Westpac New Zealand Limited

Submission to Ministry of Business, Innovation and Employment on the *Customer and Product Data Bill Exposure Draft*

24 July 2023

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 the *Unlocking value from our customer data* discussion document (**Discussion Document**) and the exposure draft of the Customer and Product Data Bill (**Bill**). Thank you for the opportunity to provide feedback on the draft proposals.

1.2 Westpac's contact for this submission is:

Head of Regulatory Affairs
Westpac New Zealand Limited
16 Takutai Square
Auckland 1010

Phone: Privacy of natural persons
Email:

2. KEY SUBMISSIONS

2.1 Westpac supports the introduction of a consumer data right (**CDR**) in New Zealand, and is excited about the prospects for offering real tangible value to our customers through an elegant and integrated customer data ecosystem. To ensure we develop a safe, secure and seamless environment for all New Zealanders, there are a number of key areas where further consultation and consideration is necessary. Given the limited timeframe for making submissions, Westpac has identified the following key points which we consider core to the successful implementation of the CDR regime in New Zealand. We have also provided specific feedback on a number of consultation questions set out in the Discussion Document. Westpac would welcome the opportunity to engage further with MBIE on these matters and the overall design of the CDR framework as set out in the Bill.

Building a trusted CDR ecosystem through accreditation and standards

2.2 Accreditation is inextricably linked to the concept of trust. The uptake of CDR will depend on both whether the experience is simple and easy for customers but also whether users can trust the system, and there needs to be a holistic approach to building trust in the CDR framework rather than considering accreditation in isolation. While a separate accreditation regime may not be necessary for all participants in the CDR ecosystem, it is essential that all participants adhere to a baseline standard of responsibility when handling data. In particular, downstream recipients of data should be subject to specific obligations around data and overall cyber security and ethical use of data. This will help to build trust in the ecosystem and encourage greater levels of customer use.

Clearly defined principles of liability are fundamental to the integrity and success of the CDR regime

2.3 Further consideration and clarity is required regarding the assignment of liability. From a customer-centric perspective, the regime must compel all CDR participants to create safe environments for customers. If the Bill fails to appropriately allocate liability to the party who is best placed to prevent or resolve the issue, this will create weakness in the system, cause detriment to customers, and ultimately reduce uptake and participation in this ecosystem.

2.4 It is also fundamental that the Bill includes an equivalent provision to that in s 56GC of the Australian Competition and Consumer Act, which provides CDR participants an exemption from liability where they have complied with the requirements of the Bill in good faith. Without a provision to this effect in the Bill, it is possible that CDR participants may find themselves liable for loss or damage that has occurred outside of their reasonable control and potentially create disincentives or barriers to entry. This opens the door to potentially unfair liability scenarios that run contrary to standard legal contractual interpretation in terms of allocation of liability. This may negatively impact uptake of the regime by accredited requestors who may not be able to properly insure themselves against the potential liabilities of participating in the CDR regime.

Acknowledging and leveraging the interplay between Open Banking and CDR

2.5 Given the significant investment that has gone into Open Banking in New Zealand, including the development of Application Programming Interfaces (**API**) and associated standards, Westpac strongly recommends that the government recognises the overlap with CDR and leverage the work that has already been done in Open Banking. While it is useful that the Discussion Document acknowledges that the standards already developed by the Payments NZ API Centre would be the "natural starting point", it is imperative from a cost and efficiency perspective that banks are not required to duplicate infrastructure and/or compliance systems to effectively manage two distinct regimes for a substantially similar outcome. For that reason, Westpac expects significant alignment between the Payments NZ standards and the new regime to remove duplication of investment. It is therefore important that where differences exist, there is sufficient consideration of the steps required to align the two regimes, so that the objective of moving first with banking can be achieved within the timeframes for implementation without significant additional investment.

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

2.6 Westpac understands that there will be further consultation on the details of the CDR regime as the regulations and standards are developed, and encourages close engagement with industry and our customers throughout the designation process. Given the complexities involved, the initial designation should focus on a narrow set of key requirements which can then be expanded over time, rather than taking an expansive approach from the outset. This will enable banks to focus initial efforts on a more targeted set of capabilities which are most likely to be utilised by customers and deliver value, rather than a broader suite of requirements which may see limited overall usage. Such an approach will also help to avoid unnecessary cost and delays in the implementation of the CDR regime. Both Australian and UK implementations were unnecessarily broad at the outset resulting in significant investment in unused capability.

The complexities of banking-related product data require further consideration

2.7 Considering the purpose of the CDR, there is limited practical benefit to providing access to banking related product data through an electronic system. It would create an unethically narrow view of product features and benefits, which is potentially at odds with a bank's other statutory obligations. For example, under the Conduct of Financial Institutions legislation where banks have an obligation to deliver the best outcomes for customers. There are very few use cases where products can be accurately and fairly compared on a like-for-like basis and encouraging innovation of product design is an important aspect to encourage a healthy marketplace that benefits consumers.

2.8 Taking a simplistic view of product data fails to acknowledge the complexities and variabilities of each product and the need for customers to obtain individual financial advice to enable them to make an

informed decision about what the best option is for them. Also, introducing a requirement to standardise the presentation of product data would require significant work for banks, and potentially stifle innovation by reducing the drive to create more nuanced and personalised products for customers. It may also encourage 'gaming' or setting of specific data points.

2.9 A greater level of consultation with banks is therefore required before any designation of banking-related product data is made under the regulations. While the Bill contemplates consultation with various stakeholders, given the complexities around these considerations, the Bill should include minimum standards regarding the consultation process.

3. RESPONSE TO CONSULTATION QUESTIONS

Question 1: Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?

3.1 Westpac agrees that the general applicability of the Privacy Act is appropriate in relation to the provision and receipt of personal information. Westpac submits that additional protections are appropriate, particularly:

(a) applicability to certain non-personal information data (such as business transaction history); and

(b) additional requirements of contemporary data management should be included to increase trust, security and confidence in the proposed ecosystem.

3.2 Such additional requirements can be set out in the relevant regulations and could include:

(a) *Data Classification and Definition*: The process of classifying and defining data fields into categories such as critical data elements, non-material data elements, and key data elements.

(b) *Data Flow Definition*: Documenting and updating data flows, especially in cases of multiple recipients, and maintaining logs of data receipts for tracking and managing data lineage.

(c) *Data Quality Assurance*: Monitoring the quality of data to ensure accuracy, completeness, consistency, timeliness, fitness for use, and availability.

(d) *Purpose and Usage Documentation*: Clearly defining and documenting the purpose for which the data was received and how it can be used, ensuring ethical usage and avoiding inappropriate commercialisation.

(e) *Data Incident Management*: Having robust processes for managing incidents that may compromise data security or integrity.

(f) *Data Control Identification*: Identifying and implementing data controls that maintain a consistent standard of data, with emphasis on completeness attributes, accuracy, consistency, and fitness for use. This also involves the automation of jobs and interfaces for load assurance, data quality rules, and supporting tools.

(g) *Accountability and Change Management*: Clearly establishing accountability for data management, implementing effective change controls, and ensuring seamless handshakes between participants.

Question 2: Should there be a maximum duration for customer consent? What conditions should apply?

3.3 To maximise participation and reduce implementation cost for businesses, consent should be able to be provided on an *enduring basis*, subject to customer validation through a regular/annual statement or reminder, prompting the customer to decide whether to update or revoke their enduring consent. This will mitigate the issues that arose in the UK where consent automatically expired after 90 days and ultimately led to customer frustration and a decrease in participation. The concept of consent modification is also not practical for data holders or accredited requestors. Westpac therefore considers that it should not be included in the Bill, other than enabling a customer to amend the duration of their consent.

Question 6: **What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?**

3.4 The consent process must be as simple as possible for customers, while retaining the necessary requirements to demonstrate genuine, informed consent. Requirements for consent should not be overly prescribed in the regulations and are better placed to sit in the standards. This will enable the requirements to be amended more easily if there are barriers or issues that arise, and to allow for different requirements for designated data-holders and designated data, depending on the sensitivity of the data, and whether the consent is authorising read only access or action initiation.

3.5 Pursuant to clause 30 of the Bill, the Customer must be reasonably informed about what the authorisation relates to. There will need to be clear guidance on what details have to be provided to a customer in order to justify whether they have been 'reasonably informed'. As is the case under the Privacy Act, where 'authorisation' is not defined, there are varying levels of understanding and interpretation as to what is required in order to obtain proper authorisation.

3.6 To ensure the CDR regime operates consistently and builds trust, the requirements for consent must be clear and unambiguous. Overall, the relationship facilitated by the consent mechanism must strive to be transparent to all participants, but particularly to customers. In terms of obtaining authorisation for data sharing, the Bill is not clear enough about when authorisation is required at different stages of the process. In the interests of clarity and certainty, Westpac submits that a more straightforward approach would be for the Bill to clarify that there is a two-step authorisation process:

(a) Customer authorises their data being collected and used by an accredited requestor. Accredited requestor submits a request for the data from the data holder.

(b) Data holder obtains the customer's authorisation to disclose the data to the accredited requestor.

3.7 The following matters require specific consideration in the design of the consent process:

(a) *Scope of the consent:* In terms of *transparency* of consent, it is important that the consent process is built in way to enable data holders to see the complete scope of the consent. For example, each consent given by a customer must be distinct and specific enough so that

revocation of one consent for the use of data by a down-stream third party provider does not inadvertently switch off or withdraw other consents for data which may flow through the same accredited requestor (i.e. an aggregator). In a situation where one accredited requestor is pulling data for a range of down-stream third parties to provide services to a customer, the data holder must be able to see each of the separate consents for those downstream providers in order to action a specific withdrawal request from a customer and be in a position to accurately inform the customer about the consequences of revoking their consent – which is a requirement in the Bill.

(b) *Actioning a withdrawal*: Clause 34 of the Bill requires withdrawal requests to be given "immediate effect". This should be amended to allow some level of flexibility for participants where their systems may not yet be developed in a way that allows for immediate revocation. In Australia, if the customer withdraws authorisation, the data holder must action that request as soon as possible, within two business days at the most. A similar timeframe for actioning withdrawal requests should be included in the draft Bill. This would align with a similar construct in the Unsolicited Electronic Messages Act 2017 which requires a business to unsubscribe a customer from marketing material within 5 business days of their request.

(c) *Joint account holders and secondary users*: The current drafting of the Bill does not expressly allow for an authorised representative to act on behalf of a customer. Clause 22 of the Bill does require the regulations to prescribe when and how secondary users can make a request or give an authorisation on behalf of a customer, and how these requests and authorisations are to be dealt with by data-holders. For individual customers, an equivalent construct to section 57 of the Privacy Act could be included where a customer can appoint a representative to act on their behalf, provided that the identity of that person can be appropriately verified and there is sufficient evidence that the person is properly authorised by the individual to provide such consent. However, further consultation is required to acknowledge and address the complexities and scale of signing authorities that may apply for various types of bank accounts. Westpac supports the suggestion that MBIE leverages the existing policies and processes used by the banks in relation to managing joint account holders. MBIE should also look to the work already undertaken by Payments NZ on this point to avoid duplication of systems and processes across the Open Banking and CDR regimes (such as the API Centre's Customer Experience Guidelines and its Principle of Equivalency).

Question 10: **What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?**

3.8 The government should consider the following when initiating standard setting with the banking sector under the proposed Bill:

(a) *Scope Limitations*: A scope limited by industry may limit the full potential of the data exchange ecosystem. For instance, the inclusion of adjacent industries or supporting industry providers, such as accountancy services, could add significant value to the data. Access to codified transaction data and chart of accounts information for small businesses, for example, could greatly enhance the utility of financial data, driving better business decisions and improved financial management.

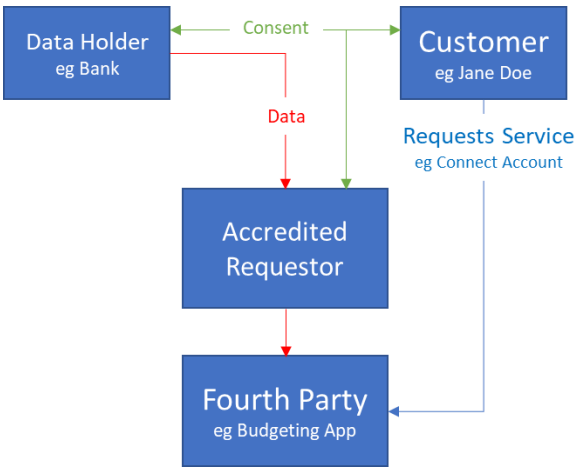
(b) *Interoperability with Emerging Standards*: MBIE should consider the robust series of standards already defined by Payments NZ API Centre while forming the CDR regime. However, the formation of standards is an evolving process. Globally, new approaches to developing standards, such as Canada's Zero Copy for data integration, are emerging. It is crucial that the standards set forth in the Bill are flexible and adaptable, allowing them to stay relevant and interoperable with international standards.

(c) *Potential for Confusion with Existing Regimes:* With the likely concurrent introduction of this Bill and the standards from the Payments NZ API Centre, there is potential for confusion in managing interactions with accredited recipients. The current industry regime is based on bilateral contracts and lacks a proportional system for the management of liability and redress considering the asymmetry of risk in data exchange. To mitigate this, MBIE could consider accelerating the CDR register and trust processes, clarifying the roles and responsibilities for all parties involved.

(d) *Societal Purpose and Broader Economic Rationale:* The proposed Bill enables the exchange of customer and product data but could benefit from a clearer articulation of its broader societal purpose. Such purpose could be linked to enhancing small business resilience, promoting sustainable practices, or empowering individuals' agency over their data use. With a well-defined societal objective, it will be easier to determine whether future amendments to standards and new proposals align with the Bill's intent.

Question 11: **Should there be a class of accreditation for intermediaries? If so, what conditions should apply?**

3.9 Westpac agrees that there does not need to be a distinct role of *'Intermediary'* identified in the Bill. An entity functioning as an Intermediary can be accredited in the same manner as other accredited requestors. Having an accreditation regime for all participants in the CDR ecosystem may have the unintended consequence of stifling innovation and uptake, and may become a barrier to adoption of CDR. However, allowing unaccredited parties (i.e. the Fourth Party) to access data through accredited requestors also creates significant risk, which needs to be effectively managed in order to protect customers and preserve confidence in the system.



A diagram to illustrate how a Fourth Party entity receives data from an Accredited Requestor.

3.10 Westpac's suggested solution is that the relevant regulation sets out additional requirements for the accredited requestor that requires it to:

(a) undertake certain due diligence on the Fourth Party before passing data to them;

(b) ensure that the Fourth Party provides a digital mechanism for customers to view and manage their consent;

(c) itself provide a digital mechanism for customers to view and manage their consent;

(d) ensure that the customer gives informed consent with appropriate disclosures in relation to the Fourth Party;

(e) ensure that the data holder is informed of the Fourth Party on whose behalf the accredited requestor is acting; and

(f) identify the Fourth Party on the closed register.

3.11 The requirements will vary depending on the industry, the type of data being accessed, and nature of the consent obtained. For instance, the obligations to apply in relation to accountants' access to transaction history would be different to the obligations in relation to a Fourth Party obtaining enduring access to initiate payments.

3.12 A data holder should be required to provide a digital mechanism for a customer to have a "look through" to view and manage their consent in relation to each Fourth Party connection (not just the relevant accredited requestor). This means that a customer must be able to revoke their consent for a Fourth Party without interrupting any other consent given to a different Fourth Party via the same accredited requestor. However, there also needs to be recognition of the accredited requestor (such as cloud based accounting software) that would not need to inform the data holder of the Fourth Party (such as an accountant or app partner).

3.13 It is vitally important to the proper functioning and trust of the CDR ecosystem that the Bill recognises the various CDR participants and imposes obligations on them in respect of data use and security. In relation to personal information, the Privacy Act will apply to any Fourth Party (and Westpac agrees that this is a sensible approach). However, as set out in response to Question 1, there is a need to:

(a) apply some of the principles of the Privacy Act to non-personal information data (e.g. transaction history for business customers); and

(b) impose additional obligations on Fourth Parties in certain scenarios, for example where a Fourth Party has consent to initiate payments it must belong to a recognised dispute resolution service.

3.14 The liability regime in the Bill must dovetail with the accreditation and due diligence requirements set out above. For example, where a dispute arises between a customer and a Fourth Party, the data holder should not be involved. Any participant in the framework should be held accountable to both regulators and customers for their involvement and data use and handling, and the Bill should not inadvertently create "gaps" where certain participants fall outside the compliance / liability framework of the regime, and others are required to take on the liability for their actions. In order to successfully implement CDR and create a trusted CDR ecosystem, Westpac's view is that New Zealand should take inspiration from:

(a) The Qualified Trust Service Provider model seen in Europe (**QTSP**); and

(b) The Digital Identity Services Trust Framework (**DISTF**); and

(c) The EU Payment Services Directive 3 (**PSD3**).

3.15 The concepts in these models are inextricably linked in their functions and purpose with the CDR framework as customer consent can be authenticated using the DISTF and perhaps through an interaction with RealMe, or its logical successor. The 'Intermediary' could be a Qualified Trust Service Provider, or Identity Scheme provider which could be accountable for liability and redress. In this way trust can be decentralised reflecting the multiple industries, standards and diversity of participants. The Trust Service Provider becomes a source of trust in the network.

3.16 As demonstrated by the QTSP, it is vital to provide cyber trust assurance in order for customers to have trust in the CDR framework. Furthermore, the trust model needs to be built around a policy and process for data management and stewardship in relation to lineage, metadata, governance, and deletion of data. In this way the data's journey is captured holistically, and all participants in the ecosystem can have confidence they have an understanding of where the data has come from and where it is going to go.

Question 12: Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?

3.17 There is a risk that mandated insurance may act as a barrier to entry. Relevant insurance would include cyber insurance, which is expensive and difficult to obtain in New Zealand and mandating it may only allow larger players to participate in the CDR regime. Under the Australian regime an accredited requestor needs to have adequate insurance (or comparable guarantee). The ACCC does not prescribe specific amounts or types of insurance required to be held.

3.18 Rather than legislating mandatory insurance, the adequacy of a potential accredited requestor's insurance should be considered as part of the accreditation process when determining whether the applicant has a way to support liability under its arrangement with the data holder and customer. Any specific insurance requirements should be a commercial point agreed between the relevant parties rather than mandated by law, accompanied by a guidance document to provide recommendations It is also worth considering how risk can be managed in other ways besides insurance. For example a Qualified Trust Services Provider could audit the accredited requestor and provide attestation for cybersecurity.

Question 14: Do you have any other feedback on accreditation or other requirements on accredited requestors?

3.19 Further points requiring consideration include:

(a) *Length of accreditation:* There needs to be consideration on how long accreditation lasts and whether there will be a reaccreditation process or a regular audit process to ensure accredited requestors comply with the accreditation standards.

(b) *Assessment of API product:* The process of accreditation should include an assessment of the proposed API product itself.

(c) *Direct to customer data access:* The Bill contemplates that data should be made available directly to customers as well as to through accredited requestors. However, including direct-to-customer data access would significantly increase the complexity and security risks for

any electronic system design, and is not well-suited to the initial stages of a CDR generally (which is focused on producing machine-readable data in a standard format). Where customers simply wish to access their customer data, as opposed to accessing it in connection with products or services offered by an accredited requestor, it is likely that such information is already accessible through existing online and in-app banking services or via an IPP 6 request under the Privacy Act. Westpac believes that the aim of the CDR is best met through the provision of data securely and efficiently through APIs which are regulated through the accreditation process.

(d) *New techniques:* Emerging techniques in secure multi party computation allow for inherently secure data exchange. The governance of the proposed system should support evolution in data sharing best practice and allow for adoption of these techniques at a later date. Examples of these new standards include zero-copy integration and differential privacy.

(e) *Payment initiation safeguards:* Payment initiation carries significant risk of customer harm through fraud or mismanagement. We would recommend considering additional safeguards such as the active use of NZBN for account number matching. This could be enabled by mandated completion of the "Bank account for payments" data on the NZBN repository.

Question 16: What are some specific use cases which should be designed for, or encouraged for, business (including small businesses)?

3.20 Some examples include:

(a) *Cash flow management:* The ability for businesses to access and analyse their financial transaction data can greatly assist in managing cash flow effectively. By providing access to transaction histories and account balances in a machine-processable format, businesses can develop intelligent financial management tools and applications.

(b) *Treasury management:* Businesses often engage in complex treasury management activities, including cash management, liquidity forecasting, and risk management. Access to customer data, such as transaction details, account statements, and investment information, can empower businesses to build advanced treasury management systems.

(c) *Supplier payments:* Streamlining supplier payments is crucial for businesses, particularly small businesses that may have limited resources. By leveraging customer data provided by businesses, small businesses can develop innovative tools and platforms to simplify payment processes, automate invoicing, and ensure timely payments.

(d) *E-invoicing:* E-invoicing is gaining popularity as a more efficient and sustainable alternative to traditional paper-based invoicing. Enabling businesses to access customer data related to invoicing can facilitate the development of e-invoicing solutions.

(e) *Lending applications:* Holistic financial information is critical to providing lending responsibly, and the act will allow for collection of this information in a seamless way. In this respect we would encourage an extension to include non-bank financial institutions to ensure that CDR enabled lending journeys do not take a narrow view of customer commitments.

3.21 While encouraging these use cases, the Bill should maintain appropriate safeguards for data privacy and security.

Question 19: What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?

3.22 Westpac agree with the proposed requirements for ethical use of data as a condition of accreditation. Without a requirement for ethical data use, data holders are unable to regulate the use of customer data once it has been shared. This may lead to accredited requestors and other downstream recipients of data using that data for a range of purposes not contemplated within the original request or within the scope of the customer's authorisation.

3.23 Westpac also agrees with the requirement that express customer consent should be required for the de-identification of customer data, as Westpac believes that in order for customers to be able to give their proper informed consent, they must be expressly informed about all the potential uses of their data, even if that data cannot be used to identify them. There are real risks around the use of de-identified data as it has the ability to be transferred to third parties and commercialised or used to train artificial intelligence algorithms on a number of metrics. Customers should therefore have complete transparency and control over how their data is intended to be used. This level of transparency and control for customers will build trust in the system and reduce the likelihood of customer complaints.

Question 20: Are there other ways that ethical use of data and action initiation could be guided or required?

3.24 There are a number of actions that could be initiated by accredited requesters that Westpac considers pose too high a security risk to be allowed. For instance, a request for a password change or other account alterations should only be actionable by the customer. Westpac therefore proposes that a class of actions be outlined as being actionable only by the customer, to reduce the security risks associated with action initiation.

3.25 Westpac also considers that there should be safeguards imposed on the use of artificial intelligence algorithms on both de-identified customer data and product data. The unregulated availability of downstream parties to use these data types in any way provides significant security and competition risks for businesses. To inform and guide ethical use of data in this fashion, Westpac proposes that principles mentioned in the Discussion Document such as fairness, robustness and transparency are further expanded upon and incorporated into regulations or standards to which all CDR participants are subject to. This would restrict the ability of downstream parties to use data without regulation and would provide clarity for all parties on their requirements in the use of data.

3.26 It is also important for certain datapoints regarding the transmission of data to be retained with the data itself and kept accurately. The metadata that provides information on the source, format and context of data is useful if a customer wants to find the chain of transmission for their data or if a breach has occurred. Westpac proposes that the regulations impose a requirement that metadata and lineage information is kept in accurate records, and is stored, managed and passed on inline with ethical data use. This enables all CDR participants to have complete and accurate information about the transmission of customer data, which would increase trust and ensure compliance with the security measures in place.

3.27 In line with this, Westpac also recommends that privacy by design principles follow the data (whether it is personal information or not) and proactive initiatives are implemented to educate customers on how their data is used, potential misuse risks and the roles of different entities in the chain of transmission of their data. Westpac does not agree with the Discussion Document's suggestion that ethical

requirements for the safeguarding of data apply to participants in relation to data services, rather than the on-sharing of data. Westpac believes that the on-sharing of data provides a significant security risk to users in the system and should be protected by the same ethical use requirements.

3.28 We would also acknowledge that the use of 'purposeful' APIs is very well aligned with the Privacy Act, in allowing customers to share specific data for specific purposes. In this respect we would expect that over time the CDR ecosystem would replace the somewhat contentious use of screen scraping which provides access to data and capability well beyond any intended reach of a customer's privacy consent.

Question 23: Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?

3.29 Westpac considers that a data holder should have a level of discretion to decline a valid request on reasonable grounds, for example, if the Bank has identified a potential fraud or has concerns with the security of the proposed data exchange. However, despite this discretion, a data holder should not be liable in any way for complying with a valid request if it does so in accordance with the regulations.

3.30 The Discussion Document outlines that such a provision is not necessary in New Zealand. However, Westpac considers that there are likely to be a range of situations where an entity may comply in all material respects with the law, but some form of liability or loss still arises. For example, despite complying with minimum security measures to protect data, a security incident may occur and a customer may suffer loss as a result of an error of data or failure to provide data. From a payments perspective, a bank could be liable if a payment is made in breach of sanctions, breach of trust or to facilitate fraud or some other type of criminal enterprise (even if the payment is authorised). It is important to recognise that an authorised request can still be the result of fraud or coercion and customers have certain expectations that banks have processes in place to ensure they are reimbursed in such scenarios.

3.31 In these circumstances, provided the data holder has complied with its obligations under the Bill, Westpac strongly considers that it should not be liable for such loss. This aligns with MBIE's general view in the Discussion Document that compliance with an Act should not as a matter of law create or result in liability. The absence of such a provision is likely to have a negative effect on the uptake of the regime, particularly where the benefit of participation is outweighed by the legal liability risk.

3.32 Data sharing within an ecosystem is commonly facilitated through APIs. It is common practice for an API management and related cyber security systems to throttle, selectively restrict, or deny instructions to protect systems, prevent overload and limit unwanted behaviour. A data holder should be able to technically decline an API instruction, which could contain a valid request, and request that it is resent at a later time, or in accordance with agreed conformance and process standards for managing this exchange.

3.33 The Bill should also clarify the order of precedence where an obligation to release data under the CDR framework may conflict with other statutory obligations. Acknowledging that banks are vital to ensuring the stability of the financial sector in New Zealand, there is a strong public interest in ensuring that those fundamental responsibilities take precedence over CDR obligations.

Question 26: What are your views on the potential data policy requirements? Is there anything you would add or remove?

3.34 Westpac understands the purpose of the data policy is to enable customers to understand whether to do business with the data holder or accredited requestor. To ensure customers can, in fact, properly

understand how an entity deals with their data, there is a need for more prescriptive safeguards than what has been proposed. This is a fundamental requirement to build trust and transparency in the CDR ecosystem and aligns with good data governance.

3.35 Currently the Bill places too much emphasis on a customer understanding how an entity deals with their data. It is unlikely that customers will fully appreciate or understand how their data will be used and protected simply by reading a data policy available on an entity's website. In our view, the responsibility to demonstrate good data governance should sit with data holders and accredited requestors, and any entity who deals with customer data and wishes to participate in the CDR regime should have sufficient internal mechanisms, policies and processes to demonstrate and/or explain to customers how they use and protect the data they process.

3.36 Westpac expects that having good internal data policies should also be a key criteria for accreditation under the CDR regime. Therefore, the legislation should be more prescriptive about what is required from a data policy perspective, to ensure both transparency for customers and to assist accreditation bodies in their assessment process. In relation to the particular details to be included in the data policy:

(a) Westpac assumes that (as is the case under the Australian law) this policy must be separate from a data holder's or accredited requestor's privacy policy and must expressly address each of the matters listed in the legislation even though some of this detail may also be included their privacy policy;

(b) In addition to the list of details set out on page 47 of the Discussion Document, a data policy should also set out what CDR data is held and used by the entity, any security measures in place, and who the data may be disclosed to; and

(c) Along with details of the internal complaints process, it should also be clear to customers in the data policy what their rights of redress are and where they can go for dispute resolution. This aligns with other consumer protection obligations under the Fair Trading Act (s13) and Consumer Guarantees Act, to ensure that entities do not make misleading representations about a customer's rights or remedies under the CDR framework.

Question 30: What should the closed register for data holders and accredited requestors contain to be of most use to participants?

3.37 The closed register for data holders and accredited requestors should contain information to enable an efficient, secure and trusted data exchange ecosystem. The role of the initial closed register should be to support operational efficiency and maintain trust within the digital identity ecosystem. Rather than collecting and storing extensive personal data, it should contain only necessary information about data holders and accredited requestors, and only with their explicit consent. The register could initially be closed to the public for privacy reasons but accessible to participating entities for transparency and efficient operations.

3.38 More broadly, the creation of a closed register appears to contrast with the principles underpinning the DISTF, which emphasize decentralization and user control over their data. It is important to ensure that the function of such a register is aligned with DISTF principles and respects privacy, consent, and data minimization. Drawing from the lessons of the Revised Payment Services Directive (**PSD2**), which employs Qualified Trust Service Providers, Westpac envisions a similar role for 'Qualified' Trust Providers within the DISTF. These entities, rigorously vetted and qualified by an authority such as the

Payments NZ API Centre or the proposed owner of the closed register, link to the register but provide further levels of assurance.

3.39 The digital identity ecosystem's growth and evolution could lead to the distribution of register management among multiple 'Qualified' Trust Providers. This not only ensures the decentralization of trust but also allows the system to adapt flexibly to changes in the ecosystem. It also respects the principles of the DISTF, allowing for a more robust, scalable, and privacy-respecting ecosystem. Each of these accrediting entities could then issue verifiable credentials to validated participants, allowing other participants to verify these credentials independently by checking their cryptographic proof. This enhances privacy, as participants need not reveal their credentials to a central authority, only to those they interact with.

3.40 Therefore, while a closed register could serve as a pragmatic administrative tool to manage the start of implementation, it should not be the sole mechanism of establishing trust within the system. Instead, a decentralized accreditation system can create a more robust, scalable, and privacy-respecting ecosystem that aligns with the principles of the DISTF.

Question 31: Which additional information in the closed register should be machine-readable?

3.41 As a minimum, the register should maintain the following key data points for each participating entity:

(a) *Entity Name:* The official name of the entity.

(b) *Entity Type:* The type of entity (individual, organization, or thing).

(c) *Decentralized Identifier (DID):* A globally unique identifier assigned to the entity, used for securely establishing and verifying the entity's identity.

(d) *Public Key:* The public component of the entity's cryptographic key pair, used for verifying digital signatures and credential authenticity.

(e) *New Zealand Business Number (NZBN):* If the entity is a business, its NZBN serves as a globally unique identifier specific to New Zealand businesses.

(i) Payment Bank Account is secondary business data on the NZBN registry. For participants receiving payments, including non-accredited participants, consideration should be given if this information should also be provided via MBIE NZBN APIs. The purpose of this exchange would be to provide a further point of trust verification during payment requests.

(f) *Accreditation Status:* The current status of the entity's accreditation (accredited, pending, revoked, etc.).

(g) *Accreditation Level:* The level of assurance associated with the entity's accreditation, based on the rigour of the validation process they have undergone.

(h) *Dispute Contact:* Contact information for disputes or issues related to the entity's accreditation or credentials.

Question 33: Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?

3.42 Westpac believes that there should be a requirement for data holders to provide frequent reporting on the performance of their CDR APIs.

3.43 The term "real-time" has different interpretations in engineering, customer experience and process that require definition to resolve clearly. implementing true "real-time" reporting can be costly and requires careful infrastructure design to support high-speed updates without compromising performance, data quality, or introducing errors.

3.44 For example, Westpac understands that ecosystem participants will integrate services provided by us into their own services. Hence Westpac understands that the ecosystem will want to have visibility of availability, conformance and response times, but all this information need not be updated every few seconds.

3.45 To alleviate the impact on infrastructure, it is essential to define clear standards and guidelines for this reporting process. This includes specifying the level of granularity required for reporting and establishing thresholds for performance metrics. By setting reasonable expectations, data holders can strike a balance between the frequency of reporting and the feasibility of implementation.

3.46 To increase knowledge of activity in the ecosystem, frequent reporting from other participants in the ecosystem, not just Data Holders, should be required. This system wide information would be valuable to support adoption, customer education (data requests by hour, week, unique customer data retrieved) and prevent financial crime (Payment requests by status and time windows).

3.47 In addition to the previously mentioned points, it is important to consider the potential role of Trust Services Providers (**TSPs**) in the context of reporting on the performance of CDR APIs. While TSPs are not currently included in the proposed plan, their involvement could bring significant benefits to the data exchange ecosystem. TSPs, similar to their role in the European PSD2 (Open Banking) legislation, could serve as trusted entities responsible for ensuring the security, integrity, and reliability of data exchange processes.

3.48 Privacy-preserving measures must be in place to protect customer identifiers while sharing network information. Adherence to data privacy regulations and the use of anonymization techniques can help maintain the confidentiality of customer data while still providing valuable insights into network performance.

Question 34: What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?

3.49 A maximum cap on customer redress should be included in the Bill to provide certainty for data holders and accredited requestors about their potential liability under the statutory regime. Without this level of clarity, smaller businesses may be reluctant to participate in the CDR regime due to the risk of an uncapped liability for their business should something go wrong.

3.50 To align with other consumer rights under New Zealand law (such as s18(4) Consumer Guarantees Act 1993) any liability for loss or damage suffered by a customer should be limited to those resulting directly from the breach where such loss or damage was reasonably foreseeable as liable to result from the failure.

3.51 Taking into account the fairly limited value of monetary penalties or loss that could potentially be suffered by a customer in relation to the CDR regime, Westpac submits that the maximum cap on customer redress under the CDR Bill does not need to be equivalent to that provided under the Privacy Act, and should more appropriately align with the Disputes Tribunal jurisdiction to settle small claims up to $30,000.

3.52 MBIE should also consider:

(a) clarifying that any right of redress is not in addition to any other rights or remedies under other laws;

(b) a good faith exemption to liability for data holders and accredited requestors; and

(c) the ability of an accredited requestor or data holder to claim compensation from an outsourced provider for an attributable data breach.

Question 35: In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?

3.53 Westpac agrees that disputes between customers and data holders and/or accredited requestors should be dealt with by existing industry dispute resolution schemes. However, Westpac does not agree that the Disputes Tribunal should be used as a backstop for fringe cases. Westpac considers that any shared responsibility for managing complaints between MBIE and the Privacy Commissioner should be avoided as it may lead confusion unless there is a clear delineation of responsibilities. Westpac therefore recommends that non-privacy related complaints should be handled by external industry dispute schemes where possible. This will provide clarity for customers and outline a clear, well-established and tested pathway for disputes to be resolved in specific industries.

3.54 Currently, the bank has its own internal customer disputes resolutions process.. If a dispute cannot be satisfactory resolved internally, then the customer can escalate the matter to the industry regulator, the Banking Ombudsman, or for privacy specific complaints the Office of the Privacy Commissioner retains jurisdiction and oversight. Westpac are content that this current system is effective at managing disputes and should apply equally to disputes regarding the CDR regime. To this effect, Westpac agrees with the suggestion that data holders and accredited requestors should be required to be members of recognised external dispute resolution schemes, as is the case in Australia. Any disputes relating to privacy matters should remain subject to oversight and resolution by the Office of the Privacy Commissioner. To further clarify the dispute resolution roles and functions, each regulatory body should be subject to specific Terms of Reference and there should be a public facing metric around how disputes are to be raised.