

# RESPONSE ON OPEN BANKING REGULATIONS AND STANDARDS UNDER THE CUSTOMER AND PRODUCT DATA BILL

---

18 October 2024.

# INTRODUCTION AND OVERVIEW

## *Introduction*

- 1.1. ANZ Bank New Zealand Limited (**ANZ**) is grateful for the opportunity to provide feedback to the Ministry of Business, Innovation & Employment's (**MBIE's**) consultation on the Discussion Paper on Open Banking Regulations and Standards under the Customer and Product Data Bill (**Discussion Paper**).
- 1.2. ANZ is aware the New Zealand Banking Association (**NZBA**) has also provided an industry response on the consultation. ANZ has contributed to and supports the relevant aspects of that response.

## *Contact*

- 1.3. Please contact [REDACTED] if you would like to discuss the contents of this response.

## *Confidentiality*

- 1.4. ANZ requests that the information identified in this response as requiring confidentiality are kept confidential on the grounds of commercial sensitivity. If MBIE receives a request to release our response under the Official Information Act, we ask that MBIE consult with us, and our preference is that the information identified is withheld.

## *Structure*

- 1.5. The front end of this submission contains ANZ's high level comments on each section of the Discussion Paper, using the same numbering as the Discussion Paper. Attachment A includes three illustrative scenarios of possible use cases in open banking, and the complex relationships, data sharing and consent implications that may result. Those use cases, or "scenarios" are referred to throughout this document. In addition, responses to the individual questions in the Discussion Paper are included in **Attachment B**.

## *Overview and General Comments*

- 1.6. ANZ acknowledges the importance of the Customer and Product Data Bill (**Bill**) and the Open Banking Regulations and Standards (**Regulations and Standards**) to promote competition, consistency of outcomes and enable better financial services for consumers in New Zealand. We support a regime that is efficient, trustworthy, and secure.
- 1.7. While we have provided detailed comments on the Discussion Paper in this submission, ANZ draws MBIE's attention to our key concerns below. Further detail on these points is set out in the body of this submission and **Attachment B**.
  - a) Sufficient time has not been provided for the development of the open banking regulatory regime, or its implementation for industry to appropriately comply with.
  - b) Despite the Commerce Commission indicating its intention to designate the interbank payment network under the Retail Payment System Act, the scope of this designation remains unclear.
  - c) ANZ agrees with the NZBA that the current approach is causing uncertainty. We ask that a single regulator model be considered, and if that is not an option then for the Commerce Commission and MBIE to provide further clarity about how the two regimes will fit together.
  - d) Industry should be offered an opportunity to further engage with government to provide certainty around future regulations. It would be beneficial for the sector to be given the opportunity to review an exposure draft of the regulations to address any potential ambiguity.

## 2. STATUS QUO AND PROBLEM DEFINITION

- 2.1. ANZ supports open banking and has invested over [REDACTED] to date in its implementation. We are on track to meet the API Centre's mandatory implementation plan (version 2.1) by November 2024.
- 2.2. With a significant portion of ANZ mobile customers already using open banking services, we expect to see continued growth in adoption and value for customers in line with the API Centre rollout of standards.
- 2.3. We disagree with paragraph 20 of the Discussion Paper that banks' advantages as incumbent holders of customer data and our existing payment networks will undermine the effectiveness of open banking. Industry has made considerable effort to initiate open banking in New Zealand and is presently incurring the expenses to achieve this. We have been working hard to implement open banking in a way that maximises customer benefit for the investment whilst still taking our security obligations as holders of customer funds and data seriously. Our recent achievements include:
  - a) [REDACTED] of our eligible mobile customers have now made an open banking payment
  - b) August 2024 was a significant milestone for ANZ, with open banking payment volumes [REDACTED] over the previous highest volume month
  - c) We are live with Worldline, and Blink Pay. We have also signed an agreement with Qippay and have a number of other third parties in our pipeline
  - d) We have been able to do this without open banking regulation and with competition law restrictions on our ability as an industry to collaborate on risks and liability, which has been very challenging. In contrast, the UK took ~5 years after regulation to reach a 14% adoption level across the digitally active population<sup>1</sup>
- 2.4. In our view, the problem definition in the Discussion Paper also does not identify the role of central investment and legislation in facilitating the adoption of open banking. To date, New Zealand's industry has progressed open banking despite the lack of a regulatory regime or government investment. However, we contend that future government support will be necessary to establish a regime that is fit for purpose and ensures consistent outcomes.

## 3. OBJECTIVES

- 3.1. Having already invested substantially in open banking, we support the comments at paragraph 32 of the Discussion Paper that a designation should not require inefficient investments. In our view, this means that open banking should support and prioritise high value use cases that end-customers want (and will use), and that are practical and supported by a cost/benefit analysis.
- 3.2. For that reason, ANZ submits that the criteria in paragraph 35 of the Discussion Paper should be amended to refer to "wide customer uptake" and "valuable customer use cases", as well as a practicality criterion. We also submit that the reference to "efficient investment" should expressly include a cost/benefit criterion for each use case and consider efficiencies both from the perspectives of banks and third parties.

## 4. THE SCOPE OF AN OPEN BANKING DESIGNATION

- 4.1. Providers of banking services to customers should ultimately be covered by the open banking designation. ANZ proposes that the scope of designation include a principle of reciprocity, encouraging early participation by the designated data holders. In Australia, in order to ensure parties who 'take' data will also 'give' data, banks could only receive information if they were participating in their consumer data rights (CDR) regime. This led to a number of banks participating ahead of a

---

<sup>1</sup> The open banking impact report 2024, March 2024, <https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-2024-march/adoption-analysis>

requirement to do so. For example, it is proposed that Kiwibank would retain its existing 2026 timeframes to join open banking. If that happened, under a reciprocity model it would be allowed to take additional time but would not be allowed to take data until it is ready to also give data.

- 4.2. On the identity of the designated banks, ANZ supports the same principle of reciprocity, meaning that if other banks (including digital-only banks) wish to receive data, then they should also be designated as data holders and participate fully in open banking.
- 4.3. ANZ also considers the date on which designation is proposed to commence (1 December 2025) is unrealistic and would likely introduce unforeseen risks and compromise quality. It will only be practicable for ANZ to comply with the requirements of the Regulations and Standards by 1 December 2025 if the detailed rules for open banking:
  - a) are consistent with version 2.3 of the current API Centre Standards, and do not contain any additional scope, requirements or functionality (technical or operational), including items discussed in this paper, such as (but not limited to): Performance requirements and reporting, Support requirements (L), Integration into a centralised register (M), Enablement of Web channels\* for consent management (XL), Multi-authorisation payments and potentially data sharing (XL), Product data\* (XL), Any changes to industry standards\*, Ability for consent to contain details of opt in aspects of the consent (M) or Access to 7 years of data\* (XL);
  - b) if MBIE leveraging work underway within the API Centre develop commonly agreed standards for areas such as accreditation, third party onboarding, authorisation, and risk settings for use cases; and
  - c) if the "equivalency principle", as set out in the API Centre Equivalency Principle Policy<sup>2</sup> in the current open banking arrangements and exemption processes, is maintained.
- 4.4. We agree with the position in paragraph 52 of the Discussion Paper that only requests by accredited requestors should be in scope, and direct-to-customer requests should be excluded.
- 4.5. ANZ also agrees that the key focus for designated customer data should be on information that customers already have access to through retail and small business digital channels. In Australia, which has a wide scope of designated data, our related entity Australia and New Zealand Banking Group Limited (**ANZ Australia**), found it resource intensive and challenging to meet timeframes where data was not available or already provided to customers digitally. Consequently, we consider designation needs to be right-sized, based on evidence of customer demand and demonstrate a cost/benefit analysis. In particular, we submit that:
  - a) in relation to paragraph 56(a) of the Discussion Paper, customer identifiers should be restricted and if used should be hashed/encrypted for privacy and security reasons. A customer identifier is a 'unique identifier' under IPP 13 of the Privacy Act and is unique to each bank for its own operational use. In effect, this may be viewed as 'over collection' and may lead to a breach of IPP 1 given that it would not be linked to a 'purpose'.
  - b) in relation to paragraph 56(d) of the Discussion paper, "*information about the customer's eligibility for services and offers provided by the data holder*" should be clarified to relate specifically to the designated account types (rather than all services and offerings);
  - c) we strongly disagree with the proposal in paragraph 61 of the Discussion Paper that 7 years of data should be provided. According to ANZ Australia, it is not aware of any evidence of realistic use cases for this amount of data. In its experience, 90% of requests for transaction history data (in Australia) are for data less than 3 months old, making 7 years of data of little benefit to customers. ANZ currently enables customers to view 2 years of transaction data in our digital channels and share 2 years of transactional data through open banking services. Therefore, we would support a 2-year timeframe being applied to historical data requests to align with current trends and help reduce compliance costs;

---

<sup>2</sup> <https://www.apicentre.paymentsnz.co.nz/standards/using-standards/equivalency-principle-policy/#:~:text=The%20Equivalency%20Principle%20Policy%20clearly.the%20bank%27s%20terms%20and%20conditions.>

- d) in relation to paragraph 58 of the Discussion Paper, designation should only apply to retail and small business banking customers, as this accounts for the majority of use-cases. Larger customers like corporate and institutional customers tend to set up their own bespoke data sharing arrangements using their preferred external platforms, tools and processes, so there is no need for the government to act in this space; and
- e) attempting to designate product data may be unwise at this point, given the complexities of implementing customer data in the intended timeframe. ANZ considers that this should be deferred to a later point in time.

## 5. THE BENEFITS, COSTS AND RISKS OF AN OPEN BANKING DESIGNATION

5.1. While we agree that there are many benefits to open banking, we note that:

- a) there is little evidence of the scale of these benefits and the timeframe over which they are delivered;
- b) the designation of open banking will result in additional risks to security, privacy and confidentiality that will need to be managed carefully and with industry input in order to operationalise. ANZ holds concern that the risks associated with accredited requestors acting as intermediaries and on-sharing data or action rights to unaccredited third parties have not been adequately addressed. As set out in previous submissions, we do not believe that relying on the Privacy Act alone for these scenarios is sufficient. ANZ has provided further comments on the interface with the Privacy Act in its response to question 14 in **Attachment B**; and
- c) the Discussion Paper does not consider the risk associated with a data request or an action initiation conflicting with other laws. For more information, refer to our previous submissions on the Bill, and the submissions provided by the NZBA.

5.2. We understand every requirement in the Regulations and Standards on data holders will carry a direct cost for the banks. While we are already managing the costs of implementing some of these requirements via the API Centre, the extra items in the Discussion Paper (for example the requirement to provide up to 7 years' data) are likely to add materially to those costs. ANZ has invested substantially in open banking, and if the Regulations and Standards deviate from the API Centre Standards, much of this investment may be lost.

5.3. Further, participants need fair and reasonable timeframes to implement new standards. Without this, the open banking environment may not be fit for purpose, impacting the regime's effectiveness and increasing industry costs to address subsequent changes and issues.

5.4. On this basis, and given the desire to move quickly, we suggest that these factors point towards starting conservatively and expanding the scope of the designation as evidence of the benefits of open banking (and the areas which will have most benefit) become clearer, and the risks have been adequately mitigated.

## 6. ACCREDITATION CRITERIA

6.1. ANZ supports robust accreditation criteria to protect customers against scams, fraud and security issues, support confidence and uptake, and ensure that accredited requestors can meet their obligations. In our view, accreditation should not be a "one and done" exercise, but instead be subject to ongoing review. This will build trust and give customers more confidence in the reliability of the open banking regime.

6.2. ANZ is also concerned that (at least without adequate insurance and guarantee requirements) banks or customers risk not being compensated for losses that may arise where accredited requestors do not meet their obligations. In addition, scenarios with higher risk exposures (such as from higher

payment volumes) should be restricted to those with proven capabilities, maturity and adequate capital or insurance to redress customers if something goes wrong.

- 6.3. In our view, insurance should not be a mitigation for poor risk controls and should be adequate to cover the accredited requestor's potential liability arising through the open banking regime. Risk may also change over time, so insurance levels may need to be reviewed, for example as an accredited requestor grows and processes more requests or higher value payments.
- 6.4. In relation to dispute resolution:
  - a) ANZ considers that the reliance on current established dispute schemes requires further deliberation. Further comments are provided in response to question 22 in **Attachment B**.
  - b) In addition to the above, a primary concern for ANZ is the growing number of scams in the financial sector. We believe the introduction of Open Banking will not only increase the volume of scams but also change the nature of the fraudulent activity due to third party involvement.
  - c) Scams continue to be an issue for all banks, in particular, money transfer and crypto currency type of merchants/goods. Considering this, MBIE should again examine whether the schemes in their current form will be able to appropriately manage this new scope of complaints, and likewise if the schemes in their current form are the appropriate channel to address these disputes (also noting that while scams and fraud will sometimes have a privacy aspect this is not necessarily the case).
- 6.5. As mentioned in our submissions on the Bill, we have serious concerns about the sole reliance on the Privacy Act for information security, and strongly support:
  - a) a regime that treats all customer data and action initiation requests the same (regardless of whether that information is "personal information"); and
  - b) specific technical and organisational security requirements and maturity, ideally consistent with those in Australia where most of the designated data holders already operate (so that work done there can be leveraged in NZ). This aligns with "option 3" in paragraph 114 of the Discussion Document.
- 6.6. In relation to our anti-money laundering and countering financing of terrorism (**AML/CFT**) obligations, it is not immediately clear whether banks would have an obligation under the AML/CFT Act to conduct customer due diligence (**CDD**) on accredited requestors (or unaccredited requestors to who accredited requestors are on-sharing data or action rights). For efficiency, we support MBIE conducting CDD on requestors as part of the accreditation process on behalf of the data holders and permitting data holders to rely on this.
- 6.7. Finally, as explained in previous submissions on the Bill, ANZ is concerned about the ability of accredited requestors to share data with unaccredited third parties, and the complexities and risks that this creates outside the protections of the open banking regime. We have illustrated some of these concerns in the scenarios in **Attachment A**. We would support a separate, higher level of accreditation for accredited requestors that intend to act as intermediaries for an unaccredited third party, including:
  - a) higher insurance requirements,
  - b) a higher standard of compliance with its policies, and
  - c) express responsibility for the acts and omissions of those unaccredited third parties that it shares requests with or processes on behalf of.

## 7. FEES

- 7.1. ANZ does not intend to charge customers for accessing their data.
- 7.2. However, a fee system for accredited requestors that allows it to recover its costs would be required e.g., costs to service a request, ongoing maintenance and support, enhancements, and recovery of losses due to fraud and scams.

- 7.3. We therefore support the fees option at paragraph 125(c) of the Discussion Paper, which states that regulations should set pricing principles, such as requirements for them to be fair and transparent, and in line with efficient long-run costs.

## 8. DETAILED RULES FOR OPEN BANKING

### *Express and informed consent*

- 8.1. Informed and explicit customer consent is central to the new regime.
- 8.2. ANZ supports specific consents and submits that bundled consents and broadly drafted consents (e.g., that include categories or general uses or recipients of data) should be explicitly prohibited. In other words, where a purpose is specified by an accredited requestor, this should not be a broad or generic purpose (such as 'data sharing' or 'open banking services'), but instead should provide a meaningful description of the data use to the customer, so that they can make an informed choice.
- 8.3. In addition, although the Discussion Paper does consider some additional consent requirements for intermediaries (see paragraphs 141 – 146), it does not contemplate that:
- a) unaccredited third parties might continue to on-share data further to fourth or fifth parties, outside the protections of the Bill;
  - b) an intermediary might use the customer data itself (in addition to passing it on to unaccredited third parties). In our view, consent to sharing with a third party should not be conditioned on consenting to use of data for other purposes by the intermediary.
- 8.4. ANZ submits that customers should be able to view and track all consents with any third party they have consented to share data with. We consider it is unreasonable to expect customers to remember and log into multiple portals provided by different intermediary services to view, track and amend consents. Similarly, customers and other account signatories should be able to see the same consent data regardless of whether they are viewing their consents via a third party or through a bank. We believe additional analysis is required for how long consent requests should stay open for approval and addressed in Standards development.

### *Fraud mitigation and payments*

- 8.5. In addition to robust consent mechanisms, there should be obligations on all parties to undertake prudent fraud and financial crime protection measures, such as bot checks and sanctions checks.
- 8.6. For this to be feasible, all parties will need visibility of the identities of individuals and businesses in the chain of requests for a payment, including the identities of any intermediaries and unaccredited parties processing the request. Please see **Attachment A** for further illustration. ANZ and other banks have agreed practices to reduce likelihood of scams/fraud (for example we have agreed not to share payment links in emails or texts). We suggest that accredited requestors (and any unaccredited parties involved in a request) should also operate consistently with these rules.
- 8.7. ANZ supports the principle that accredited requestors should be responsible for unauthorised payments and that they should reimburse banks where the banks reimburse customers. However, clarity is needed on how this will align with the proposed voluntary reimbursement process for scam victims. Moreover, we are also concerned about our ability to recover remediation amounts, especially in events affecting multiple payments— this could topple an accredited requestor, and our ability to recover amounts via insurance payments. As previously submitted, it is for this reason that ANZ supports a safe harbour from liability that may arise in the context of a fraudulent payment, where we have complied with our requirements under the Bill and Regulations and Standards in good faith.
- 8.8. We reiterate that banks processing open banking payments should not be liable for losses caused by the errors or omissions of other parties, or where they have been the victims of crime. This is central to our ability to process payments quickly and in high volumes.

### *Joint accounts and secondary users*

- 8.9. Joint accounts, multi-signatory accounts and secondary users create additional layers of complexity for consents, particularly when the data is on-shared by an intermediary. For example, if one account signatory authorises data sharing with an intermediary, and then another party authorises the intermediary to on-share data to an unaccredited party, it is not certain that the original account signatories would have visibility of that. Please see **Attachment A** for further illustration.

## 9. STANDARDS FOR OPEN BANKING

### *Standards for open banking*

- 9.1. ANZ supports leveraging the existing open banking standards in the open banking regime and the work that industry has done to date. ANZ is working towards compliance of version 2.1 and v2.3 of the API Centre's implementation plan and standards.
- 9.2. There are three areas of concern for ANZ in the v2.3 standards:
- 1) **Customer statement data is not available** – The statements standard requires that we provide statement periods. This data is not available to our customers for accounts other than Credit Cards. Periods are used to generate pdf statements and then not accessible to our systems. Statement data is not in scope for the Australian CDR.
  - 2) **Statement files break ‘account centric’ consent model and introduce privacy risks** – The statements standard requires that we provide customer statement files. Without statement periods we are unable to generate statement files, which places sharing of the customers pdf statements in scope for ANZ. This is problematic because:
    - i. Customer PDF statements contain transactions for the account for the statement period, however they also include addition information about other accounts and/or personal information of the other parties associated with the account such as addresses, joint account holder names, lending limits and pricing.
    - ii. The current industry consent model is account and date range specific, meaning that only information about that account within the consented date range and for the specified account can be shared. Pdf statements include information beyond the scope of the account and potentially outside of the consent date range. For example, a credit card statement is for 14<sup>th</sup> Jun – 14<sup>TH</sup> July and a customer consent to allowing us to share transactions on that account between 1<sup>st</sup> June and 30<sup>th</sup> June.
    - iii. Given the level of investment into modern data integration services to support open data that is machine readable, we suggest that all parties should be encouraged to migrate to these secure services, rather than investment in standards that will allow further reliance on legacy, inefficient, print formatted .pdf statements. PDF statements are not in scope for the Australian CDR.
  - 3) **Use of online banking credentials in redirect to web** – Use of online banking credentials will increase the likelihood customers become victims of phishing attacks and will make it harder for customers to distinguish between a scam/fraudulent website, a screen scraping service and a legitimate open banking service. This is contrary to current education, messaging and work to protect customers. We acknowledge that the API Standards do not stipulate or mandate the use of online banking credentials, but they do not prohibit their use either and do not provide alternatives. ANZ strongly suggests that consideration be given to expressly prohibiting the use of bank credentials, as is the case with the Australian Consumer Data Right.
- 9.3. ANZ will continue to work with the API Centre on these matters and intends to apply for an exemption.



## 10. IMPLEMENTATION, MONITORING AND REVIEW

10.1. ANZ supports retaining existing institutional arrangements via the API Centre.

## ATTACHMENT A

### Overview

In this attachment we outline possible sharing models and scenarios with examples that could eventuate under the proposed designation, due to gaps or interpretation of the proposed rules.

### Disclaimer

- The scenarios below provide several fictitious customer propositions. Scenarios may or may not be used today. The consent approval and consent management dashboard are indicative only. Only information necessary for illustrating the scenarios are included. They do not meet all requirements required for customer disclosure and informed consent.

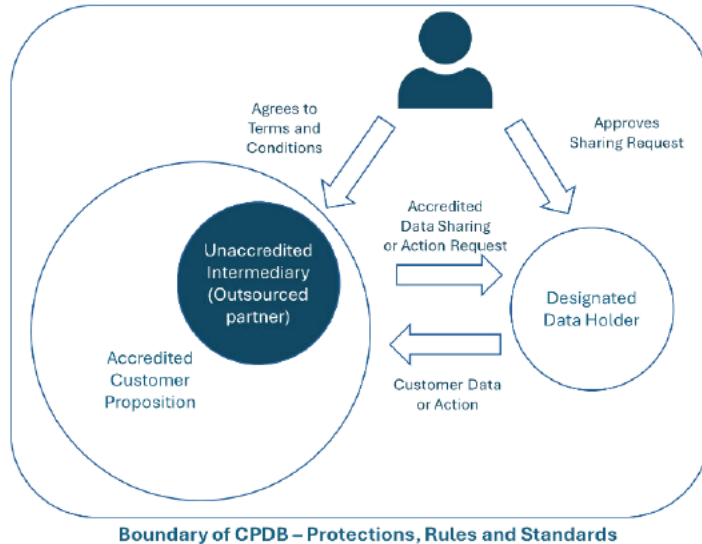
**Sharing models, scenarios and examples start on the next page.**

## Summary of sharing models and scenarios



### Model 1 - Sharing directly with an accredited recipient

In this model customers use and share directly with accredited customer propositions.



- Customers are only required to agree to one set of terms and conditions.
- Customer propositions are accredited under the Bill.
- There is no on-sharing of data or action/payment rights.
- The customer is always covered by protections under the Bill and/or the Regulations and Standards throughout their experience.
- The customer propositions may or may not use a non-accredited intermediary as an outsourced provider only. Outsourced providers provide a service only to the customer proposition, are usually hidden from the customer and operate within the same terms and conditions.
- This is the easiest to understand and safest sharing model for customers but it is unlikely to be the most common sharing model.

#### Examples:

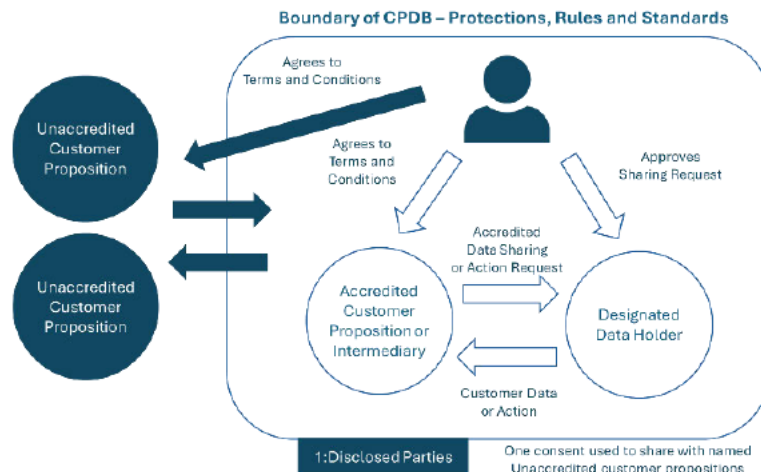
- Scenario 1a - Sharing directly with an accredited recipient, page 17.
- Scenario 1b - Sharing directly with an accredited recipient (Using an outsourced intermediary provider), page 18.

#### Model Rating

Disclosure, scope, purpose and intended use of the data that is not necessary to provide the service.	Clarity of liability, customer protections and redress.	Visibility and consistency of consent management and respecting the authority of all customers	Data holder fraud assessment and operational support.	Ease of participation for third parties.
<p>Sharing with one party for one purpose.</p> <p>Customer only needs to agree to one terms and conditions.</p> <p>Clear to the customer what service they are using and what is and is not required to provide that service.</p>	<p>All parties are accredited, operate with the Bill boundaries. No on-sharing.</p>	<p>Approver can view and manage their consents consistently between data holder and customer proposition. Joint account holders have full visibility of sharing arrangements on accounts they hold authority on, who sharing is with, who approved it and they can revoke sharing on accounts</p>	<p>Data holders have visibility of end recipient of data or payment to inform fraud assessment and provide customers with support.</p>	<p>All customer propositions must be accredited that may limit uptake</p>

## Model 2 - Sharing with an unaccredited customer proposition (disclosed during consent)

In this model customers share within an unaccredited customer proposition via accredited intermediaries. Customers start their journey within an unaccredited customer proposition. After agreeing to the terms and conditions of the customer proposition they are usually referred to an accredited intermediary service who will, on behalf of the customer proposition, seek consent from the customer to share and facilitate the sharing of data or action rights with the unaccredited customer proposition.



- Customers agree to two set of terms and conditions, one for the customer proposition and another with the intermediary service.
- Customers agree to share with an intermediary to enable access to a customer proposition.
- The customer propositions are not accredited under the Bill.
- The customer propositions may not be visible to the data holder.
- There is on-sharing of data or action/payment rights to non-accredited customer propositions.
- Accredited intermediaries create individual consents for each non-accredited customer proposition.

### Examples

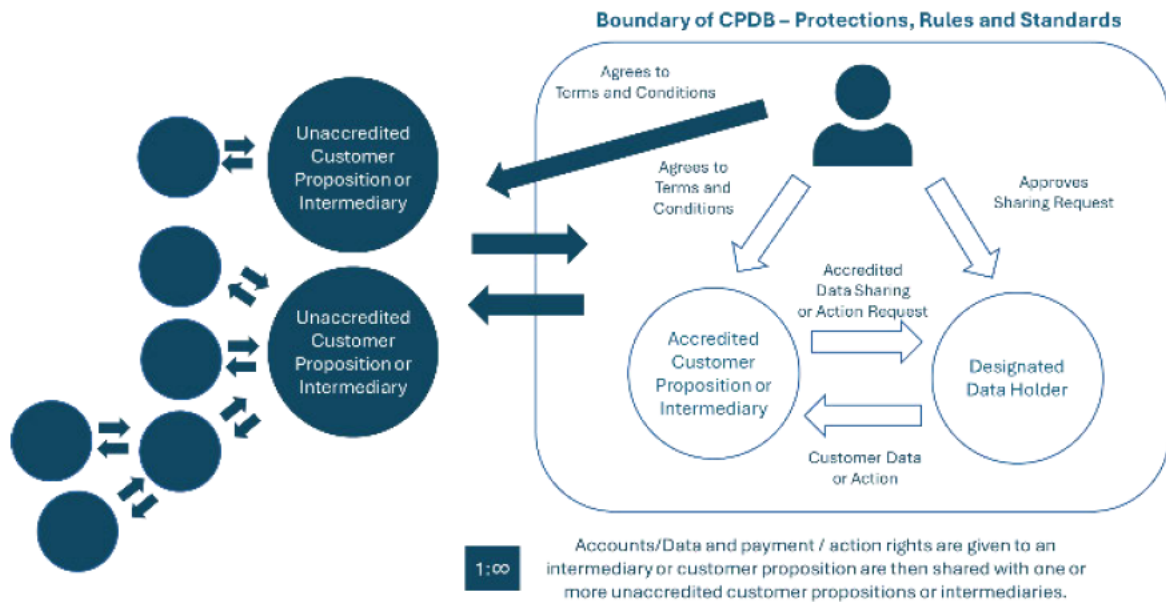
- Scenario 2a - Sharing with an unaccredited customer proposition from an accredited customer proposition, page 19.
- Scenario 2b - Sharing with an unaccredited customer proposition from an accredited intermediary, page 22.

Model Rating – Changes are required to support this model safely. See Recommended model and key recommendations, page 14.

Disclosure, scope, purpose and intended use of the data that is not necessary to provide the service.	Clarity of liability, customer protections and redress.	Visibility, consistency of consent management and respecting authority of all customers	Data holder fraud assessment and operational support.	Ease of participation for third parties.
Likely to be customer confusion on who they are sharing with, the scope and for what purpose. Intermediary terms and conditions may include purposes, scope and uses of data that go beyond the purpose and data required by the customer proposition. Customers may be required to sign-up to the intermediary service to use the customer proposition.	Sharing is occurring to unaccredited customer propositions. Protections and pathway for redress is unclear as on-sharing of business data and action rights outside of the Bill are not covered by the Privacy Act.	On-sharing may occurred without the authority or visibility of the other account holders. Approver is able to view and manage the consent in the customer proposition, intermediary and data holder. Account holders may not have visibility of the customer proposition, only the intermediary. Multiple consents will be impractical to manage as it will increasingly become harder to distinguish consents. If multiple intermediaries are used, then vis bility of consent will be distr buted and even harder for customers to manage.	Data holders have no visibility of customer proposition/and recipient of data or payment to inform fraud assessment and provide customers with support.	Customer propositions do not need to be accredited to access customer data or actions.

## Model 3 - Sharing with unaccredited recipients after initial consent

In this model accredited customer propositions or intermediaries who have received data or action rights under Model 1 or 2 on-share these to other unaccredited customer propositions after the initial consent.



- Customers must agree very broad consents to allow any intermediaries access their data or give them action rights to enable multiple different types of customer propositions.
- The customer propositions are not accredited under the Bill.
- The customer propositions will not be visible to the data holder and other account holders.
- There is on-sharing of data or action/payment rights to non-accredited customer propositions.
- Accredited intermediaries create one consent that is reused across many different non-accredited customer propositions.
- This is likely to be the most common model of sharing if not restricted.

### Examples

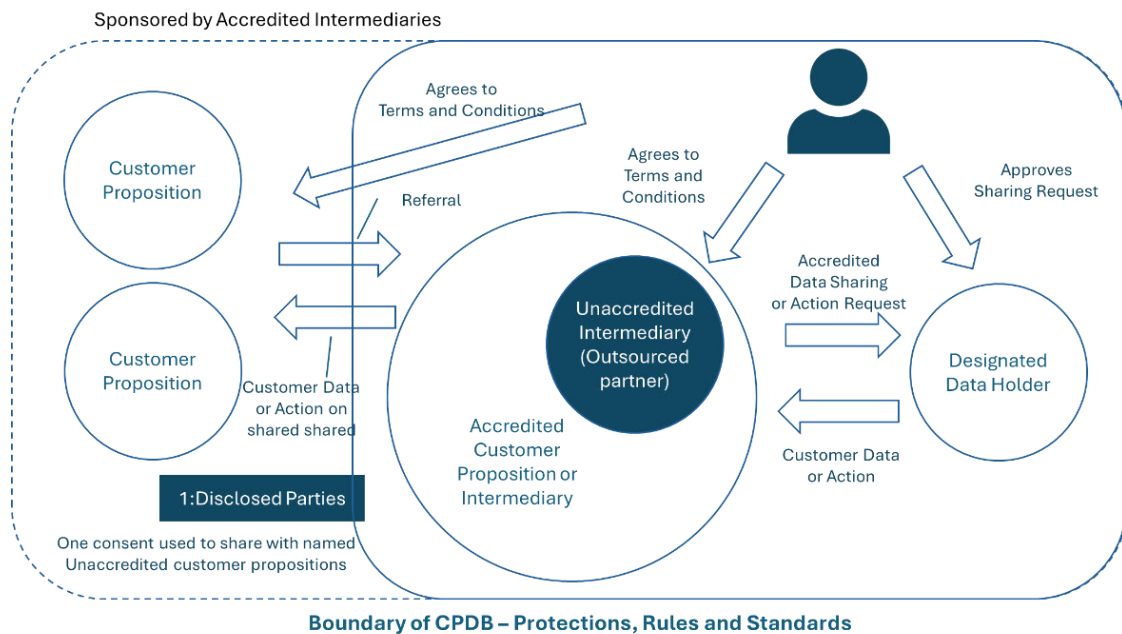
- Scenario 3a - Sharing with an unaccredited customer proposition from an accredited customer proposition, page 25.
- Scenario 3b - Sharing with an unaccredited customer proposition from an accredited intermediary, page 27.

Model Rating - This model should be prohibited.

Disclosure, scope, purpose and intended use of the data that is not necessary to provide the service.	Clarity of liability, customer protections and redress.	Visibility and consistency of consent management and respecting the authority of all customers	Data holder fraud assessment and operational support.	Ease of participation for third parties.
Likely to be customer confusion on who they are sharing with, the scope and for what purpose. Intermediary terms and conditions are very broad to enable on-sharing and include purposes, scope and uses of data that go beyond the purpose and data required by customer propositions.	Sharing is occurring to unaccredited customer propositions. Protections and pathways for redress is unclear as on-sharing of business data and action rights outside of Bill are not covered by the Privacy Act.	Approver is able to view and manage individual consents in the customer proposition and the intermediary only. Other account holders do not have visibility of the customer proposition, only the intermediary.	Data holders have no visibility of initial and further on-sharing to customer propositions/end recipients of data or payment to inform fraud assessment and provide customers with support.	Customer propositions do not need to be accredited to access customer data or actions.

## Recommended model and key recommendations

Our recommended approach is similar to Australia's CDR regime where unrestricted accredited parties can now sponsor unaccredited parties but must on pass CDR obligations through commercial agreements<sup>i</sup>.



Our view is that a sponsorship approach along with the key recommendations below provides the opportunity to develop the right balance between customer disclosure, consent and protections necessary to create and sustain customer trust<sup>ii</sup> while effectively managing risks and minimising cost to participate.

### Key recommendations

Disclosure, scope, purpose and Intended use of the data that is not necessary to provide the service.

1. The scope and purpose and the minimum data/rights needed to provide the service of the consent must pertain to the customer proposition and where the customer originated and where the relationship is held.
2. Individual consents must be created for each customer proposition and purpose.
3. Intermediaries should be limited to providing their service within the scope, purpose, terms and conditions agreed by the customer in the customer proposition and should not be permitted to unreasonably extend the purpose and scope from what is required to provide a service to the customer proposition, like the outsourced model.
4. Intermediaries should not be able to on-share or reuse data obtained for one customer proposition and re-purpose for another.
5. There needs to be clearer requirements on:
  - a. What happens if a customer revokes consent, especially when an intermediary is involved?
  - b. How changes to terms and conditions are managed and communicated to customers?

Clarity of liability, customer protections and redress.

6. Relevant protections, rules and obligations of the Bill should be 'always on and consistent'. Third parties should not be able to bypass obligations by participating and accessing through an intermediary.
7. On-sharing should be restricted to accredited intermediary services. This could be a business specialising in intermediary services or a customer proposition that on-shares data.
8. Unaccredited customer propositions must be sponsored by an accredited intermediary.
9. Accredited intermediaries should be liable to customers if an unaccredited customer proposition they sponsor cause harm or loss.

10. Relevant protections, rules and obligations of the Bill must be on passed through commercial agreements between the accredited intermediary and unaccredited customer propositions.
11. If on-sharing is permitted to unaccredited and unsponsored customer propositions:
  - a. to avoid customer confusion, it must be made clear to customers when they are sharing outside of the protections of the Bill,
  - b. the use of the intermediary's accreditation status needs to be carefully considered, and
  - c. It must be the responsibility of customer proposition to ensure appropriate agreements are in place to ensure that data is only used for the agreed purpose and treatment of data if a consent is revoked.

**Visibility and consistency of consent management and respecting the authority of all customers**

12. To provide easy identification, a centralised view of all sharing and the ability to revoke consent dashboards must be provided consistently within the customer proposition and at the data holder so that all Account owner(s) have visibility and can also revoke sharing on accounts they have authority over e.g. Joint.
13. When customers are looking to view or manage consents from within a customer proposition, they should not be required to sign-in to an intermediary service to manage consent for that customer proposition, if they are already signed into the customer proposition. If the customer have to remember user names and passwords for intermediary services they do not use often this may make it more difficult for them to withdraw their consent E.g. this should be provided securely within the customer proposition experience.
14. Only customers with the right level of authority must be able to agree to sharing. See Scenario 3b - Sharing with an unaccredited customer proposition from an accredited intermediary, page 27 to see how sharing could occur without the express and informed consent of an account owner.

**Data holder fraud assessment and operational support.**

15. The end recipient of the sharing must be disclosed to the data holder to provide:
  - a. the necessary visibility to perform fraud assessments,
  - b. operational support for the customer and other account holders, and
  - c. visibility of the consent to the customer and other account holders.

**Ease of participation for third parties.**

Refer to items 7, 8 and 9 above.

**Model Rating**

Disclosure, scope, purpose and Intended use of the data that is not necessary to provide the service.	Clarity of liability, customer protections and redress.	Visibility and consistency of consent management and respecting the authority of all customers	Data holder fraud assessment and operational support.	Ease of participation for third parties.
Scope and purpose and the minimum data/rights needed to provide the service of the consent must pertain to the customer proposition and where the customer originated and where the relationship is held	All parties are accredited or sponsored to operate with the Bill's boundaries.	Consents are easy to manage, consistently between customer propositions and data holder.  All account owners have visibility and can revoke.	Vis bility of the customer proposition/end recipient is provided a to perform effective fraud assessments and provide operational support.	Unaccredited customer propositions can participate without compromising customer protections if sponsored by an accredited intermediary.

## Example Scenarios

### Customer propositions

- **Budgie** allows personal and business customers to get insights into their spending and optimise interest across their accounts by moving money between the customer's accounts. Budgie do not share customer data with any other party.
- **budgetMaster** provides personal customers insights into their spending and ability to set and track budgets.
- **easyRec** is a tool for business customers to manage payment reconciliation. They require access to business account information. **easyRec** has an app store/marketplace of third parties. **easyRec** remains accredited.
- **homeBroker** – provides a home loan brokering service for personal customers.
- **creditChecker** – provides a credit check service to support loan applications. They are accredited.
- **HighTech** is a retailer selling electrical goods online and through their physical stores.

### Intermediaries

- **PayGate** is an intermediary service that provides payment online and instore payments capability to merchants and businesses. They hold an accreditation and provide easy connectivity to all the designated data holders.
- **InterConnect** is an intermediary service that helps unaccredited customer proposition access data and action rights under the Bill. They hold an accreditation and provide easy connectivity to all the designated data holders.

### Customer propositions that act as intermediaries

- **easyRec** is a tool for business customers to manage payment reconciliation. They require access to business account information.
- **brokerCRM** – provides an online system for brokers and their clients. They are accredited.

### Data Holders

- **123 Bank** provides personal banking services to personal customers.
- **ABC Bank** provides personal banking services to personal customers.

### Customer profiles and relationships

Read left and up.

	<b>Bob</b>	<b>Jane</b>	<b>John</b>	<b>Neil</b>
<b>Bob</b>	<del>Wife of Bob</del>	Husband of Jane	Business partner of John	Employs Neil
<b>Jane</b>	Wife of Bob	<del>Business partner of Bob</del>	No relationship	No relationship
<b>John</b>	Business partner of Bob	No relationship	<del>Employee of John</del>	Employs Neil
<b>Neil</b>	Employee of Bob	No relationship	Employee of John	<del>Employee of John</del>

For the purposes of these examples all customers bank with **123 Bank**.

<b>123 Bank</b>			
<b>Jane</b> (wife of Bob)	<b>Bob</b> (husband of Jane; business partner of John)	<b>John</b> (business partner of Bob)	<b>Neil</b> (employee of Bob and John)
Jane's <b>personal</b> transaction account(s)	Bob's <b>personal</b> transaction account(s)	<del>Bob's personal transaction account(s)</del>	<del>Bob's personal transaction account(s)</del>
Jane's <b>personal</b> credit card account	<del>Jane's personal credit card account</del>	<del>Jane's personal credit card account</del>	<del>Jane's personal credit card account</del>
Jane and Bob's joint <b>personal</b> transaction account		<del>Jane and Bob's joint personal transaction account</del>	<del>Jane and Bob's joint personal transaction account</del>
<del>Jane and Bob's joint personal transaction account</del>	Bob and John's <b>business</b> transaction account		<del>Bob and John's business transaction account</del>



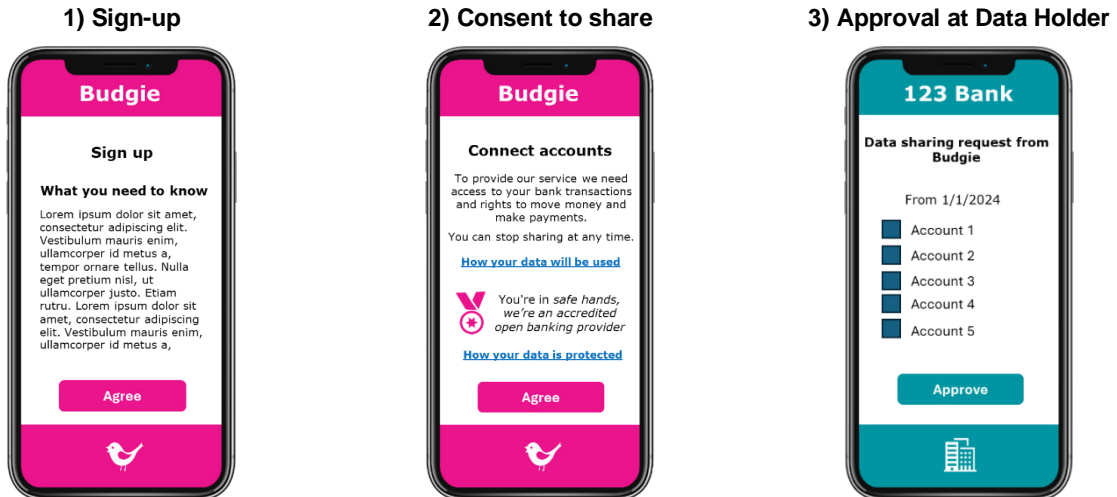
## Model 1 - Sharing directly with an accredited recipient

### Scenario 1a - Sharing directly with an accredited recipient

#### Example 1a.1 - Bob signs-up for Budgie

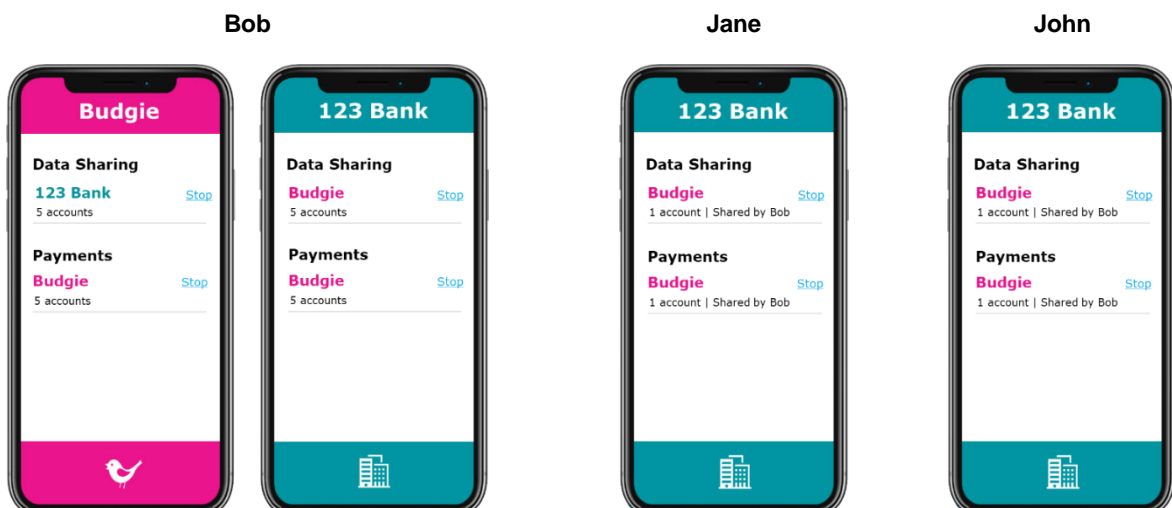
Bob is keen to understand where his money is going and signs up to **Budgie**.

Indicative customer sharing experience



- Bob signs up to Budgie and is asked to agree to their terms and conditions.
  - Bob opens their 123 Bank app.
  - Budgie asks Bob to connect their accounts.
  - Reviews request(s)
    1. selects accounts
    2. approves the consent
  - They inform the customer they are an accredited open banking provider under the Bill.
  - Bob agrees for his transactions and action/payment rights to be shared with Budgie.
- Sharing Requested**
- Transactional data for personal, joint and business accounts.
  - Rights to move money between accounts.
- Sharing Approved**
- Data:** A personal account; a joint account held with Bob's partner Jane. They both have individual authority on the account, and a business account held with his business partner John. They both have individual authority on the account
- Action:** A payment/move money right for each connected account.

Indicative customer consent management experience



## Scenario 1b - Sharing directly with an accredited recipient (Using an outsourced intermediary provider)

### Example 1b.1 - John signs-up for easyRec

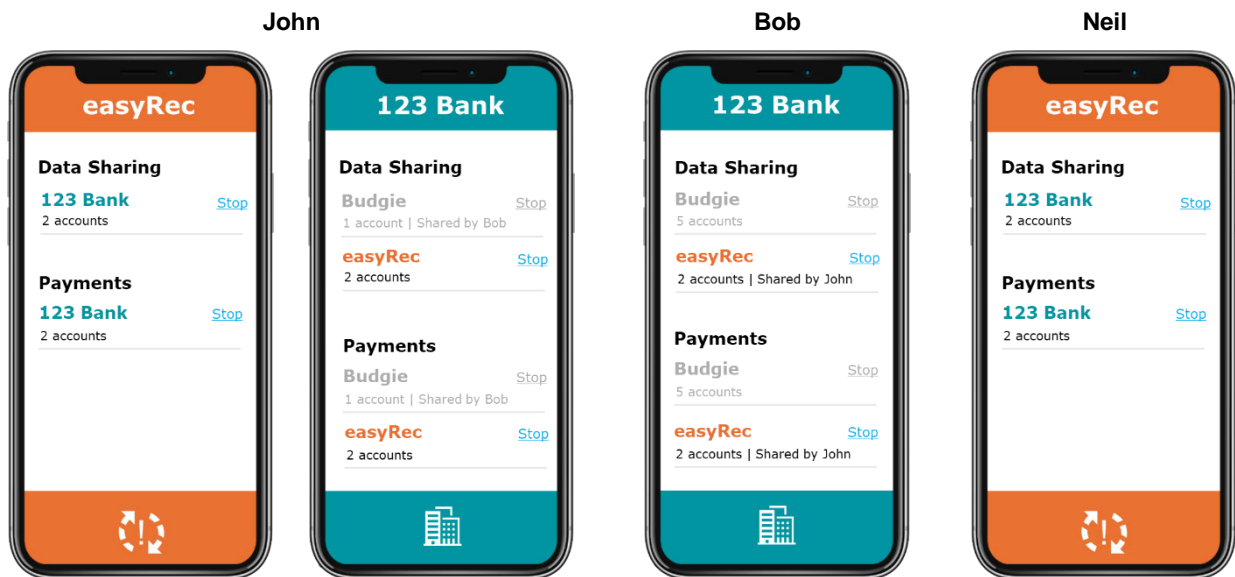
John wants to improve the efficiency of his business by saving time on payment reconciliation and cashflow. He finds a service called **easyRec**. John invites Bob and one other employee Neil (who does not have authority on the accounts) to use **easyRec**. All parties can now see data shared under the consent in **easyRec**.

#### Indicative customer sharing experience

As per above.

Sharing Requested	Sharing Approved	
	Data	Action
<ul style="list-style-type: none"> <li>Business transactional data</li> <li>Rights to move money between accounts and make payments from the accounts to automatically pay invoices.</li> </ul>	<ul style="list-style-type: none"> <li>Business transactional account and business credit card held with his business partner Bob. They both have individual authority on the account.</li> </ul>	<ul style="list-style-type: none"> <li>A payment right for business credit card and transactional account.</li> </ul>

#### Indicative customer consent management experience



Sharing models, scenarios and examples continue on next page.

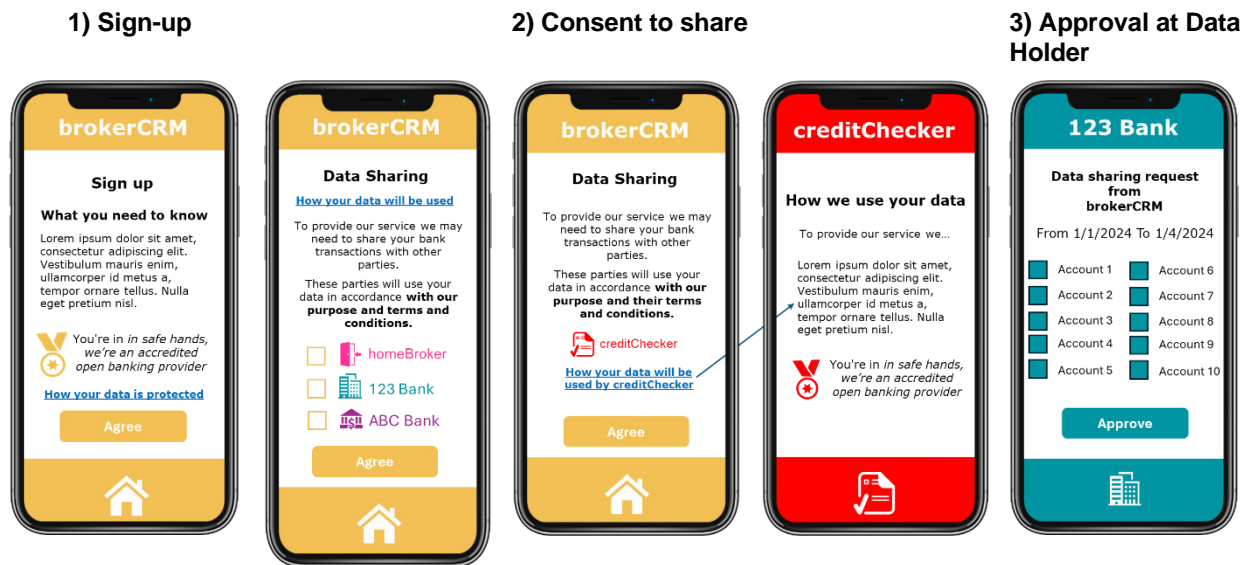
## Model 2 - Sharing with an unaccredited customer proposition (disclosed during consent)

### Scenario 2a - Sharing with an unaccredited customer proposition from an accredited customer proposition

#### Example 2a.1 - Jane signs up to brokerCRM

Jane is looking for help to buy her first home and finds **brokerCRM** a digital service that will help connect them with a physical broker (**homeBroker**) and makes it easy to get ready and apply for a home loan.

Indicative customer sharing experience



Jane signs up to **brokerCRM**.

They inform the customer they are an accredited open banking provider under the Bill.

- **brokerCRM** asks Jane to connect their accounts.
- They disclose that
  - Jane's data and derived data will be shared with and used by **creditChecker**, **homeBroker** and Jane's selected loan providers strictly for the purpose of helping to provide a loan.
  - Jane's data shared with loan providers and **homeBroker** is within the terms and conditions of **brokerCRM**.
  - Automated and ongoing data sharing is not in place with these parties and data is shared as required. This is a key difference between an unaccredited customer proposition connecting to intermediary who can pull data or execute actions on demand.
  - Jane's data shared with **creditChecker** uses their terms and conditions and Jane must agree to these.
- Jane agrees for her transactions to be shared with **brokerCRM**.

#### Sharing Requested

- 120 days of transactional data for her personal and joint accounts.

- Jane opens her 123 Bank app.
- Reviews request(s)
  3. selects accounts
  4. approves the consent

#### Sharing Approved Data

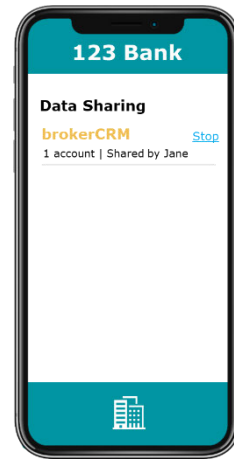
- a personal account and credit card,
- a joint account held with Jane's partner Bob. They both have individual authority on the account.

Indicative customer consent management experience

Jane



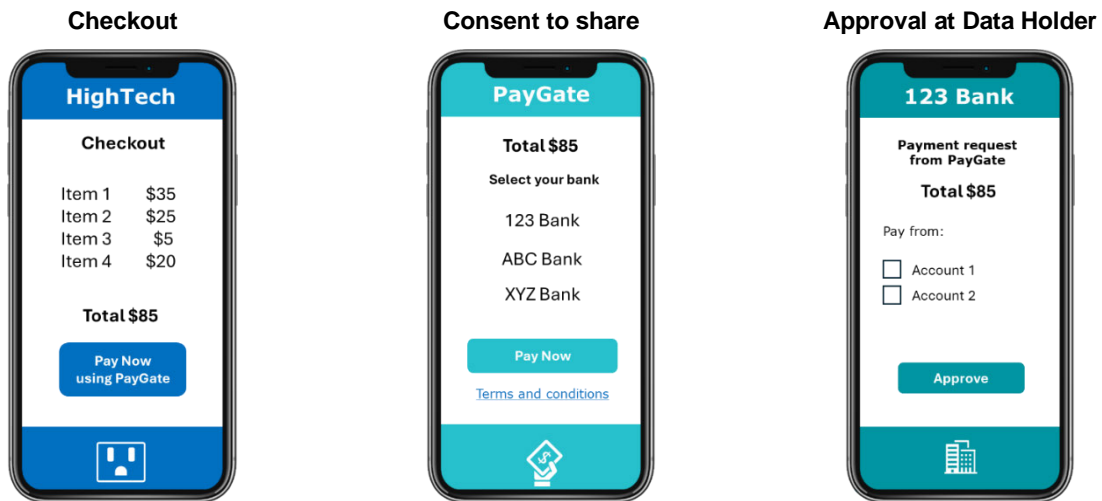
Bob



Sharing models, scenarios and examples continue on the next page.

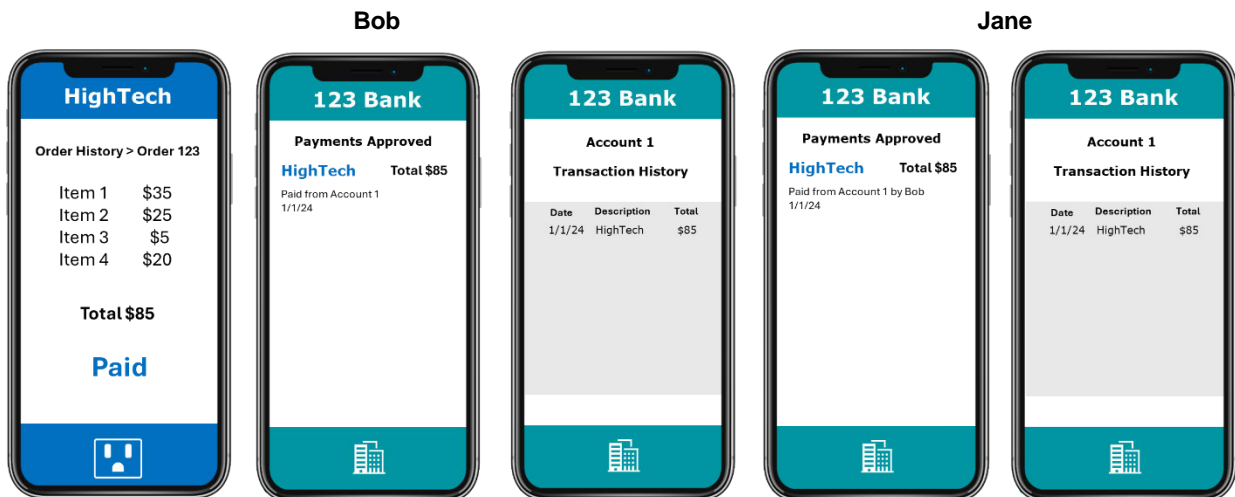
## Example 2a.2 - Bob makes a one-off payment to HighTech (unaccredited) using PayGate (Accredited)

Indicative customer sharing experience



- Bob adds items to their checkout and selects to Pay Now.
- Customer is referred to PayGate (Accredited) to complete the payment.
- They inform the customer they are an accredited open banking provider under the Bill.
- Customer selects to pay using open banking, selects their bank and then Pay Now.
- The customer is not required to create an account with PayGate.
- Customer opens their 123 Bank app.
- Reviews request
  1. selects account
  2. approves the payment

Indicative customer consent management experience



## Scenario 2b - Sharing with an unaccredited customer proposition from an accredited intermediary

### Example 2b.1 - Bob signs-up for Budgie via an accredited intermediary service Interconnect

Bob is keen to understand where his money is going and signs up to **Budgie**.  
 Indicative customer sharing experience

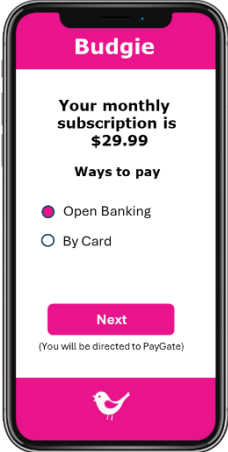
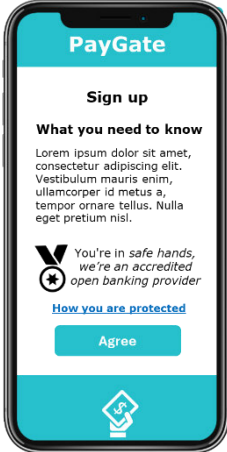
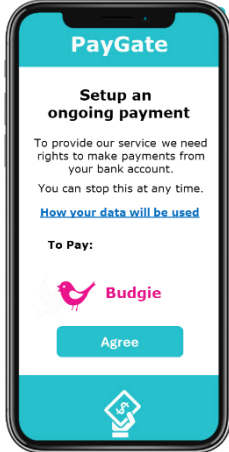
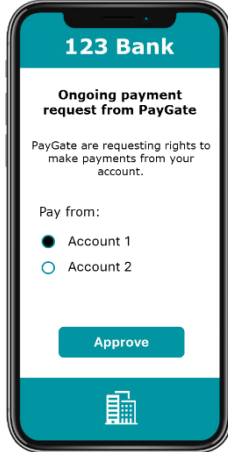
Sign-up	Sign-up	Consent to share	Approval at Data Holder
<ul style="list-style-type: none"> <li>• Bob signs up to Budgie (unaccredited) and is asked to agree to their terms and conditions.</li> <li>• Bob is referred to Interconnect (Accredited)</li> </ul>	<ul style="list-style-type: none"> <li>• InterConnect inform Bob that they are an accredited open banking provider under the Bill and that in order to use Budgie they must sign-up and agree to their terms and conditions.</li> <li>• Bob agrees to InterConnect's terms and conditions and creates a new customer account.</li> </ul>	<ul style="list-style-type: none"> <li>• Interconnect then asks Bob for the purposes of enabling Budgie's service to connect the accounts they would like to use with Budgie.</li> <li>• Bob agrees for their transactions and action/payment rights to be shared with Interconnect and on shared to Budgie.</li> </ul> <p><b>Sharing Requested</b></p> <ul style="list-style-type: none"> <li>• Transactional data for personal, joint and business accounts.</li> <li>• Rights to move money between accounts.</li> </ul>	<ul style="list-style-type: none"> <li>• Bob opens their 123 Bank app.</li> <li>• Reviews request(s), Selects Accounts and Approves the consent</li> </ul> <p><b>Sharing Approved</b></p> <p><b>Data:</b> a personal account; a joint account held with his wife Jane. They both have individual authority on the account; and a business account held with his business partner John. They both have individual authority on the account</p> <p><b>Payments:</b> A payment / move money right for each connected account.</p>

### Indicative customer consent management experience

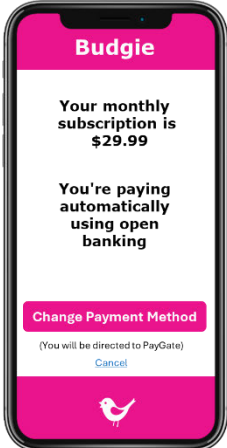

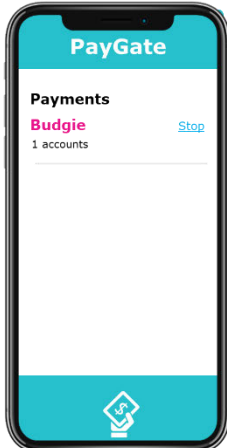
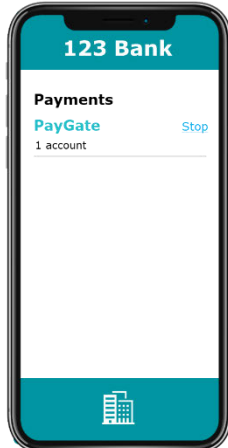
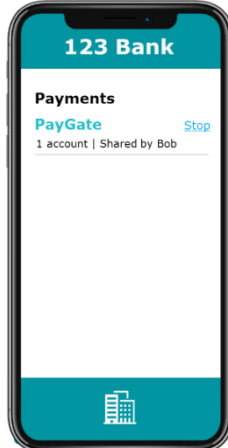
Bob	Jane	John

## Example 2b.2 Bob schedules payment of his monthly Budgie subscription (unaccredited) using PayGate (Accredited)

Indicative customer sharing experience

Referral	Sign-up	Consent to payment rights	Approval of payment rights
			
<ul style="list-style-type: none"> <li>Bob chooses to pay their ongoing subscription using open banking.</li> <li>Bob is referred to PayGate (Accredited) to setup the payment.</li> </ul>	<ul style="list-style-type: none"> <li>Bob is required to sign-up for PayGate and agrees to the Terms and Conditions.</li> <li>They inform the customer they are an accredited open banking provider under the Bill.</li> </ul>	<ul style="list-style-type: none"> <li>PayGate request rights to make payments from the customer's account.</li> </ul>	<ul style="list-style-type: none"> <li>Bob opens their 123 Bank app.</li> <li>Reviews request                             <ol style="list-style-type: none"> <li>Selects an account</li> <li>Approves the ongoing payment request.</li> </ol> </li> </ul>

Indicative customer consent management experience

Bob			Jane	
				

Risk considerations

- ! It is not clear which party determines the scope and purpose of the consent? Is this Budgie/BudgetMaster where the customer relationship is help and the consent originated, or the intermediary service (which holds no relationship to the customer) or both?
- ! If InterConnect / PayGate are separate services and not outsourced providers to Budgie/BudgetMaster the customer must agree to two different terms and conditions, one with Budgie/BudgetMaster where they originated and another set with the InterConnect.

- ! InterConnects and PayGate's terms and conditions may include purposes, scope and uses of data that go beyond the purpose and data required by Budgie/BudgetMaster.
- ! It is not clear if express and informed consent requirements proposed apply to the sharing from 123 Bank (data holder) to InterConnect / PayGate as the accredited recipients only or for any subsequent on-sharing outside of the Bill (e.g. to Budgie/ BudgetMaster) under the privacy act for personal data or no specified requirements for Business data or Actions.
- ! Likely to be customer confusion on whether they are sharing with an accredited party or an unaccredited party. When the customer is referred to InterConnect / PayGate as accredited parties - it would be reasonable for customers to expect that all parties are therefore accredited to the same level and that the same protections apply to Budgie/ BudgetMaster which they do not.
- ! The pathway for redress if something goes wrong is unclear.
- ! InterConnect / PayGate are not providing the name of the end recipient of data or payment to 123 Bank and therefore there isn't clear visibility for fraud assessments or operational support.
- ! In their 123 Bank apps, Jane or Bob are not able to identify the customer proposition for the consent. This will become impractical to manage as it will increasingly become harder to distinguish consents, if Jane or Bob also use other customer propositions that use InterConnect or PayGate as an intermediary.
- ! Jane is required to use InterConnect to manage sharing with BudgetMaster. Bob has no access.
- ! Bob is required to use InterConnect and PayGate to manage sharing with Budgie. Jane has no access.
- ! Bob should not be required to create an account or be required to sign-in to modify payments. Secure access should be provided from the Budgie.
- ! It is not clear what happens if Bob revokes consent:
  - 1) From Budgie – Will this revoke consent at Interconnect/PayGate and 123 Bank,
  - 2) From InterConnect/PayGate - Will this revoke access at Budgie and 123 Bank? and,
  - 3) From 123 Bank, will this revoke access at Interconnect/PayGate and Budgie?

**Sharing models, scenarios and examples continue on the next page.**



## Model 3 - Sharing with unaccredited recipients after initial consent

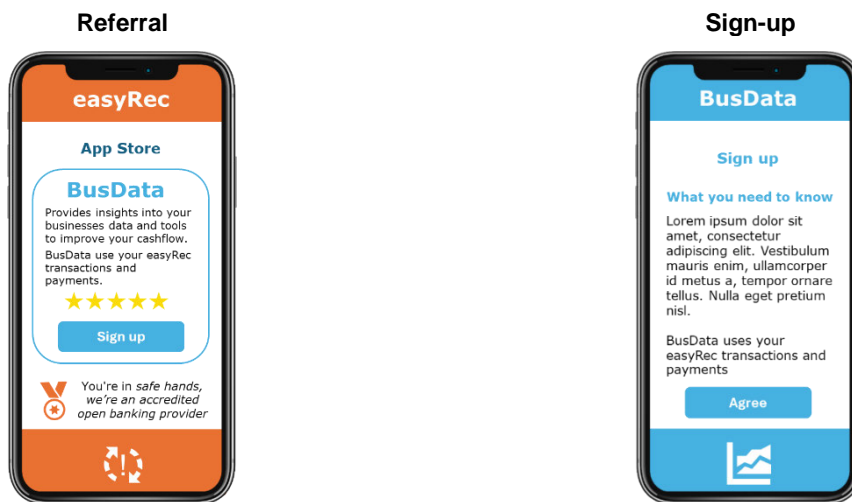
### Scenario 3a - Sharing with an unaccredited customer proposition from an accredited customer proposition

#### Example 3a.1 - Neil signs-up for BusDat

BusDat provides insights into business data and advice to improve cashflow. They are unaccredited.

Neil is searching for a tool to help him undertake his job. He finds **BusDat** in the **easyRec** ecosystem website which seems to meet his needs. He downloads the app and is asked to approve data and payment rights to be shared with **BusDat**. He agrees to the terms and conditions and starts to use the app.

#### Indicative Customer Sharing Experience



- Customer finds **BusData** in the **easyRec** app store.
- They tap/click to sign-up for **BusData**.
- **easyRec** refer the customer to **BusData**
- Customer signs up to **BusData** and is asked to agree to their terms and conditions.

#### Sharing Requested

- Business transaction data
- Payment rights to pay invoices.

#### Sharing Approved

- Business transactional account and business credit card held at **easyRec**.
- A payment right for the business transactional account.

He tries out the payment capability to move money between the business accounts and make a payment from one of the business accounts to pay an invoice.

#### Indicative customer consent management experience



Unfortunately, BusDat are the target of a cyber attack who compromises the service due to weak protections.

The attack was two fold:

1. Data: The attackers retrieved the most recent transactions and published sensitive information on social media to competitors this included payroll, purchases, payments received from key clients. While there was no financial loss, key clients lost trust in them and they lost their business.
2. Payments: The attackers changed the recipient bank account and initiate false payments. easyRec processed these payment and they are approved by 123 Bank. John and Bob lost \$43,000 from two fraudulent payments.

John and Bob were not aware that Neil was using this service. John and Bob tried to seek redress from BusData who shortly after the compromise ceased trading. easyRec denied responsibility as they were acting on instructions from BusData and that this was clearly outlined in their terms and conditions. John argued that he did not agree to terms and conditions. easyRec again pointed to their terms and conditions that clearly stated that admin users, which Neil was, can on share data and payment rights.

easyRec were able to determine who they on shared to and undertook no responsibility to assess their worthiness initially or ongoing. They are not accountable for BusData's failings or poor processes

#### Risk considerations

- ! Neil agrees to terms and sharing of data and payment rights when he holds no authority on the business accounts.
- ! Payments are showing in 123 Bank as payments to easyRec, misleading the customer that they are legitimate payments to an accredited party.
- ! Bob has no visibility of the sharing as he does not use easyRec and is not able to view or stop the sharing. John may have visibility of the sharing in the easyRec App.
- ! BusData's operational and fraud controls were weak and below the standards required to be accredited.
- ! easyRec key terms and conditions on sharing are buried in their terms and conditions which John did not read or understand.
- ! 123 Bank reviewed what they believed to be legitimate payments from easyRec and these were in line with previous payments.

**Sharing models, scenarios and examples continue on the next page.**

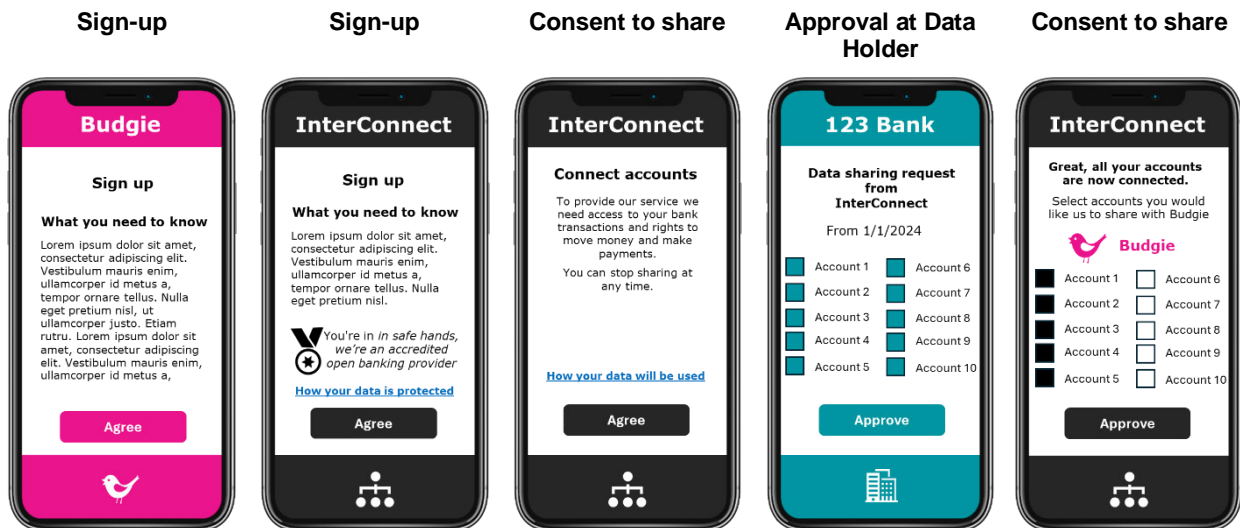
## Scenario 3b - Sharing with an unaccredited customer proposition from an accredited intermediary

Same as scenario 3a, however intermediary establishes broad customer consent(s) and then aggregates data and action rights and on shares to multiple unaccredited customer propositions.

### Example 3b.1 - Bob signs-up for Budgie

Bob is keen to understand where his money is going and signs up to **Budgie**.

Indicative customer sharing experience



- Bob signs up to Budgie (unaccredited) and is asked to agree to their terms and conditions.

- Bob is referred to Interconnect (Accredited).

#### Sharing Requested

- Transactional data for personal, joint and business accounts
- to move money between accounts.

- InterConnect inform Bob that they are an accredited open banking provider under the Bill and that in order to use Budgie they must sign-up and agree to their terms and conditions.

- Bob agrees
- to InterConnect's terms and conditions and creates a new customer account.

- InterConnect then asks Bob to connect all of his accounts and give them payment rights for the purposes of InterConnect aggregating his accounts for use with Budgie and other customer propositions in future.

- Bob agrees for their transactions and action/payment rights to be shared with Interconnect.

#### Sharing Requested

- **ALL** Transactional data for personal, joint and business accounts
- to move money between accounts.

- Bob opens their 123 Bank app.
- Reviews request(s)
  1. Selects Accounts
  2. Approves the consent

#### Sharing Approved Data:

- 10 accounts in total,
- 7 personal accounts,
- 1 personal credit card,
- a joint account held with Bob's partner Jane. They both have individual authority on the account, and
- a business account held with his business partner John. They both have individual authority on the account.

#### Payments:

- A payment/move money right for each connected account.

- InterConnect confirm all Bob's accounts are now connected and asks which accounts to share with Budgie.

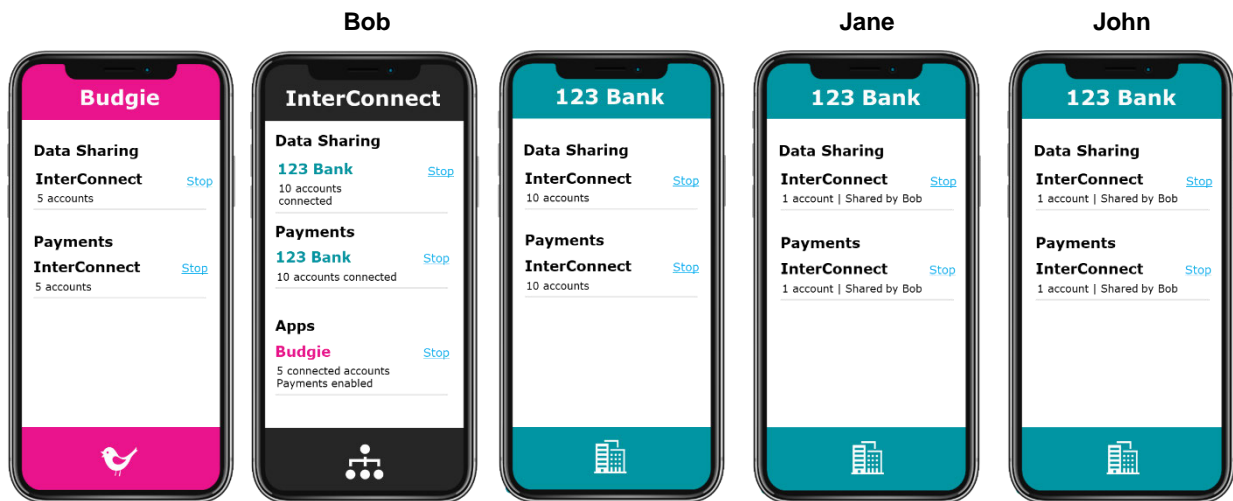
#### Sharing Approved Data:

- 1 personal account,
- a joint account held with Bob's partner Jane. They both have individual authority on the account, and
- a business account held with his business partner John. They both have individual authority on the account.

#### Payments:

- A payment/move money right for each connected account.

Indicative customer consent management experience



Sharing models, scenarios and examples continue on the next page.

## Example 3b.2 - Bob signs-up for BudgetMaster

Bob is also keen to try out BudgetMaster.

Indicative customer sharing experience



- Bob signs up to BudgetMaster (unaccredited) and is asked to agree to their terms and conditions.
- Bob is referred to Interconnect (Accredited).
- As Bob is an existing customer he signs in.
- Bob Reviews request(s)
  1. Selects Accounts
  2. Approves the consent

### Sharing Requested

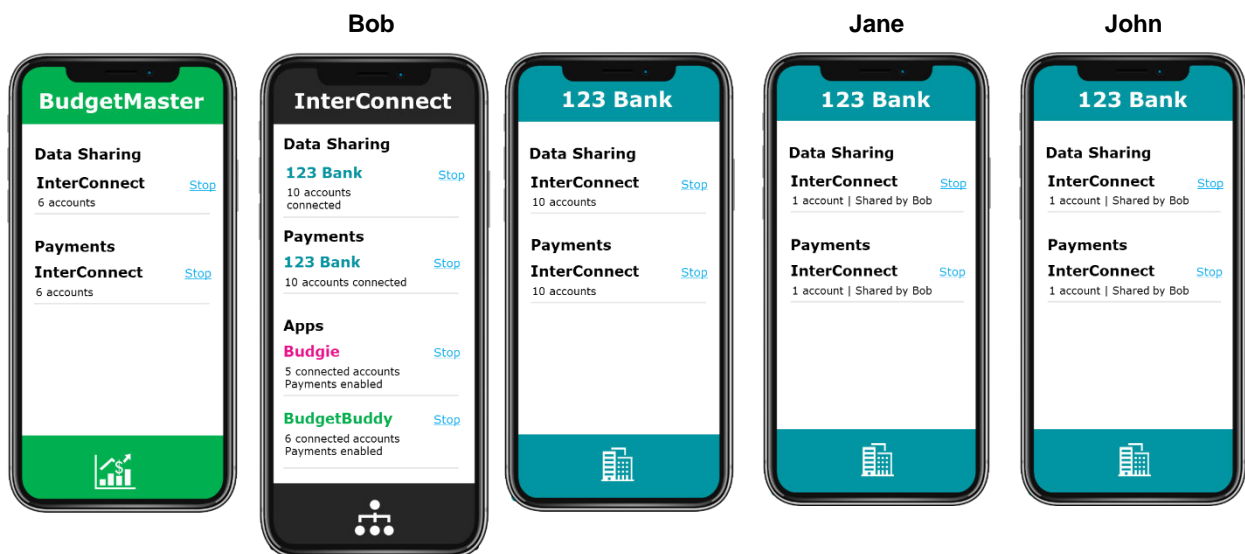
- Transactional data for personal, joint and business accounts.
- Rights to move money between accounts.

### Sharing Approved

**Data:** 1 personal account; a joint account held with Bob's partner Jane. They both have individual authority on the account; and a business account held with his business partner John. They both have individual authority on the account.

**Payments:** A payment/move money right for each connected account.

Indicative customer consent management experience



## Risk considerations

- ! This model has all the same risk concerns as Model 2 - Sharing with an unaccredited customer proposition (disclosed during consent)
- ! To enable on-sharing to other unaccredited customer propositions InterConnect's terms and conditions are very broad and include purposes, scope and uses of data that go far beyond the purpose and data required by Budgie and BudgetMaster.
- ! Sharing may occur with InterConnect ahead of being required to enable customer propositions which is the case for accounts 7,8,9,10.
- ! As data and rights are reused, there is no visibility of the individual customer propositions for 123 Bank to assess fraud or for the approver and the other account holders in 123 Bank app.

## ATTACHMENT B

### 1. RESPONSES TO QUESTIONS

Status quo and problem definition	
1.	<p>How do you expect the implementation and use of open banking to evolve in the absence of designation under the Bill? What degree of uptake do you expect?</p> <p>N/A</p>
2.	<p>Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?</p> <p>Please see paragraphs 2.1 - 2.4 of our submission. While ANZ supports open banking as a whole, ANZ disagrees with paragraph 20 of the Discussion Paper, as industry has made considerable effort to initiate open banking.</p>
3.	<p>What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?</p> <p>Please see paragraphs 3.1 - 3.2 of our submission. ANZ submits that open banking should support use cases that end-customers want, and will use, and that are practical and supported by a cost/benefit analysis. In addition, in paragraph 40 of the Discussion Paper, MBIE refers to a focus on applications with the "highest economic or social value" to map implementation plans. ANZ proposes that a more feasible approach could be to focus on mobile first as a digital growth area, rather than considering all platforms.</p>
4.	<p>Do you have any comments on the criteria that should be used to assess designation options?</p> <p>Please see paragraphs 3.1 - 3.2 of our submission. ANZ submits that the criteria in paragraph 35 of the Discussion Paper should be amended to refer to "wide <u>customer</u> uptake" and "valuable <u>customer</u> use cases", as well as a practicality criterion. We also submit that the reference to "efficient investment" should expressly include a cost/benefit criterion for each use case and consider efficiencies from both the perspectives of banks and third parties.</p>
The Scope of an open banking designation	
5.	<p>Do you agree that the banks covered and timeframes should be based on the API Centre Minimum Open Banking Implementation Plan? Do you have any concerns about the specific implementation dates suggested?</p> <p>Please see paragraphs 4.1 - 4.3 of our submission. ANZ submits that the scope of designation include a principle of reciprocity, to encourage early participation. ANZ further submits that the 1 December 2025 date is not realistic and risks compromising quality.</p>
6.	<p>Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?</p> <p>See paragraphs 4.1 – 4.3 of our submission</p> <p>In relation to the designation of other deposit takers, the Verian Personal Banking Survey Report, commissioned by the Commerce Commission and referenced at footnotes 13 - 15 of the Discussion Paper, notes that Māori, Pasifika and lower income households are more likely to use other providers, or medium-sized banks (like Kiwibank). On this basis, if designation only includes the five largest banks, there is a risk that these sectors of the community will be disadvantaged because they will not</p>

	<p>initially have access to open banking services unless they either switch to or open new accounts with the five largest banks.</p> <p>ANZ also notes the comment at paragraph 49(b) of the Discussion Paper, that 44% of people have a personal loan with a financial institution other than the five largest banks. This further shows that there might be a competitive and financial wellbeing benefit if more deposit takers are included, and this may help the more vulnerable communities in New Zealand.</p>
7.	<p>Do you agree that, in the first instance, only requests by accredited requestors be designated? Do you have any comments on when and how direct requests by banking customers could be designated under the Bill?</p>
	<p>We agree with this position. Please see paragraph 4.4 of our submission.</p>
8.	<p>Do you have any comments on the customer data to be designated?</p>
	<p>Please see paragraph 4.5 of our submission. ANZ submits that the focus should be on information that customers already have access to through retail and small business digital channels.</p> <p>ANZ also supports a flexible regime that ensures growth of innovation and keeps compliance costs to a minimum.</p> <p>ANZ further submits that customer identifiers should be excluded from scope and if required, replaced with a hashed customer equivalent. Please see paragraph 4.5(a) of our submission.</p>
9.	<p>Do you have any comments on whether product data should be designated? What product data should be included? When should the product data designation come into force?</p>
	<p>Please see paragraph 4.5(e) of our submission. In summary, ANZ submits that attempting to designate product data is unwise at this point, given the complexities of implementing customer data in the intended timeframe.</p> <p>In addition, ANZ notes that each additional element that is designated adds another level of complexity, less control and higher costs. Each additional use case introduces different operational and risk considerations that must be worked through across the value chain, including non-financial risk, AML/CFT, privacy, legal, products, customer protection and information security.</p> <p>At present, the designation of data in Australia has been costly and resource intensive, given the wide scope of data. Designation needs to be reasonable to avoid these high costs, while still allowing flexibility, growth and innovation. However, constraining the data to be designated could impact industry and customers later.</p> <p>If product data is to be designated, then ANZ submits that the timeframe in paragraph 68 of the Discussion Paper (6 months from the proposed dates for customer data and actions) will not be sufficient. There is no clear framework yet as to the scope of product data, and the consequences of getting the regulations on product data wrong could be costly. For example, there is a risk that the product data may be reorganised in such a way by a third party that it no longer accurately describes the product it relates to, or otherwise fails to declare the key components of the product.</p>
10.	<p>Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?</p>



	Please see paragraphs 1.6 – 1.7 of our submission, regarding the uncertainty caused by the additional proposed designation by the Commerce Commission.
<b>The benefits, costs and risks of an open banking designation</b>	
11.	Do you agree with our assessment of how the designation will affect the interests of customers (other than in relation to security, privacy and confidentiality of customer data)? Is anything missing? For businesses: What specific applications and benefits are you aware of that are likely to be enabled by the designation? What is the likely scale of these benefits, and over what timeframe will they occur?
	Please see paragraph 5.1 of our submission.
12.	Do you agree with our assessment of the costs and benefits to banks from designation under the Bill (other than those relating to security, privacy or confidentiality)? Is anything missing? For banks: Would you be able to quantify the potential additional costs to your organisation associated with designation under the Bill? i.e. that would not be borne under the Minimum Open Banking Implementation Plan.
	<p>Please see section 5 of our submission. Every requirement in the Regulations and Standards carries a direct cost for the banks, and ANZ has invested ██████████ to date.</p> <p>In addition, ANZ agrees with MBIE's comment at paragraph 78 of the Discussion Paper that there will be a significant additional cost for banks, particularly in relation to 78(b).</p> <p>MBIE's comments at paragraph 77 of the Discussion Paper (relating to the additional IT implementation costs) downplay the continued costs to develop open banking systems. These continuing costs are likely to be high, given the additional work every data point or offering imposes on banks, multiplied by each channel they are required to be compatible with, and the additional upkeep required.</p> <p>ANZ also notes that in Australia, banks were called out for data quality issues (see the ACCC report <a href="#">here</a>). To avoid this happening in New Zealand, MBIE must continue to reevaluate the costs/benefits as the regime evolves. For example, if data is not currently available, then it may not be feasible or realistic to include in the regime until it is available.</p> <p>There will also be additional costs if banks also need to provide product data.</p>
13.	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
	N/A
14.	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?
	<p>Please see paragraph 5.1 of our submission. ANZ submits that the risks to security, privacy and confidentiality need to be managed carefully.</p> <p>To expand on this, ANZ does not agree that the reliance on the Privacy Act 2020 alone will help mitigate the risks of open banking. Whilst we acknowledge the intended approach of relying on existing protections for customer data under the Privacy Act is attractive in principle, in practice, it has clear gaps. For example, there are scenarios where it is not clear that the data is 'personal information', such as information about businesses and action initiation requests.</p>

	ANZ has also recognised there are gaps between the Information Privacy Principles (IPPs) and the Regulations and Standards. For example, the IPPs do not require agencies to collect express and informed consent from individuals prior to the collection, use or disclosure of their data, however, this is a key component of the open banking regime. Further, there are several exceptions for disclosing personal information under IPP 11 without individual consent, which are broad. Therefore, ANZ submits that assessing complaints against the IPPs is insufficient to adequately protect open banking data.
15.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	This will depend on whether derived data is included. Derived data could include bank intellectual property.
<b>Accreditation criteria – what specific criteria should business need to meet before they can become accredited to make requests on behalf of consumers?</b>	
16.	Do you have any insights into how many businesses would wish to seek accreditation, as opposed to using an accredited intermediary to request banking data? For businesses: How likely are you to seek accreditation? What would make you more or less likely to apply?
	N/A
17.	Do you agree that directors and senior managers of accredited requestors should be subject to a fit and proper person test? Do you have any comments on the advantages or disadvantages of this test, or other options?
	ANZ agrees with the fit and proper person test.  ANZ also submits that a sanctions check should be undertaken.
18.	Do you agree that requestors whose directors and senior managers have already met the 'fit and proper' licensing or certification test by the Reserve Bank, Financial Markets Authority or Commerce Commission should be deemed to meet this requirement without further assessment?
	ANZ agrees with this in principle, but we would need to see further detail to be able to provide appropriate comment.
19.	Do you consider that, in the absence of insurance or guarantee requirements, there is a significant risk of banks or customers not being fully compensated for any loss that might reasonably be expected to arise from an accredited requestor breaching its obligations?
	Please see paragraphs 6.2 – 6.3 of our submission. ANZ submits that insurance should not be a mitigation for poor risk controls, and should adequately cover the accredited requestor's potential liability.
20.	Do you have any comments on the availability and cost of professional indemnity insurance and/or cyber insurance, and how this may impact on the ability of prospective requestors to participate in this regime?
	In ANZ's experience with onboarding third parties to date, insurance appears to be widely available. We do not have adequate data to make a comment on costs.
21.	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
	While ANZ agrees that a principles-based approach could work, it will need to be properly tracked, supervised and reviewed on a regular basis.

22.

Do you agree that accredited requestors in open banking should be required to be a member of a financial services disputes resolution scheme?

Please see paragraph 6.4 of our submission. ANZ supports the intention behind MBIE's proposal to consider how complaints and disputes under the open banking regime may be resolved. However, ANZ's view is that MBIE's proposal to address open banking disputes via the New Zealand established dispute schemes (the schemes) requires further deliberation to ensure dispute resolution is fair, accessible, transparent, consistent and effective for consumers across all involved industries.

A clear and well governed framework that considers all parties is necessary for New Zealand's open banking regime. Data is a growing commodity in the digital economy, therefore, a robust and consistent complaints resolution process will be required to address future complaints in this area to promote consumer trust and the continual sharing of data.

We consider it is essential to establish a clear and efficient process for consumers when multiple entities under the open banking regime are involved in a single complaint. The process should minimise administrative burdens for both consumers and participants, while ensuring consistency in both the experience and the handling of the complaint.

While appropriate for managing complaints regarding financial services, our view is that MBIE's proposal to utilise the schemes to address customer complaints related to open banking issues does not sufficiently consider the impact it may have on consumers and the potential compliance costs for participants.

ANZ would like to draw MBIE's attention to the following for further consideration:

- the requirement for each participant to have an internal dispute resolution process;
- whether the schemes will have the expertise and resources to address open banking complaints where intermediaries and on sharing of personal data, business data and action/payment rights has occurred and resulted in customer harm or loss. See Attachment A - Model 2 - Sharing with an unaccredited customer proposition (disclosed during consent), page 19;
- if each scheme's terms of reference adequately allow for consideration of open banking complaints;
- how consistency of approach, timeliness of investigations and outcomes across each scheme will be achieved and monitored, if the proposed approach is undertaken;
- how schemes will consider complaints about multiple parties, that may be members of different schemes but affect a single consumer;
- a potential increase levies for participants would likely increase financial pressure, especially during a period of significant investment in launching open banking. This is in addition to updating systems, processes and upskilling staff; and
- how consumers will be educated about resolving disputes under the open banking regime.

It is ANZ's view that the questions above should be considered and addressed as early as possible to ensure the regime is fit for purpose and is appropriately structured to address future customer complaints.

If MBIE is seeking to amend the remit of the schemes, an alternative approach could include the introduction of a single disputes body. ANZ understands this approach has been adopted in Australia with the establishment of the Australian Financial Complaints Authority (AFCA). AFCA is an independent authority, which considers complaints that previously would have been handled by the Financial Ombudsman Service, the Credit and Investments Ombudsman and the Superannuation Complaints Tribunal.

Employing one disputes authority for open banking and financial services may assist in creating more consistent outcomes for customers and industry alike, particularly with the introduction of multiple cross- industry participants in open banking, for example telecommunications or fintech companies.

Like AFCA, one disputes authority in New Zealand for open banking would likely be appropriately resourced to investigate open banking cases because of its level of membership. Having this resource would mean the authority could employ the necessary experts to investigate open banking cases, ensuring appropriate outcomes for consumers and participants.

In addition to the above, a primary concern for ANZ is the growing number of scams in the financial sector. We believe the introduction of open banking will not only increase the volume of scams but also change the nature of the fraudulent activity due to third party involvement.

Other jurisdictions, such as Australia, have seen a rise in complex scams. Almost eleven thousand scam related complaints were made to AFCA in 2023- 24 alone. It is our view that the introduction of open banking will only add to the complexity of scams.<sup>3</sup>

Considering the trend and the change in scope of complaints that Australia is facing since the introduction of open banking, it is our view that New Zealand is likely to experience similar circumstances. Considering the above, MBIE should again examine whether the schemes in their current form will be able to appropriately manage this new scope of complaints, and likewise if the schemes in their current form are the appropriate channel to address these disputes.

23.

Do you consider that information security requirements should form part of accreditation?

Please see paragraph 6.5 of our submission. ANZ submits that information security requirements should form part of the accreditation, subject to our concerns set out at paragraph 6.5 and in response to question 24 below.

24.

Do you have any comments on the level of prescription or specific requirements that should apply to information security? For businesses: What information security standards and certifications are available to firms in New Zealand, and what is the approximate cost of obtaining them?

<sup>3</sup> <https://www.afca.org.au/news/media-releases/financial-complaints-rise-further-9-to-record-105000-in-2023-24#:~:text=Scam%2Drelated%20complaints%20rose%2081,month%20the%20previous%20financial%20year.>

	<p>Please see paragraph 6.5 of our submission . ANZ holds concern around the reliance on the requirements of the Privacy Act 2020 in relation to information security, and instead supports "option 3" of paragraph 114 of the Discussion Document (<i>a more prescriptive set of information security requirements along the lines of the Australia CDR Rules, potentially with expectations of third-party certifications against specific standards (e.g. ISO 27001)</i>).</p> <p>ANZ also supports an open banking regime that treats all customer data and action initiation requests the same (regardless of whether the information is "personal information") to promote more consistent outcomes across the board.</p>
25.	<p>Do you agree that additional criteria of accreditation be the applicant demonstrate compliance with its policies around customer data, product data and action initiation and with the Act?</p>
	<p>ANZ supports these additional criteria.</p>
26.	<p>Do you consider any additional accreditation criteria are necessary?</p>
	<p>Please see paragraphs 6.1, 6.6 and 6.7 of our submission, and ANZ's comments in relation to intermediaries in its submission on the Bill.</p> <p>Expanding on the key points made in those paragraphs, unaccredited third parties should not be able to bypass the regulations and standards by participating through an accredited recipient. ANZ submits that there should be a different class of accreditation for intermediaries, where accredited recipients who share data with unaccredited recipients should be required to:</p> <ol style="list-style-type: none"> <li>1. sponsor the unaccredited recipient;</li> <li>2. ensure that the unaccredited recipient they sponsor meets minimum requirements and operates within the regulations and standards; and</li> <li>3. be accountable for the actions of a third party they sponsor.</li> </ol> <p>There are also other additional risks with using the open banking regime. Currently, ANZ accepts instructions directly from the customer and acts accordingly. In doing so, we can implement our own fraud detection and financial crime detection methods to detect and prevent fraud. Through the open banking regime, as we are acting on the instructions of the accredited requestor, ANZ is reliant on the accredited requestor conducting these fraud detection processes. Without a proper fraud assessment being undertaken on the accredited requestor or full visibility of transactions, this exposes more risks into the system. ANZ submits that accredited requestors should be subjected to fraud testing and be required to implement fraud detection methods as part of the accreditation process, so that the system is not exposed to any additional risks.</p>
<p>Fees – what restrictions should there be on fees for providing customer data or initiating payments?</p>	
27.	<p>What would be the impact of requests under the Bill being free, for banking?</p>
	<p>Please see paragraphs 7.1 – 7.3 of our submission. For clarity, ANZ does not intend to charge customers for access to their data, or for payment initiation. ANZ would</p>

	want the ability to charge accredited requestors in line with points made in question 28.
28.	If requests under the Bill were not free, what limits or restrictions should be placed on charging fees? Do you have any comments on the costs and benefits of the various options?
	Please see section 7 of our submission. ANZ submits that pricing should be subject to pricing principles, including being fair and transparent, and in line with efficient long-run costs.
<b>The detailed rules for open banking</b>	
29.	Do you agree with the proposals to ensure that consents given to accredited requestors are sufficiently informed? Are there any other obligations that should apply to ensure that consents are express and informed?
	<p>Please see paragraphs 8.1 – 8.4 of our submission and Attachment A.</p> <p>To ensure customers provide informed and expressed consent and remain consistently protected we propose:</p> <ul style="list-style-type: none"> <li>• a new sharing model where unaccredited third parties are sponsored by accredited intermediaries, and</li> <li>• 15 key recommendations, see Attachment A, Pages 13 - 14.</li> </ul> <p>We consider that informed and express consent is essential to the new regime. Without changes, there is considerable risk of customers providing uninformed consent, or worse being misled. As proposed complex sharing and on-sharing models involving unaccredited third parties would be possible.</p> <p>In some cases, customers might reasonably believe they are sharing data with an accredited party under the protections of the Bill. However, during the same sharing experience, they could inadvertently share data with an unaccredited party that does not meet the same accreditation standards and operates outside the open banking regime, offering significantly reduced protections.</p> <p>See Attachment A.</p> <ul style="list-style-type: none"> <li>• Scenario 2a - Sharing with an unaccredited customer proposition from an accredited customer proposition, page 19.</li> <li>• Scenario 2b - Sharing with an unaccredited customer proposition from an accredited intermediary, page 22.</li> <li>• Scenario 3b - Sharing with an unaccredited customer proposition from an accredited intermediary, page 27.</li> </ul> <p>There are also risks that sharing could occur without the authority and/or visibility of other account holders, Scenario 3a - Sharing with an unaccredited customer proposition from an accredited customer proposition, Attachment A, page 25.</p> <p>In any of these scenarios it will be very difficult for customers to understand who they are giving consent to, for what purpose, who is protecting them and what protection are in place.</p>

Without a single clear dispute and resolution processes, it will be challenging for customers to know where to go if something goes wrong. It will also be difficult for them to obtain redress in a timely way due to the complexity that will be involved in determining who is at fault.

Customers should ideally only be required to agree to one set of terms and conditions for the service that they are using, to avoid confusion. This should come from the party that the customer 'sees' is providing the service to them.

In relation to paragraph 137(b) and 137(c) of the Discussion Paper, determining who is providing what service to the customer, and the minimum sharing (and use of data) required to provide the customer with the service, is subjective. This complexity makes it difficult to determine when accredited intermediaries are involved, and whether the customer wishes to share data with an unaccredited third party.

The definition of services should be clear about who is providing a service to whom. In our view, the third-party customer service or proposition is the one where the customer started their journey, and where the customer relationship is held. When a customer is referred to an intermediary service to help facilitate sharing, they are providing a service to the third-party customer service or proposition, not directly to the customer.

In this scenario, intermediaries should be limited to providing their service within the scope, purpose, terms and conditions agreed by the customer in the customer proposition. They should not be permitted to unreasonably extend the purpose and scope from what is required to provide a service to the customer proposition e.g., the outsourced model.

More specific definitions on what should be disclosed upfront as opposed to contained in terms and conditions, regardless of if it is necessary to provide their service or not. This could include:

- use of data in AI Models; and
- if customer data is on-shared or sold as either the raw data, in de-identified aggregated datasets, or derived data.

Third parties should also be able to set a timeout or expiry for consent, if not approved within a certain time. Third parties should also be able to remove a consent that is no longer valid, e.g., if a payment has been made using another method.

30.

Should customers be able to opt out of specific uses of their data that are not necessary to provide the service? Do you have any comments on the advantages and disadvantages of this?

Please see paragraph 8.2 of our submission and noting points in question 29 regarding the complexity of the models when an intermediary is used and the likely customer confusion around who is providing the service.

In principle ANZ supports customers being able to opt out of some specific uses of their data. However, we recognise the additional cost this could bring, and this is something that has been considered by industry standards today.

An alternative, and potentially more practical approach, could be:

- 1) to have obligations for any non-essential use of data or uses of data to be disclosed at time of consent. Apple have a concept of 'Privacy Nutrition Labels' that require apps to disclose what types of data your app collects and how it is used. See <https://developer.apple.com/app-store/app-privacy-details/>.
- 2) if there is on-sharing outside of the terms and conditions to other parties with different terms and conditions, these must be disclosed at the point of consent and the customer must agree to them. See Scenario 2a - Sharing with an unaccredited customer proposition from an accredited customer proposition, Attachment A, page 19.

Further consideration is required in relation to:

- how changes to terms and conditions will be made. For example, should customers be explicitly informed and given the option to withdraw their consent if the terms of use change?
- what happens if consent is withdrawn? and
- intermediaries' services.

Included in our 15 key recommendations, see Attachment A, Page 14 is a recommendation that if an intermediary service is used, it should be limited to providing their service within the scope, purpose, terms and conditions agreed by the customer in the customer proposition and should not be permitted to unreasonably extend the purpose and scope from what is required to provide a service to that customer proposition. This would limit intermediaries from broadening the purpose, scope and use and avoid the option of needing to ask the customer if they would be happy for the purpose and scope defined by the customer proposition to be extended.

We also recommend that on-sharing should be restricted to accredited intermediary services and parties disclosed in the consent. If this recommendation was not adopted, then to manage risk the risk of on-sharing occurring without visibility of account holders, customers must have the option to choose whether they allow the on-sharing of their data or action rights, at the point of consent.

31.	Should customers have the ability to set an expiry on ongoing consents? Do you have any comments on the advantages and disadvantages of this?
32.	ANZ supports an open-ended consent with requirements for customers to receive regular reminders about the consent, rather than for consent to automatically expire at a set point in time.
32.	Do you agree with the proposals in this paper to help ensure that consents given to accredited requestors acting as intermediaries are sufficiently informed? Are there any other obligations that should apply to ensure that consents given to intermediaries are express and informed?
32.	Please see paragraphs 8.3 - 8.4 of our submission and Attachment A, Page 14 for key recommendations on accredited requestors acting as intermediaries.  ANZ agrees with paragraphs 141 to 145 of the Discussion Paper that accredited requestors must meet additional requirements when they act as intermediaries, such as subsequent consent requirements for sharing with unaccredited parties. However, ANZ has some concerns about how these additional requirements are applied.



***Accredited requestors should be responsible for ensuring unaccredited parties receiving open banking data continue to comply with the Regulations and Standards.***

ANZ disagrees with the propositions in paragraph 146 of the Discussion Paper, that unaccredited persons should not be subject to any restrictions on their use and disclosure of data.

This means any further sharing of open banking data will only be governed by the Privacy Act (and this only applies to personal information). As we have outlined in our response to question 14 above, the Privacy Act is not equivalent to the protections under the Regulations and Standards. By not extending the obligations under the Bill and the Regulations and Standards to unaccredited persons, this will create the same issues as ANZ has previously raised in its submission on the Bill.

Further, by not imposing similar obligations on all participants of the open banking ecosystem (data holders, accredited requestors and unaccredited persons), it may discourage unaccredited persons to request data from accredited requestors, as requesting data from another unaccredited person will be less cumbersome. This may reduce the transparency and security benefits the open banking regime provides, and it could increase risks around data retention and secondary data uses by unaccredited persons.

ANZ submits that accredited requestors should be responsible for ensuring that unaccredited parties receiving open banking data continue to comply with the Regulations and Standards, as this will ensure that security and privacy obligations under the open banking regime continue to apply, regardless of who is holding and sharing the customer data. Unaccredited parties should also be obliged to operate within the boundaries of the original customer consent, and accredited requestors should be responsible for monitoring this.

***Customers need to be adequately informed, to avoid confusion.***

It is not clear on how consent requirements will practically work to ensure express and informed customer consent when an intermediary is involved. This could lead to many potential sharing scenarios with unintended consequences, without clearer and more specific requirements. This is further complicated as there is no clear restriction of on-sharing.

Key areas of likely customer confusion and concern are:

- Purpose and scope: For what service is the customer giving consent? This is critical and will determine the purpose of the consent and the minimum data/rights needed to provide the service.
  - Is this the customer proposition where the customer originated, the intermediary service, or both?
  - Should an intermediary be able to set a scope and purpose greater than that required by the customer proposition, if that is necessary for them to provide their service? Or should the intermediary be limited to providing a service to the customer proposition only, or only within the purpose defined by the customer proposition?

- Which party is ultimately responsible for determining the scope and purpose of the consent?
- Where their data is being shared, stored and used:
  - Customers may be confused as to whether they are sharing with an accredited party or an unaccredited party.

When an accredited party is introduced, it would be reasonable for customers to expect that all parties are accredited to the same level and that protections are the same.

Given this, customers must be informed when their data is shared outside of the open banking regime explicitly, and what protections the customer will lose by agreeing to such use. Customers should also be informed that:

1. if their data is 'personal information', the Privacy Act will also apply; and
2. if their data is business information or actions, no other protections will apply.

This information should also be disclosed to data holders, so that they can make customers aware at the time of confirming their consent.

***The additional requirements should cover all businesses acting as intermediaries.***  
 ANZ submits that the language should reflect all businesses "acting as intermediaries", and not just businesses that identify themselves as an intermediary. This will limit the situations where an accredited requestor becomes an unaccredited intermediary.

***Additional considerations:***

ANZ submits the following in relation to the following points made by MBIE in the Discussion Paper:

1. In relation to paragraph 142, intermediaries should not be able to change the purpose and scope of the original customer request.
2. In relation to paragraph 143, this information should also be disclosed to the data holder. This should extend to how each party will use that data (such as providing their terms and conditions, or privacy policy), as well as what happens to their data when the customer revokes their consent.
3. In relation to paragraph 144, this subsequent consent needs to go back to the data holder, and not just through the intermediary.

33.	Do you agree with the proposals to ensure that payment authorisations given to accredited requestors are sufficiently informed? Are there any other obligations that should apply to ensure that payment consents are express and informed? Should there be any other limitations on merchants or other unaccredited persons collecting authorisations, or instructing payments?
34.	As drafted, an intermediary would only be accountable for informing a customer, and not for any other failings (such as their practices and processes failing to meet the standards). ANZ submits that an accredited requestor should also be liable to redress data holders and customers if they fail to meet their other obligations under the Bill.
34.	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?

	<p>ANZ supports the need for customer dashboards to give customers and other account holders the visibility and control of consents. These must be consistently available at customer propositions/third parties and for data holders.</p> <p>Please see paragraph 8.4 of our submission and Attachment A, Page 14 for key recommendations 12-14 covering visibility and consistency of consent management and respecting the authority of all customers.</p> <p>We recommend MBIE consider a phased approach that:</p> <ol style="list-style-type: none"> <li>1) initially sets a minimum requirement for mobile applications as this is aligned to the mobile first approach that industry has taken today; and</li> <li>2) considers if additional channels are necessary given target customers and those served by data holders' mobile channel.</li> </ol>
<b>Joint customers</b>	
<b>35.</b>	<p>Should there be any exceptions to joint customers being able to access account information, other than those provided by clause 16 of the Bill? What would the practical impact of additional exceptions be on the operation of open banking?</p>
	<p>Please see paragraph 8.9 of our submission.</p> <p>Account mandates say who can use an account, and how (see: <a href="https://bankomb.org.nz/guides-and-cases/quick-guides/bank-accounts/account-mandates">https://bankomb.org.nz/guides-and-cases/quick-guides/bank-accounts/account-mandates</a>). There is no clear mandate or account authority for data sharing today and this has been an ongoing conversation for industry.</p> <p>For example, some customers only have 'view access'. While a customer's transactional data can be downloaded and shared with view access today, customers with view access do not have rights to operate or make payments on an account.</p> <p>Agreeing to an instruction to setup ongoing data sharing more closely aligns to a 'transact', 'operate' or 'owner' mandate. However, it is not clear which customers can instruct data holders to set up open banking data sharing, meaning data holders might be accepting instructions from customers with 'view access'</p> <p>There has also been uncertainty about how data sharing should work for a multi-authorisation mandate when more than one person must approve a transaction. This is mostly used by businesses, but it is also relevant for other organisations as part of their governance processes.</p> <p>Further guidance on how existing mandates should apply within the Bill needs further conversation with industry and customers.</p>
<b>36.</b>	<p>Are regulations needed to deal with joint customers making payments, or are the default provisions of the Bill sufficient? What would the practical impact of the default provisions of the Bill on the operation of open banking?</p>
	<p>Please see paragraph 8.9 of our submission.</p>

There is clear equivalency with existing mandates for payments. If a customer can make a payment today without the approval of another account holder, then the custom can approve an open banking payment consent.

ANZ also notes that the Discussion Paper does not consider multi-authorisation payment consents, and this is not currently supported by industry standards. From our experience, this would be more valuable than some other features the Discussion Paper proposes to include, such as the requirement to provide .pdf statements.

## Secondary users

37.

Are there any issues with designating authorised signatories on a customer's account as secondary users? What else should regulations provide for secondary users?

Please see paragraph 8.9 of our submission.

## Payment limits

38.

How should payment limits be set?

Payment limits are a very complicated topic. They are one of the key controls we use to maintaining customer and system trust by balancing:

- our responsibility and duty of care to our customers to keep them and their money safe, with
- the customer ability to freely engage in trade/make payments, with
- ANZ's risk exposure.

Limits can vary by customer, type of customer, payment type, channel and third party. Today, risk exposure sits with banks and therefore rightly control payment limits.

As proposed, the risk factors and risk exposure is likely to be very different under the CPDB and inherently higher risk because, but not limited to:

- the proposed liability regime could be different,
- the accreditation criteria of third parties is likely to be lower than what banks are held to and operate at,
- the maturity and size of third-party operations and their ability to focus on fraud preventions - compared to banks who have teams of people and extensive preventative fraud protections and controls in place,
- the third party's ability to redress customers or banks when something does goes wrong,
- the fraud protections in place for open banking payments may not be equivalent to other payment types,
- new payment type/experience that introduces new and different fraud considerations and various attack vectors that continuously evolve,
- the final rules, standards and use cases,
- the level of information provided to support informed fraud assessment and decisions, and that

- on-sharing may occur to unaccredited third parties with even lower controls

These risks and the risk exposure need to be fully understood, controlled, mitigated, and/or accepted with a clear liability framework before any changes to the status quo are made.

We would be comfortable with third parties setting lower limits than what we are providing to third parties to reduce their risk exposure.

### Remediation of unauthorised payment

39. Do you agree that accredited requestors should remediate banks for unauthorised payments that they request? Are there any other steps that should be required to be taken where unauthorised payments occur?

Please see paragraphs 8.7 - 8.8 of our submission. ANZ supports the principle that accredited requestors should remediate banks for unauthorised payments that they request. ANZ also strongly supports a safe harbour to cover situations where ANZ has complied with its obligations under the Bill and Regulations and Standards in good faith.

### Content of the register and on-boarding of accredited requestors

40. What functionality should the register have? Is certain functionality critical on commencement of the designation, or could functionality be added later?

N/A

41. What additional information needs to be held by the register to support this functionality? Should this information be publicly available, or only available to participants?

As per our comments at paragraph 6.6 of our submission, it is not clear whether banks have AML/CFT obligations in relation to accredited requestors. MBIE should conduct CDD on accredited requestors as part of the accreditation process, and make the assessment available on the register.

42. Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?

N/A

### Content of policies relating to customer data and action initiation

43. Do you agree with the proposed content of accredited requestor customer data policies? Is there anything else that should be required to be included?

In addition to the requirements specified in paragraph 180 of the Discussion Paper, the Regulations and Standards should also consider the following:

1. In relation to paragraph 180(b), if the geographic location of where the data is stored is outside New Zealand, the storage provider or cloud provider should also be required to protect the data in a way that, overall, provides comparable safeguards to those in the Bill and the Regulations and Standards (similar to IPP 12 under the Privacy Act).
2. In relation to paragraph 180(c), "who benefits from each purpose for which customer data is used" is quite broad, as there may be indirect beneficiaries who may not be involved in collection, use or disclosure of the data. MBIE could consider narrowing this to only specify who will be directly using or benefiting from the data. This should also apply to paragraph 180(d), in relation to de-identified customer data.

Furthermore, the customer data policy should also:

3. describe the process for obtaining express and informed consent from customers and explain how the consent can be withdrawn;
4. specify third parties with whom the data will be shared with and expressly state that these unaccredited parties may not apply the same standards as the open banking regime;
5. specify how long data will be retained for and how it will be securely deleted if it is no longer required;
6. specify how customers will be informed about changes to the policies and how they can contact the requestor should they have questions or concerns, and how they can exercise their rights under the Bill; and
7. outline procedures on how data breaches and other security incidents will be handled, and how the notification process will work.

## Standards for open banking

44.

Do you agree with the proposed standards? Should any additional standards be prescribed?

See paragraphs 9.1 – 9.3 of our submission. ANZ supports leveraging existing open banking standards, but ANZ's success is dependent on flexibility with exemptions, and the equivalency principle.

45.

When should version 3.0 of the API Centre standards become mandatory?

The timeline of version 3.0 should be considered and prioritised alongside other priority items that are currently not included in the industry plan.

These include, but not limited to:

- Mandated performance requirements and reporting to 150 tps\* (XXL) to 50tps (XL)
- Mandated support requirements (L),
- Integration into a centralised register (M),
- Web channels\* (XL),
- Multi-authorisation payments and potentially data sharing (XL),
- Product data\* (XL),

	<ul style="list-style-type: none"> <li>• Any changes to industry standards*,</li> <li>• Ability for consent to contain details of opt in aspects of the consent (M),</li> <li>• Access to 7 years of data* (XL).</li> </ul> <p>*ANZ's recommendation is that these are deferred.</p> <p>A fair and reasonable timeframe should be provided to implement agreed scope after the version 2.3 Implementation Plan has been delivered in November 2025.</p>
46.	If product data were included in the designation, what standards should be adopted or developed for product data?
	As discussed above, ANZ does not believe that product data should be included in the designation at this time.
47.	Do you have any comments on performance standards that should apply?
	<p>There needs to be sufficient standards to support third party propositions in the market, whilst considering the number of customers using that third party service. It is best practice to assess the criticality (whether there are alternatives for customers to use when the service is down, etc.). This means evolving the performance standards overtime.</p> <p>In addition, the performance of the systems needs ongoing reporting and monitoring to continue improving the systems. This should not be limited just to technical measure but include trust and operational aspects. All parties should be required to report on:</p> <ol style="list-style-type: none"> <li>1. parties who have been onboarded or off boarded;</li> <li>2. customer complaints received relating to open banking services;</li> <li>3. any disputes currently under investigation; and</li> <li>4. confirmed cases of fraud.</li> </ol> <p>Equally, the performance should be assessed at a high level across all parties for the benefit of customers and businesses wanting to use third party services.</p>
48.	How can MBIE most effectively monitor performance?
	ANZ supports retaining existing institutional arrangements via the API Centre.
49.	Are existing institutional arrangements with the API Centre fit for purpose, to achieve desired outcomes? If not, what changes should be considered? How should the approach change over time as other sectors are designated?
	ANZ supports retaining existing institutional arrangements via the API Centre.
<b>General Comments:</b>	

---

<sup>i</sup> The Office of the Australian Information Commissioner, *Sponsored accreditation model: privacy obligations of an affiliate*, December 2021, <https://www.oaic.gov.au/consumer-data-right/consumer-data-right-guidance-for-business/privacy-obligations/sponsored-accreditation-model-privacy-obligations-of-an-affiliate>

<sup>ii</sup> Boston Consultancy Group, *Building Trust in Business Ecosystems*, February 2021, <https://www.bcg.com/publications/2021/building-trust-in-business-ecosystems>.