Mr Bruce Cooper
General Manager
Consumer Data Right Branch
Australian Competition & Consumer Commission
Level 2, 23 Marcus Clarke Street
CANBERRA ACT 2601
Via: Consultation Hub

12 October 2018

Dear Mr Cooper

Westpac Group Submission – Consumer Data Right Rules Framework

The Westpac Group (**Westpac**) welcomes the opportunity to provide a response to the Consumer Data Right Rules Framework (**Rules Framework**) and thanks the Australian Competition & Consumer Commission (**ACCC**) for the opportunity to meet to discuss certain aspects of the Rules Framework as well as participate in recent roundtables.

In addition, Westpac supports the submission made by the Australian Banking Association (**ABA**).

Introduction

As stated in earlier submissions on Open Banking, Westpac supports the Government's introduction of a Consumer Data Right (**CDR**) regime in Australia. We agree that the application of the CDR to the banking sector, and subsequently to other sectors in the economy, has the potential to transform the competitive landscape by giving individuals greater access to, and the ability to share, their data.

We support the Government's approach to place the value of consumer data in the hands of the consumer so they are the decision makers in the CDR regime and have the ability to direct where their data is transferred.

Trust in the CDR regime is integral to its success. We know that customers trust banks with their data and their financial assets. Recent research conducted by RFi in Australia highlights that consumers trust their major financial institutions with their data more than other institutions.[1] We also know that the majority of consumers feel uncertain or hesitant about sharing their data. Investing in education on the CDR will be critical to ensure consumers not only understand their data is within their control but also how to share data in a safe and secure way and how they may have confidence in the CDR regime to facilitate this.

The underlying CDR framework must also be sufficiently robust to support the safe transfer and the use of customer data for a limited range of approved purposes, thereby protecting customer

[1] RFi, *Open Banking Consumer Multiclient Study,* September 2018.

privacy and information from day one. The first iteration of the Rules Framework should focus on achieving a robust and secure CDR regime for 1 July 2019. Phasing will be central to the CDR framework's implementation. Similarly, technical scope will need to be iterative to enable phased delivery and build on prior versions.

We note the ACCC intends to progressively develop rules and does not propose to address all potential issues in the first version, instead only seeking to make rules on the matters that are essential and feasible for the commencement of Open Banking on 1 July 2019.

Westpac welcomes that approach.

We consider that only those rules that are technically feasible and aligned to the policy intent of the Open Banking Review[2] should be in scope for 1 July 2019. Those items that aren't technically feasible should be versioned into later phases so as not to present a distraction and put at risk successfully achieving delivery of open banking for the majority of customers.

With respect to the types of data to be disclosed by 1 July 2019, we note that banks strive to give their customers the best online banking experience and this is a source of competitive tension among banks today. These online banking systems are now mature. This means that any data that we consider to be valuable to customers, and is not highly complex to expose, is currently available in online banking. We consider that in principle the presence or absence of information available in online banking today is useful to guide ACCC's thinking on what could be in scope for a 1 July 2019 start date, noting the level of detail will vary by the type of each transaction.

We emphasise that it should only be a guide as there is significant variability in the types of information available (and therefore which can be viewed by the customer) depending on the nature of the transaction.

We agree with the key proposals outlined in the Rules Framework that an accredited data recipient may only collect and use a consumer's data where it has obtained their informed and express consent, and in accordance with the scope of that consent. We also agree that a data holder must share a consumer's data with an accredited data recipient where the consumer directs and authorises it and that consent must be informed, specific, clear, express and freely given.

This submission outlines the key areas of the Rules Framework we agree should be in scope (and which we consider are technically feasible for 1 July 2019); key areas where we do not agree, in principle, with their inclusion and the reasons why; and other issues.

Attachment A also sets out the proposed customer, product and transaction data sets contained in the Rules Framework and Westpac's technical assessment, privacy assessment and our recommended approach to those.[3]

[2] Scott Farrell, *Open Banking – Customers choice convenience confidence*, December 2017.

[3] Noting that this commentary specifically relates to those data sets as applied to retail products in scope for the 1 July 2019 start date (deposit, transaction, credit and debit cards) and not for corporate customers and products.

Key Areas that should be in scope for 1 July 2019

Accounts with simple authorisation

We welcome clarification that accounts with complex authorisations are out of scope for 1 July 2019. Again, we consider that inclusion of accounts which have simple authorisations in place (ie where account holders can individually and independently authorise transactions) will enable banks to fully focus on delivering open banking for the majority of their online customers.

Privacy considerations for joint accounts (even in cases where customers can individually and independently authorise transactions[4]) still need to be worked through as it does not necessarily follow that because an individual (customer A) has the right to transact that they will also have the right to share data relating to another account holder (customer B). In our view, this issue is not best addressed by providing customer B with the right to terminate the sharing after it has been established by customer A. The termination approach, in our view, is also not well aligned with customer transparency and also the requirements relating to the provision of clear and informed consent. Additional considerations are also likely to apply for vulnerable customers that will need to be addressed.

We agree with the ACCC assessment of the Open Banking review recommendation that authority to transfer money as a proxy for authority to transfer data for joint accounts may not necessarily "…*resolve all issues for accounts that allow multiple parties to view and/or transact on the account, or that otherwise entail complex account arrangements*."[5] We would go further and suggest that it does not resolve the issue for accounts where two or more parties are required to authorise each transaction. In such cases the accounts would require the authority of all individuals to exercise the CDR and consent and authorisation flows are complex.

As noted above, we also agree that there are "*particular risks that can arise in relation to vulnerable consumers, including those at risk of financial or other exploitation by other account holders*."[6]

In addition there are technical barriers to being able to accommodate these customers within the Consumer Data Right Framework as presently designed. That is, we cannot think of a way to implement multi-party authorisations using the re-direct flow.[7]

---

[4] That is, for 'one-to-sign' accounts.

[5] ACCC, *Consumer Data Right Rules Framework*, p 33.

[6] Ibid. We note that the revised Banking Code of Practice, scheduled to come in force on 1 July 2019, contains a new commitment intended to address situations where joint account holders are subject to financial abuse. The new obligation is that banks will be required to comply with a request of any joint account holder to require all parties to authorise withdrawals. Once a bank acts on that request individual joint account holders who previously could independently withdraw funds would now no longer be able to do so. It would follow that following such a request they would also no longer be able to independently transfer data and that all parties would be required to authorise data sharing.

[7] We know that Data61 is strongly considering using the UK model redirect based flow to authenticate customers rather than a decoupled approach (although a definitive decision is yet to be made). The redirect model redirects from a third party site or app to a page that asks a customer to provide their internet banking username and password. This is different to a de-coupled approach which we consider is the best and most secure approach to authentication and authorisation. While we know the most recent version of the UK standards has added guidelines and support for decoupled flows in addition to redirect flows this is for the purpose of payment initiation See e.g: https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines.pdf

In terms of corporate customers we re-iterate our views from earlier submissions on the need to exclude such customers from the day one scope. In terms of our largest institutional customers it remains a live issue as to whether such customers should ever be in scope. Aside from the technical complexities in designing a consent and authorisation process that would support such customers we think the potential uses or benefits of the CDR regime to those customers are extremely limited and are likely being met by current competitive tender processes.

Online customers

We support the ACCC's view that the first version of the rules should only extend the CDR to consumers who have access to and use online banking – which includes consumers who use a web browser or a mobile app to access their accounts.

Accreditation and reciprocity

Summary

- The initial accreditation tier should be set at the highest standard of participant to ensure security from the outset. Lower tiers should be added (on a customised basis with the data shared reflecting the accreditation level) once there is confidence in the regime to preserve the integrity of the system.

- Reciprocity should be included from day one. The capacity to provide equivalent data on request from the consumer should be built into the accreditation system to maximise the robustness of the CDR regime.

We agree with the Rules Framework position that the initial tier of accreditation as at 1 July 2019 should be set at a standard which permits the participant to receive and hold the full scope of CDR data which is part of the regime.

Given the current environment in which the CDR Rules are evolving, and to ensure the regime is set up safely and for success, we support tiered accreditation. In our view, to maintain the integrity of the regime, the first tier of accreditation should be set at the highest standard of participant. Once the initial sharing processes have commenced and other key requirements set and implemented there would be more information available to base the appropriate access permissions for additional tiers as described in the Framework.

On reciprocity, we note the ACCC's view that it does not consider the principle of reciprocity to mean that a data holder is entitled to request or obtain data from an accredited data recipient before sharing data it has been directed to share by a CDR consumer (ie that reciprocity is not a 'quid pro quo' arrangement).

Westpac agrees with this statement. We consider that reciprocity (in accordance with the Open Banking review) refers to the capacity of the participants to provide equivalent data as part of their participation in the CDR regime. In line with the Open Banking Report, we consider that having such capacity amongst the participants would support a safer environment in which this system will flourish. Requiring this capacity should naturally form part of the accreditation system.

As outlined in our submission to Government on the draft *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (**the Bill**) we consider reciprocity to be an important feature of the Open Banking system and consider it should be included from day one. In particular, a fair and balanced regime is dependent upon reciprocity.

We agree with the assessment that the concept of reciprocity raises complex issues requiring further consideration. We are available to work with Treasury and the ACCC on how the regime should be implemented and managed. We also support the work that ABA is commissioning to develop a principles framework to implement reciprocity in Australia. We consider this will assist the ACCC in this process.

Advertised product information including interest rates, fees and charges

As the Rules Framework is presently drafted it is not clear whether interest rates, fees and charges relate to advertised rates or bespoke (ie individually negotiated rates).[8] However we note that clarity has since been provided via the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2018 (Designation) which refers to "tailored" information being required to be shared.

We confirm that we consider that only advertised rates, fees and charges should be in scope for 1 July 2019 and note that in the UK model no bespoke product data is required to be made available on lending products (including interest rates).

Where interest rate discounts, fees and charges on accounts are bundled (mortgage, offset, savings, credit card) we consider that exposing the actual interest rate on one product set will not necessarily provide a more accurate representation of the customer's total situation for the purposes of product comparisons.

We consider that given transaction data will be made available via application programming interfaces (**APIs**) under the CDR it will be open to the accredited third party to look at the transaction data history and determine what has been paid/charged in the past rather than looking to what is to be paid/charged in the future. That is, it is much easier to construct what interest, fees and charges have been applied to an account rather than look to what will or could apply as this is dependent on a range of factors. The construction of fees, charges and interest paid may not represent the complete position when viewed in isolation from other accounts which are relevant to that fee, charge etc (for example, a package fee/fee waiver).

There are also technical challenges with exposing bespoke (individually negotiated) interest rates, fees and charges and we consider these cannot be overcome for a 1 July 2019 implementation.

A key challenge is that details of fees, charges and interest rates are often computed rather than stored. That is, the particulars reside within the source code of a considerable number of legacy mainframe computer programs, rather than purely being stored as data in a database.

The computation can also be based on customer behaviour (that is depositing a certain amount in an account). Computations will also only occur at certain points in time (for example the end of the month).

Obtaining these data sets is then not just a matter of copying data but a laborious extraction of business rules.

[8] Op cit n 5, pp 19-22.

In addition, data sets can be held in multiple places and across product sets. Sometimes pricing is implemented as complex pricing tables and sometimes pricing is implemented in rules engines.

Pricing that involves two or more accounts (such as a linked savings account example – see below) would require additional consideration on how to represent via APIs and additional technical complexity to extract linked pricing rules.

Example – Account with bonus interest rate

Account pays 1% interest p.a. for balances under $1000 and 2% p.a. for that part of the balance, if any, that is above $1000. There is also a bonus of 5% p.a. interest paid if $2000 or more is deposited in the account every month and also 5 Visa/Mastercard debit withdrawals are made from a linked deposit account.

Optionality for deletion or de-identification

Summary
An entity should be permitted to determine whether it is more appropriate to de-identify or destroy unsolicited CDR data and PS 4 should be amended to reflect the existing position under APP 4.

The Rules Framework Paper notes that the ACCC is considering how redundant data should be dealt with.[9] It also notes that while the Open Banking review did not recommend a right of deletion the ACCC queries whether allowing accredited data recipients the ability to retain de-identified data is consistent with the consumer-centric aims of Open Banking.

We understand the concern about the ability to retain data after uses are spent/ the data becomes redundant (unless we are required to retain the data by law). From a consumer perspective we also understand the desire to delete data in such cases.

From a technical perspective, there are a range of complexities in deleting data. For example, data from other financial institutions may be propagated throughout many bank systems under the CDR regime. To support deletion of CDR data, changes need to be made to each system in the value chain to understand the data's lineage and whether it is subject to CDR deletion/ rules.

In addition, under existing law[10] (recognising the technical challenges associated with data destruction)[11] an organisation may either destroy or de-identify unsolicited personal information. This must be done as soon as practicable if it is lawful and reasonable to do so (and that information is not otherwise permitted or required to be retained). Privacy Safeguard (**PS**) 4, as

[9] Op cit, n 5, p 56.
[10] Australian Privacy Principle (APP) 4.
[11] For example data backup for resiliency and availability purposes.

currently drafted, is more narrow than the Australian Privacy Principle (**APP**) 4 and requires entities to destroy unsolicited CDR data as soon as practicable unless otherwise required under law or a court/tribunal order, with no option for the entity to de-identify that data instead.

In contrast, PS 11 has been drafted in an equivalent manner to APP 11 in that entities can choose to de-identify or destroy CDR data as appropriate when it can no longer be used (in accordance with the Rules).

Under the General Data Protection Regulation (**GDPR**), the UK Information Commissioner's Office has recognised that deleting information from a system is not always a straightforward matter. For example, in certain circumstances, personal data may need to be retained for reasons other than compliance with laws, such as where deletion may affect the integrity of the data of other individuals.[12]

We propose that PS 4 should be amended to reflect the existing position under APP 4 i.e. unsolicited CDR data can be de-identified or destroyed to ensure the most appropriate actions can be taken with respect to such data depending on the circumstances.

Overlapping privacy regimes

As a general comment, and consistent with our submission on the Bill, we do not think it is feasible to have the APPs and Privacy Safeguards apply simultaneously, particularly where there are inconsistencies between those two regimes. Overlapping and inconsistent regimes will also make it difficult for consumers to understand their rights and the available protections.

We acknowledge the amendments that have been proposed via the Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation (**Bill**) that acknowledge the challenges for data holders that are also data recipients and look forward to the release of the rules to better understand how the overlap between the two regimes will be addressed.

Specific comments on the Privacy Safeguards are outlined below.

Restrictions on use – prohibitions on on-selling and direct marketing

> **Summary**
> Informed consent should be required for CDR data to be used for direct marketing.

PS 7 generally permits the use of CDR data for direct marketing only when permitted by the Rules and where a valid consent has been provided in accordance with the Rules. In contrast, the Framework Paper proposes that direct marketing will be prohibited entirely under the Rules.

The Framework Paper's position is significantly stricter than APP 7 which permits the use of personal information for direct marketing in particular circumstances, typically with the use of a simple means to opt-out. The GDPR also expressly permits direct marketing where it is considered a legitimate interest without requiring consent from the individual, or alternately with the individual's consent.

On this basis and to be in step with other regulations, we believe that direct marketing using CDR data should be permitted in accordance with the proposed restrictions for other types of

[12] https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

use and disclosures under the Bill and Framework Paper i.e. in accordance with the customer's express, specific and informed consent and the Rules.

Outsourcing

Summary

- Entities should be permitted to transfer CDR data to both domestic and offshore non-accredited outsourced service providers subject to appropriate safeguards being in place such as compliance with appropriate security obligations.
- For offshore transfers to outsourced providers, appropriate security obligations and contractual protections should be required, rather than consumer consent.
- Onward transfers by outsourced providers to subcontractors should be permitted subject to appropriate security obligations and contractual protections.
- Requiring a full list of outsourced service providers to be included in a CDR policy may detract from the underlying policy purpose (being a clearly expressed and transparent customer communication).

Westpac is supportive of the proposed approach outlined in the Framework Paper requiring accredited data recipients to have minimum safeguards in place in outsourcing arrangements which involve the disclosure of CDR data.

Westpac, like many other large organisations, has existing arrangements with outsourced service providers including those that utilise an offshore support model and who may, subject to appropriate technical and organisational measures being in place, have access to Westpac data to perform services for Westpac. As a practical matter, we have concerns in relation to the proposal in the Framework Paper and the Bill to obtain consumer consent to those arrangements as follows:

- PS 8 requires all overseas recipients of CDR data to be accredited entities (unless they satisfy other conditions in the Rules).

  We consider this approach is impractical for outsourced providers who provide services to an accredited data recipient and instead it should be the responsibility of the accredited data recipient to ensure an appropriate contract, risk management and processes are in place to enable the accredited data recipient to meet its responsibilities under the CDR regime. We believe the proposed approach for domestic outsourced service providers should apply in the same way to those that utilise an offshore support model.

- Section 12.1.2 of the Framework Paper states that accredited data recipients must obtain consent to send CDR data to offshore providers.

We note that this position is not consistent with APP 8 which does not require consent, and instead requires Westpac to take reasonable steps to ensure that the offshore provider does not breach the APPs (unless an exception applies). Under the APP Guidelines, recommended reasonable steps include entering into appropriately robust contracts. In addition, under the APP Guidelines, disclosure to an offshore provider in circumstances where the discloser retains "effective control" is considered a "use" rather than a "disclosure" - meaning APP 8 does not apply to such disclosures to offshore providers. We also note that an approach whereby consumer consent is required is not consistent with other recent regulatory approaches (such as GDPR which like APP 8 focuses on ensuring appropriate safeguards are in place for offshore transfers, for example via mandated contractual protections).

On this basis, we propose that the focus for offshore transfers should be on ensuring appropriate safeguards and security are in place similar to the current position under APP 8. Additionally, clarity is required as to whether the reference to "transfer" in the Bill and Rules will be treated similarly to "disclosure" under the APPs i.e. to capture access to data held in Australia by offshore entities.

- Section 12.1.2 of the Framework Paper states that outsourced providers could be restricted from any onward disclosures e.g. to their own subcontractors.

  We propose that onward disclosures should be permitted provided that a contract with the outsourced service provider requires that provider to flow down the relevant protections to their subcontractor. This is a similar position to what is required under GDPR and would ensure the chain of disclosure is rigorously protected whilst still balancing business efficacy.

- Section 6.8 of the Framework Paper states that a list of outsourced service providers must be provided in the consumer-facing CDR policy. We query the practicality of this with large organisations with complex operations that involve hundreds of service providers. Given that the CDR policy is intended to be clear, transparent and easy to read, we believe requiring a full list rather than categories of providers may make it more difficult for customers to understand and evaluate the nature of those providers to whom their data will be disclosed.

The Bill requires all overseas recipients of CDR data to be accredited entities. The Rules Framework Paper contemplates permitting accredited data recipients to outsource services to non–accredited service providers (domestic) provided the use is within the scope of the original consent from the individual and subject to specific rules.

We support this proposal subject to it being aligned with existing law relating to use of offshore outsourced providers, namely that it reflects that consent is not required so long as entities have taken reasonable steps to ensure that the offshore provider does not breach the APPs.[13]

[13] APP 8.

Minors

We note that the ACCC does not propose to make rules that would treat minors differently to any other consumer who may take advantage of the CDR.

We note under the Privacy Act, minors are presumed to not have capacity if they are less than 15 years of age. We consider if minors are to be included in the CDR regime that it may be appropriate to follow that guidance regarding capacity.

Key areas that should not be in scope

Derived data

In terms of derived data we re-iterate our views from earlier submissions that derived data should not be in scope. We agree with ACCC's assessment that 'transformed' or 'value-added' can encompass a spectrum of activities from simple transformation of data (such as calculation) to analysis. In this respect we welcome the clarification provided via the Designation and Bill that data holders will only be obliged to share data specified in the Designation (and not derived data).

We also welcome the ACCC clarification that while some data sets may include derived data this does not extend to data that results from 'material enhancement' as contemplated by the Open Banking review. However we note that some of the data sets contemplated by the ACCC for inclusion (such as metadata - geolocation) would constitute 'material enhancement' and should therefore not be included.

Other Issues

Privacy Safeguard 6 – use or disclosure of CDR data

Summary
The permitted scope for use of CDR data should be expanded, (to include other appropriate authorised uses) so that consent is manageable, in line with current Australian privacy law and other data protection regimes such as GDPR or alternatively clarity provided as to when the CDR regime will cease to apply to data and the APPs commence. We look forward to seeing clarification in the rules on this issue.

Under APPs 3 and 6 respectively:

- collection of personal information is restricted to collection that is reasonably necessary for a business' functions and activities; and
- use or disclosure of personal information is restricted to the primary purpose for collection or a reasonably expected secondary purpose which relates to the primary purpose.

The collection of sensitive information is the only collection for which the individual's consent is required.

Generally, PS 6 permits an entity to disclose CDR data only if permitted by the Rules, even if the consumer has provided a valid consent. The Framework Paper has suggested that only the following disclosures would be permitted under the Rules:

- disclosures made on the basis of having obtained consent, authorisation and/or authentication in accordance with the Rules (with consent to be freely given, express, informed, specific, time limited and easily withdrawn); or
- disclosure of data by a data holder directly to the consumer.

We believe that this is a very restrictive scope of permitted disclosure, particularly where there are overlapping regimes. For example under GDPR, consent is not required to disclose, use and process personal data – provided an entity can rely on one of the lawful bases for processing such as relevantly, legitimate interests or contract.

Limiting the use of CDR data to where such specific active consent has been obtained will create significant operational difficulties in practice. Given that personal information would be a subset of what would be considered CDR data, the overlap between regimes would mean maintaining separate organisational structures and management of data systems to ensure separate treatment of data received via the CDR regime as opposed to traditional avenues which would be an excessive burden on businesses and preclude the provision of efficient services to consumers. For example, it would lead to separate systems and processes being required based on how the same type of data is received. Currently, Westpac requests electronic copies of payslips from customers to verify their income for lending purposes. If the same income information was supplied to Westpac under the CDR regime, this could result in the same information having to be treated entirely differently based on how the information was received.

We also query how change may be efficiently managed. For example, if Westpac receives a customer's CDR data for a specific purpose (as specified in the original consent), and subsequently the same customer decides that the data ought to be used for a different purpose, would a new freely given, express, informed, specific, time limited and easily withdrawn consent be required from the customer for that use prior to use?

We also confirm our earlier comments in relation to the Bill which acknowledges the challenges for data holders that are also data recipients and look forward to the release of the rules to better understand how the overlap between the two regimes will be addressed.

Record keeping

We note the record keeping requirements are largely consistent with the Open Banking Report recommendations.

Section 14.3 of the Framework Paper states that an accredited data recipient will be required to keep and maintain records relating to any outsourcing arrangements the accredited data recipient has in place, any transfers of consumer data outside of the CDR regime and the subsequent use of such data.

As mentioned above, due to the size and complexity of Westpac's operations and its relationships with many service providers, a requirement to maintain records of "all outsourcing arrangements" would be complex.

We also note that the proposed requirement in section 14.3 of the Framework Paper to keep records of "the subsequent use" of consumer data that has been transferred out of the CDR regime is potentially very broad and may be difficult or impossible to determine. We presume this is only intended to apply to transfers to an outsourced service provider (as opposed to other recipients that receive CDR data outside of the CDR regime at a customer's request). For example, if a consumer directs an accredited data recipient to disclose their data to a non-accredited entity (as contemplated in section 12.1.1 of the Framework Paper), the accredited data recipient is required to notify the consumer that the CDR protections no longer apply, that the non-accredited entity's handling of their data may not be covered by the Privacy Act, and disclosure is at the consumer's own risk. In this case, the accredited data recipient is not liable for misuse once the data is transferred, and it would be inconsistent with this to require the accredited data recipient to keep records of "the subsequent use" of the consumer's data. We request that any record keeping requirements be limited to outsourced service providers and then in accordance with the "Outsourcing" section above.

Penalties

Summary
The penalties should be aligned with the existing penalties under the Privacy Act.

In our submission in relation to the Bill, we noted that the civil penalties regime under the Privacy Safeguards is far more significant than the existing civil penalty provision relating to the APPs. Additionally, under the Privacy Safeguards, there is no requirement for a breach to be serious or repeated in order for a civil penalty to be applied.

In addition to this, the Framework Paper contemplates all Rules which impose obligations on data holders or ADRs to be subject to additional civil penalty provisions. It is unclear to us how the provisions will apply across the CDR regime as a whole and we do not believe this is aligned with the policy intent of the CDR regime.

We acknowledge that this issue appears to be under consideration by Treasury.

Dispute resolution

We agree with the position in the Rules Framework Paper that a particular form of ADR should not be mandated across the board as the most appropriate form of ADR will differ based on customer size, type and account complexity.

We also agree that the list of proposed internal dispute resolution procedures to be set out in the Rules is appropriate in setting out how CDR disputes should be dealt with internally.

Westpac's current practices aim for resolution as soon as possible, but no later than 45 days after becoming aware of the dispute. However, in some cases, timing is affected by factors such

as the complexity of the matter or customer response times. In those circumstances, it is possible that resolution times may exceed 45 days. ASIC Regulatory Guide 165 *Licensing: Internal and external dispute resolution* (**RG165**) and the 2019 Banking Code of Practice both recognise this and allow for complaints to go beyond this timeframe. Westpac proposes that to manage this, in line with both RG 165 and the 2019 Banking Code of Practice, the entity be required to provide updates to the complainant if the dispute is not resolved within 45 days.

We welcome the opportunity to discuss the issues raised in this submission. Please do not hesitate to contact Roza Lozusic at [redacted] if you would like any further information or wish to discuss.

Yours sincerely,

Michael Choueifate

Head of Government Affairs

Attachment A – Commentary on proposed data set inclusions.

Note that this commentary specifically relates to the category of data sets as applied to retail products in scope for the 1 July 2019 start date (deposit, transaction, credit and debit cards) and not for corporate customers and products.

Customer Data			
Proposal	**Technical considerations**	**Privacy/other considerations**	**Recommendation**
Customer name		For 1 July 2019, recommend that individual customer data to be shared only relates to the customer who is giving the consent due to privacy concerns. e.g. for one-to-sign joint accounts, the details of the customer(s) who did not give consent would not be shared.	Agree that these details should be included, subject to appropriate constraints, for example: • only the data of the individual who is giving consent will be shared • customers can opt out of sharing this data and still take advantage of the CDR.
Customer contact details			
Customer account number(s)		Customer account numbers could be credit card numbers or BSB and account numbers. Disclosing this information unnecessarily increases the risk of fraudulent transactions. We recommend that for 1 July 2019 these numbers be masked, e.g. account number 123456789 is represented as XXXXX6789. A further benefit of this is that, for example, less stringent security controls would be required for data recipients thus allowing greater participation.	We agree that these details should be included subject to the security measures and considerations outlined in the "privacy/other considerations" section.

Payee lists on the account(s)		We need to consider the impact to the payees of their BSB and account number(s) being shared given privacy considerations. Without due consideration, sharing this detail would also increase the risk of fraudulent transactions. In addition there is the potential for errors to multiply since it relies on payer (presumably account holder) entering payee details accurately.	Given it is not feasible to obtain the consent of each payee in a typical payee list, our recommendation is to not include these details for 1 July 2019 and work through the privacy implications fully prior to implementation.
Direct debit authorisations on the account(s)			
- Direct debits Where the customer has given their deposit account details (BSB and account number), or their credit or debit card details (card number, expiry date and security code), to allow a merchant or service provider to debit their account regularly to pay for the services they provide them.	To comply with the 2019 Banking Code of Practice amendments, Westpac is building a technical solution to identify direct debits from an account's transaction history. The Banking Code of Practice already caters for the constraints that banks have in producing this data: • Restricted to the previous 13 months • The list will include only those direct debits and recurring payments that are known to the bank from the information they receive about the transactions on the account.		Agree that these details should be included subject to the limitations outlined in the 2019 Banking Code of Practice. The rules should acknowledge that as this data is derived from analytics that there is a high risk the data may be inaccurate. Therefore, there should be no guarantee of accuracy, nor a requirement to notify in the event that an inaccuracy is found.
- Scheduled and future-dated payments Where a customer has used their bank's online banking channel to instruct the bank to send a fixed amount of money from their account (usually a deposit account or a credit card account) to a third party account using either the third party's BSB and account number or their BPay Biller Code at some time in the future. Once-off payments are referred to as "future-		To the extent a scheduled or future-dated payment recipient could be an individual, need to consider the impact to the recipient having their account number(s) shared given privacy considerations. Without due consideration, allowing this would increase the risk of fraudulent transactions.	Given it is not feasible to obtain the consent of each payee of each scheduled payment, our recommendation is to not include this sensitive data for the 1 July 2019 implementation and work through the privacy implications fully prior to implementation. We agree, however, that other fields of this data should be included, such as payment amount and payment schedule.

dated payments". Payments that recur on a fixed schedule are called "scheduled payments".			
- Scheduled and future-dated transfers Where a customer has used their bank's online banking channel to instruct the bank to send a fixed amount of money from their deposit account to another one of their accounts. Once-off transfers are referred to as "future-dated transfers". Payments that recur on a fixed schedule are called "scheduled transfers".			We agree that these details should be included.
Account-level information – authorisations on the account		We need to consider the impact to the authorised individuals having their account authorisation details shared by another authorised individual given privacy considerations. Without due consideration, allowing this would increase the risk of fraudulent transactions.	"Account-level authorisations" are not defined. We assume that this refers to other parties to the account who were set up at the time of account opening. Recommend inclusion of this data without revealing the identity of the other individual parties to the account. e.g. this account is held jointly with one other party whose first name is "Jane" (but do not include last name for contact details).
Account-level information – account-level contact details		We need to consider the impact to the authorised individuals having their contact details shared by another authorised individual given privacy considerations. Without due consideration, allowing this would increase the risk of fraudulent transactions.	The privacy considerations would need to be worked through.
Any unique identifiers associated with the listed items		To the extent a unique identifier could be considered personal information, need to consider the privacy considerations.	This is a relatively complex interplay between functionality, privacy and security. We recommend the ACCC specifies the unique identifiers that it deems important and gives the standards body discretion in defining this and the privacy issues be appropriately

			considered.
Transaction Data			
Proposal	**Technical considerations**	**Privacy/other considerations**	**Position and Recommendation**
The opening and closing balance of an account for the period specified			Agree that it should be included
The date on which a transaction was made			Agree that it should be included
The relevant identifier for the counter-party to a transaction	Including this would be difficult for Westpac and the industry as a whole. In some cases transactions are shared between banks and within banking systems including information about the payment (eg 'deduct this much from that account' is exchanged rather than 'pay this account this much from that account'). The type of exchange depends on the system of record and bank.		Agree that it should be included, if this identifier for this transaction is visible in the data holder's online channel. As per other commentary, need to evaluate the privacy considerations of the specific data about individual counter-parties which is proposed to be disclosed.
The amount debited or credited pursuant to the transaction			Agree that it should be included
The balance on the account prior to and following a transaction			We consider we can provide a balance at the current point in time. We can also provide end of day, end of month, current and current available balance. The data is not typically held by banks but is derived at the time of display and calculated from the opening balance and applied transactions.
Any description in relation to the transaction, whether entered by the consumer or the data holder	Statement narratives would fall into this category. Statement narratives are value-added data in the sense that they are usually constructed from other fields.	There is potentially sensitive data in this field – credit card numbers, phone numbers, account numbers etc. Suggest that on 1 July 2019 this field be masked given the considerations raised above concerning fraud risk.	Agree that it should be included but it should be masked for 1 July 2019. e.g. credit card numbers should be replaced with a format such as XXX 1234 in line with our earlier comments.
Any identifier or categorisation of the transaction by the data holder (that is, debit, credit, fee, interest, etc.)			Agree that it should be included to the extent that it does not involve derived data. As an example, it should include

			whether a transaction is a debit, credit, fee or interest but should not include whether a transaction was related to groceries. Transaction categorisation that is achieved through complex analytics and therefore is material enhancement is out of scope for the CDR regime. Additionally, for the details we agree should be included, they should only be required to be disclosed where the transaction is also categorised in the bank's online channel.
Transaction metadata			Transaction metadata is achieved through complex analytics and there is material enhancement which is out of scope. As per comments above we understand value added data which is materially enhanced is out of scope for Open Banking.
Product Data			
Proposal	**Technical considerations**	**Privacy/other considerations**	**Position and Recommendation**
Product type			Agree that it should be included
Product name			Agree that it should be included
Product prices	*See body of submission*		*See body of submission*
All fees and charges, including interest rates, associated with the product, and the circumstances in which these apply	*See body of submission.*		*See body of submission*
Features and benefits	Many of these are not stored in a structured fashion. Suggest that for 1 July 2019, this is a free text field.		Please see comments elsewhere about complexity of providing tailored information/information not contained in a structured form in a database.
Terms and conditions	These are not stored in a structured fashion. Suggest that for 1 July 2019, this is a free text field.		Agree that standard terms and conditions for current products should be included but as a hyperlink to the relevant PDF.
Customer eligibility criteria	Many of these are not stored in a		Agree that it should be included but as a

	structured fashion. Suggest that for 1 July 2019, this is a free text field.		link to PDF.
Product data that relates to an identifiable or reasonably identifiable person, i.e. where it relates to an account or accounts that a customer holds.	Producing this data, especially in a format that matches the likely standard for 5.3.3, requires a long lead time to fully implement. Partial implementation introduces the risk of a misinformed decision by the customer.		As per comments elsewhere in our submission.