other banks have successfully partnered with FinTechs for access to open banking APIs. This suggests the existence of competitive market and commercial terms that can support the proliferation of valuable open banking use cases for customers. Based on this, there does not appear to be a need for regulatory intervention with respect to fees.

2.24 Should regulatory intervention be pursued, it should be targeted at enhancing transparency and simplicity of fees to assist with efficient partnering and system wide third-party uptake. We believe that this will lead to competitive pricing outcomes within the market (to the extent this is currently lacking). This also appears to be consistent with the Commerce Commission's proposals in the Network Designation (with respect to pricing) which suggests that it could "*set pricing principles in relation to API access or other fees impacting open banking*"[3] as opposed to exploring the imposition of limits and controls on fees.

Initial designation should focus on requirements most likely to deliver value to customers

2.25 We believe that the roll out of the CDR across the banking industry should be staggered to allow participants to focus on and refine a targeted set of capabilities which are most likely to deliver value to customers in the most efficient way.

2.26 The focus initially should be on simple use cases with the largest scope for fast consumer uptake without needing to build complex technical or regulatory frameworks to support them.

2.27 For example, business customers are inherently more complex than consumers often having multiple signatories and authorisation roles that can make consent requirements more complex. In this regard we refer to the Australian example where to facilitate CDR a new administrative role needed to be created to authorise data sharing at significant investment cost from Banks.

2.28 In addition, many business customers have existing bespoke solutions in place to access their data. Therefore, it is unlikely that a standardised open banking mechanism is the right solution to meet their needs.

2.29 For the reasons outlined above, the initial designation should be limited to retail customers (as defined under the Financial Markets Conduct Act 2013) and for business customers, those with a single account authority.

Inconsistencies between the scope of Designation and the Commerce Commission's recommendation to designation the interbank network

2.30 Westpac believes that regulation of open banking is best achieved through a single comprehensive regulatory framework such as proposed under the Bill and has significant concerns around the interplay between the CDR regime and the Network Designation**.** In particular, there are

[3] At page 35 of Commerce Commission's " *our reasons to support our recommendation to the Minister to designate the interbank payment network – August 2024".*

inconsistencies between the scope of designation proposed under the Consultation Paper and the Network Designation:

a) **Payment Initiation:** The Consultation Paper proposes that the only designated action will be payment initiation, whereas the Network Designation specifically excludes payment initiation from the scope of the CDR regime.

b) **Restrictions on fees:** As noted above, the Commerce Commission has indicated that it is likely that where fees are concerned, it is looking at setting *pricing principles* in relation to API access.[4] This implies that the Commission is not currently considering imposing price limits or requiring that access should be provided for free which are both options that are being explored under the Consultation Document. As stated above, Westpac does not believe that restrictions on fees are justified. However, any regulatory intervention targeting fees should be done under a single regulatory framework that that pricing is clear, transparent and easy to understand for the benefit of improving competition and efficiency.

2.31 We urge MBIE and the Commerce Commission to provide, as a matter of priority clarity, as to their proposed respective roles and responsibilities.

API Centre Governance

2.32 Westpac believes that it is important that industry continues to play a lead role in the development of standards under the CDR regime. However, we recognise that now would be an appropriate time to consider the role of the API Centre within the Payments NZ governance structure.

2.33 The API Centre has made a number of significant achievements with its work around the development of standards and building an understanding of what is needed to develop a successful API eco-system. We believe that those lessons would be valuable beyond banking and to the development of the CDR regime with its sector-wide focus. This provides a timely opportunity to evolve the API Centre from solely a banking focussed body to a body that is responsible for developing standards for the entire CDR eco-system.

2.34 We believe that there would be a number of efficiencies gained from such an approach of having a centre of excellence for developing sector-wide API standards and there would be significant opportunity for sharing information between industries. We would also support the API Centre taking a central role in the development of Digital Identity which we see as being key to the successful implementation of the CDR regime.

2.35 As a consequence of this expanded remit, a formal separation of the API Centre from the rest of PNZ into a separate governance structure would be needed to ensure that the API Centre appropriately represents all impacted industries as well as consumer groups. As a consequence, this model would necessitate the development of an appropriate funding model for the API Centre that would be representative of its participation and sustainable on an ongoing basis.

[4] At page 35 of Commerce Commission's " *our reasons to support our recommendation to the Minister to designate the interbank payment network – August 2024".*