Delegation systems and professional trust accounts

Akahu responses

19 June 2026

Thank you for the opportunity to respond to the consultation paper.

Ease of using open banking is critical to consumer uptake, and therefore the value that consumers will get from the regulated open banking system. So we think that the topics in this consultation paper are important, and we appreciate the thought that has gone into the proposal.

We support many aspects of the proposal, but we have some specific recommendations below that we consider would make the policies more effective and aligned with the purposes of the regulated system.

In particular, most of the issues in the consultation paper are related to whether customers are able to use the regulated open banking system by default. We think that equivalency should be the core guiding principle for default permissions. The regulated system should not provide customers with less ability to share data than they already have through a bank's electronic facilities.

Regulation 6

Issue 1: Logins in the name of the business

We agree with the description of this issue in the consultation document. In our experience to date, this is the only scenario where the Regulation 6 system would provide a net positive impact.

The current situation

This issue is commonly observed with ANZ business customers that use ANZ's goMoney app with credentials that are attributed to their business rather than an individual. In most cases these customers are unaware that this distinction exists.

When this subset of customers attempt to use ANZ's open banking service, they are presented with a generic error screen in the goMoney app. A portion of customers then abandon the process because there is no obvious way for them to self-diagnose and resolve the issue, and the other portion seek manual support from the 4th party service or Akahu to troubleshoot the issue.

When this type of support issue is raised to Akahu (directly by the customer or via one of our 4th party customers), we contact ANZ to diagnose the issue, because we cannot diagnose the issue ourselves based on the lack of detail provided to the customer in ANZ's error screen.

If ANZ confirms the use of non-individual credentials, ANZ recommends that the individual calls ANZ's call center to request that their business accounts are linked to individual credentials

through a process called "Customer Select"[1]. If the customer does not already have individual ANZ credentials, as is frequently the case, they have to first onboard with ANZ as a new customer (including identity verification processes) before they can proceed with setting up Customer Select.

This process creates significant support load, customer frustration, and abandonment because:

- Some individuals don't bother getting support and simply abandon the process.
- Some individuals request support, but by the time information has been gathered and shared with ANZ, and the issue has been diagnosed by ANZ, the individual is frustrated and unwilling to try again.
- When the resolution pathway is explained, some individuals don't want to spend time on the phone with ANZ's call centre to set up Customer Select.
- For the portion of individuals that decide to call ANZ's call centre and set up Customer Select, some don't already have personal credentials with ANZ, and need to onboard as a new customer in order to obtain personal credentials.
- A portion of individuals that contact ANZ's call centre are getting incorrect advice on how to enable open banking for their accounts, leading to further support load, frustration, and abandonment.
- Some individuals find that after completing the Customer Select setup, they have business accounts that aren't yet supported by ANZ for open banking.

The "nominated representative issue" in Australia

In Australia, a material portion of customers must first establish specific permissions with their bank before using open banking. This is known as the "nom rep" issue, and it has been a significant barrier to uptake in Australia's CDR regime.

The experience in Australia demonstrates that where a customer needs to actively set up access to open banking with their bank before they can use open banking, uptake is materially reduced and support burden increases. New Zealand should avoid creating a similar barrier to customer access.

Recommendations

We recommend that:

- MBIE provides guidance that the system referred to in the proposal must be available via the data holder's electronic facilities, to clarify that the obligations cannot be met through a call centre.

[1] Here is the PDF support article that Akahu created to help ANZ customers that experience this issue. This support article describes the process that ANZ customers are required to complete in order to set up Customer Select.

- MBIE provides guidance that the authorisation delegation system referred to in the proposal is intended to facilitate access to open banking where default access controls are insufficient. The system should not be generally applicable, and should not provide data holders with the flexibility to impose default barriers to using open banking.

Issue 2: Entitlement to authorise data-sharing via open banking

A large portion of customer support requests, frustration, and abandonment is due to banks implementing their regulated open banking services in a way that is more restrictive than unregulated open banking methods.

Appropriate default permissions to share data through the regulated system are fundamental to consumer uptake. We consider it critical that there is a stronger stance on default permissions than what is set out in the current proposal.

Issues with current default access to open banking in the regulated system

Over the last 6 months, we have dealt with a large volume of support requests from customers that have been attempting to use the regulated open banking system.

The most common issue is that accounts are simply not available to the customer after they have authenticated with their bank. Many of these customers are attempting to transition from an unregulated form of open banking, such as reverse-engineered integrations or proprietary APIs, to the regulated system. But when they attempt to connect their same accounts via the regulated system, those accounts are not available. This leads to significant customer frustration, customer churn from products that are using the regulated system, and a negative perception of the regulated system.

To provide a tangible example, Xero customers in New Zealand can access the following business accounts through proprietary bank APIs:

- ANZ: Multi-auth accounts, and other accounts that are only accessible via online banking, which ANZ has not yet made available in the regulated open banking system.
- ASB: Foreign currency accounts, and other accounts that are only accessible via online banking, which ASB has not yet made available in the regulated open banking system.
- BNZ: Multi-auth accounts, foreign currency accounts, term deposit accounts, and some types of business credit card accounts, which BNZ has not yet made available in the regulated open banking system.

- Westpac: Multi-auth accounts, non-profit accounts, and some types of credit card accounts, which Westpac has not yet made available in the regulated open banking system.

The current account coverage limitations in the regulated system create an uneven playing field for products that use open banking, and result in customers having a bad experience when attempting to use a product that relies on the regulated open banking system[2].

Equivalency is the most important principle for default permissions

Equivalency is the most important principle to apply to default permissions for data sharing. If a customer can download data from a bank's electronic facility and share that data manually, then that same customer should be able to share data using the regulated system.

We disagree with the assertion from some banks that data sharing is a materially different access permission from the ability to download data and share it manually. If sharing data through open banking is an "action", then downloading PDF or CSV files is an "action" too.

We agree with the comment in the consultation paper which notes that "if the customer has given an employee the technical ability to download account information through online banking, only the customer's own policies can address issues of inappropriate or unauthorised sharing of that information."

Insights from unregulated forms of open banking

Reverse-engineered bank integrations have been used in New Zealand for over 20 years. These types of integrations are inherently "equivalent", because they interface with APIs that serve the electronic facilities of the bank. So the account coverage and data coverage through reverse-engineered integrations are exactly equivalent to what the customer can access when logging in to the bank's electronic facilities.

In Akahu's case, we have used reverse-engineered integrations extensively for 5.5 years. We are not aware of a single instance where a business customer has claimed that an individual was acting outside of their authority when sharing data using an unregulated form of open banking. So we think there is a long track record to support the idea that, if an individual can share data manually via a bank's electronic facilities, that same individual should be able to share data using the regulated system.

If there were issues with applying the equivalency approach to default permissions, those issues would have become apparent over the last 20 years through unregulated forms of open banking.

[2] This issue is exacerbated because some banks are alluding to products like Xero using open banking APIs that are available to other third parties, when in fact those products are using proprietary bank APIs. This leads to business customers being confused and frustrated when the account coverage they had in a product like Xero is more restricted when they switch to another product that uses the regulated open banking system.

Data sharing is better than manual sharing options

The regulated system also offers more controls compared to manual abilities to exfiltrate data from a bank's system, for example:

- There is a clear audit trail of the individual who granted the consent, and the entity that has received the data.
- Any ongoing data consent is visible to relevant customers, and able to be revoked.
- The data is collected by an accredited requestor, which has regulatory obligations.
- The data is restricted to what the accredited requestor has specifically requested, as opposed to the more expansive dataset that is often downloaded manually by default.
- The data is shared via API, rather than being downloaded to a local computer and often shared through other mechanisms such as email from there.

Default options are much more important than the Regulation 6 system

We think it's critical that default permissions to share data are addressed through guidance (or amendments to the general definitions in the regulation if required), rather than the system referred to in Regulation 6.

If banks are able to design their own policies regarding default permissions, without a requirement regarding equivalency, the regulated system will be more restrictive than unregulated open banking methods, and customer uptake will be negatively affected. This is clearly visible from the current bank implementations which offer a non-equivalent level of default access.

The system referred to in Regulation 6 should be reserved for narrow scenarios like the ANZ scenario described in the section above.

Recommendation

We recommend that:

- The regulations require equivalency with a customer's ability to access data or make payments in the bank's electronic facilities.

We think this is by far the most important principle to ensure appropriate default access to open banking, and that a bank's "policy for default access" must comply with this obligation. Equivalency should be defined in the regulation so that it applies to all banks in the same way, to avoid differing interpretations of that requirement.

Issue 3: Customers who require multiple authorisers to make payments cannot share data through open banking

Data sharing from multi-auth accounts was in-scope for the Payments NZ-governed system

Default permissions for data sharing, including for multi-auth accounts, is a topic that was discussed extensively in API Centre forums. The purpose of those discussions was to flush out whether we needed to develop standards for data sharing from multi-auth accounts. But since all banks that were part of the implementation plan confirmed that they would support authorisation of data sharing from a single individual (and not require multiple authorisers on an account to approve a data sharing request), then it was decided that specific standards to address this scenario were unnecessary.

Given this background, we think it is disingenuous for any bank to now claim that its internal policies restrict a single individual from sharing data from a multi-auth account.

In our view, subject to the time-based exemptions regarding business platforms, the regulation already requires banks to support data sharing from multi-auth accounts. There is a specific exclusion for payment initiation from multi-auth accounts, and no equivalent exclusion for data sharing. So in our view, if a multi-auth account is a "relevant account", then the general obligations apply.

We recommend:

- Guidance to clarify that multi-auth accounts are required to be supported for data sharing through the regulated system. We note that many multi-auth accounts are accessible via platforms that are currently subject to the time-based exemptions, which provide banks with ample time to make any necessary changes to support those types of accounts for data sharing.

Professional trust accounts

Default permissions to authorise data sharing

As discussed above, we consider it critical that the regulation has a stronger stance regarding default permissions for data sharing. Specifically, we think that the regulation should require equivalency for default permissions, meaning that if an individual can download and share

data manually via a bank's electronic facilities, then the same individual should be able to share data via the regulated system.

We think that this rationale applies equally to professional trust accounts. In this scenario, a single individual can share data manually, so there is no rationale for a bank to apply additional restrictions to sharing data via the regulated system.

We strongly recommend that default permissions to share data are addressed through guidance (or amendments to the general definitions in the regulation if required), rather than the system referred to in Regulation 6.

If banks are able to design their own policies, without a requirement regarding equivalency, the regulated system will be more restrictive than unregulated open banking methods, and customer uptake will be negatively affected. This is clearly visible from current bank implementations which offer a non-equivalent level of default access.

The system referred to in Regulation 6 should be reserved for narrow scenarios like the ANZ scenario described above.

Demand from these types of customers

While this segment of customers with professional trust accounts is small in number, the demand for open banking and customer value are both very high.

Akahu has facilitated unregulated forms of open banking for all of the five example groups that are described in the consultation paper. In particular, there is high demand from body corporate managers, property managers, and non-bank financial service providers. These organisations often want to implement a high level of automation to their operations, and want programmatic connectivity with their bank data in order to facilitate that automation.

We consider it very important that this customer segment is supported through the regulated system.

Inclusion of client accounts

Paragraph 31 describes concerns that MBIE has received from interested parties regarding sub-accounts. We consider that most of these concerns are incorrect or misleading, and we provide comments on each point below.

> *a. Standards: The standards are ill-suited to these types of account, as the client accounts have account numbers in a different format from general bank accounts and are not reflected in the standards*

We think this assertion is incorrect. Many accounts, such as credit card accounts, savings accounts, loan accounts, and investment accounts, often use account identifiers that are in a

different format from general bank accounts. This does not cause a problem, and has no bearing on whether these accounts are required to be supported in the regulated system. Multiple banks already make accounts with "non-standard" account numbers via the regulated system, despite these formats not being technically supported by the standards.

> *b. Cost: It will be costly for the banks to implement, as specific technology will be required in relation to these types of account*

We understand that costs associated with supporting open banking are largely related to enabling open banking for a specific digital platform.

> *c. Authorisation: There are uncertainties about who the 'customer' is for the client accounts – whether it is the holder of the account, or the client for whom the account is held on behalf. This results in uncertainty about who would be able to authorise open banking requests from these accounts: the account holder or the client.*

There is no uncertainty on this point. The legal owner of trust assets is the trustee(s). If an account is held by a trustee(s), then any individual with authority to act on behalf of the trustee(s) is able to use open banking. This scenario is no different to other types of accounts that are supported via the regulated system where the account holder is a trustee.

> *d. Legal obligations: It could inadvertently put professionals at risk of breaching their legal obligations if they share data or payments without the clients' permission.*

We think this assertion is incorrect. Trustees already have the ability to share data and initiate payments on behalf of beneficiaries in a bank's electronic facilities. Open banking enables those same activities in 3rd party software. For example a body corporate manager may share data into an accounting solution like Xero.

> *e. Use cases: As with the umbrella accounts, there is uncertainty as to use cases for open banking for these types of account.*

We think this assertion is incorrect. The use cases for "umbrella accounts" are well-understood and commonly supported through unregulated forms of open banking. The most popular use cases are:

- Sharing data with accounting and tax solutions.
- Sharing data with internal systems in order to automate reconciliation processes.
- Sharing data with internal systems for automated notifications and reporting.

Whether sub-accounts are call debt securities

Banks may structure professional trust accounts differently

We understand that banks may structure professional trust accounts in different ways.

The professional trust account structure that we are most familiar with has a single parent account, which provides normal features associated with a transaction account, such as the ability to make payments.

That parent account may have multiple sub-accounts which serve as sub-ledgers for the parent account. This enables visual separation of funds that are held on trust for different beneficiaries or purposes.

In the structures that we are familiar with, all inflows and outflows go through the parent account. So if there is an inflow *to* a sub-account or outflow *from* a sub-account, there is a corresponding transaction record in the parent account. This means that the ability to share data from the parent account is generally sufficient to meet the needs of common use cases.

We think that general guidance on sub-accounts is unnecessary

If a bank has structured sub-accounts as a virtual abstraction layer over the parent account, and those sub-accounts do not have any rights that are independent of the parent trust account, then we agree with the view that those sub-accounts are not call debt securities.

However if the professional trust accounts are structured in a way that provides independent rights and obligations for each sub-account, then we think that those sub-accounts would meet the definition of call debt securities.

Accordingly, we don't think that MBIE should issue general guidance that sub-accounts are out of scope. Instead, we think that each bank should consider whether their particular structure leads to sub-accounts meeting the definition of call debt securities.

Recommendation on professional trust accounts

In our submissions regarding Regulation 6, we describe how unregulated open banking methods serve as a benchmark for how well the regulated open banking system is working.

We consider it critical that account coverage through the regulated system is on par or better than the account coverage that is available through unregulated open banking methods. So we consider it very important that professional trust accounts are supported in the regulated system, since they are already supported through unregulated forms of open banking.

We think the issues regarding professional trust accounts are well-addressed through our general recommendations regarding default permissions and Regulation 6, and there is no need for specific rules in relation to professional trust accounts. In particular, we recommend that:

- The "policy for default access" requires equivalency with a customer's ability to share data or make payments in the bank's electronic facilities. We think this is the most

important principle to ensure appropriate default access to open banking, and it applies well to the issues that have been raised in the consultation paper regarding professional trust accounts.

- MBIE provides guidance that the authorisation delegation system referred to in the proposal is intended to facilitate access to open banking where default access controls are insufficient. The system should not be generally applicable, and should not provide data holders with the flexibility to impose default barriers to using open banking. This is critical to avoid the "nominated representative issue" that has been a significant barrier to uptake in Australia's CDR regime, where a customer needs to actively set up access to open banking with their bank before they can use open banking.