MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Technical proposal: Delegation requirements and treatment of professional trust accounts for Regulated Open Banking

Overview

1. MBIE seeks feedback on proposals relating to the treatment within the Regulated Open Banking system of authorisation delegation and professional trust accounts. We invite feedback to consumerdataright@mbie.govt.nz by **midday Wednesday 10 June 2026**. Please indicate if there is any content in your feedback you would prefer to be withheld if your feedback is publicly released under the *Official Information Act 1982*.

Background to this consultation

2. In April 2026 MBIE consulted on draft amendment regulations to set out the pathway for extending open banking to a wider range of business customers. More information on that consultation is available at www.mbie.govt.nz/have-your-say/consultation-on-exposure-draft-amendment-open-banking-regulations-relating-to-business-banking-digital-channels.

3. After that consultation, in May 2026 Government amended the open banking regulations to require designated banks to extend Regulated Open Banking to customers that use their business electronic facilities by 1 June 2027, with some exceptions.

4. During that consultation stakeholders provided feedback about delegation system requirements and the treatment of professional trust accounts. The regulations needed to be amended before 1 June 2026 which meant there was insufficient time to properly analyse and address these issues as part of the broader changes.

5. MBIE is now undertaking further analysis and consultation on these two additional issues, which may result in subsequent amendments to the regulations in the coming months.

Objectives

6. Our analysis has been guided by the following criteria[1]:
   a. Provides for efficient investment and does not pose a barrier to entry in banking
   b. Provides for wide uptake by fintechs[2] and valuable services to customers
   c. Provides customer trust in information and payments security
   d. Aligns with the broader regulated open banking system.

[1] These criteria align with the criteria used to design the Regulated Open Banking system as a whole, which are set out in MBIE's 2025 Regulatory Impact Statement for the initial open banking designation.
[2] 'Fintechs' refers to financial technology companies, which in this case include accredited requestors and other organisations participating in the regulated open banking system through an accredited intermediary.

Confirmation and delegation system

Background

7. The *Customer and Product Data (General Requirements) Regulations 2025* include a requirement at Regulation 6 that banks provide a system for customers (such as businesses) to notify the bank that individuals associated with the business (such as their staff or accountants) have the authority to give consent to share the customer's bank account data via open banking.

8. Following the May 2026 amendments to the regulations, this requirement will now commence on 1 June 2027, alongside the requirement for banks to provide open banking on their business electronic facilities.

9. In consultation on the draft amendments, submitters generally supported the intent of providing clarity about how this kind of delegation should occur, but had concerns about how the system would apply in practice.

Problem definition

10. Regulation 6 was intended to address three issues that were identified by fintechs in 2025:

Issue 1: Logins in the name of the business

11. The first issue relates to some business accounts which have online banking logins in the name of the business, rather than in the name of individuals associated with the business. As open banking is structured so that authorisations for data-sharing and payments are made by identifiable individuals, when the banking login is in the name of the business itself, there is no individual who has the technical entitlement to authorise open banking. Currently when one of these business customers wants to authorise data sharing or payments via open banking, they must undertake a complex and time-consuming process to notify the bank and rectify the issue. This creates significant friction and reduces open banking uptake.

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

12. The second issue relates to levels of entitlement to authorise open banking data-sharing. A business customer of a bank can assign various entitlements to individuals associated to the business (e.g. staff, accountants). Each of the banks have a slightly different set of entitlements for the customer to choose from. For example, the entitlements might include (from least to most access):

View only	The individual can view transaction history and download statements, but cannot create or approve payments, change payees, or open and close accounts.
Prepare transactions	The individual can prepare payments, set up payees, view balances and transactions, but cannot approve or release payments, or change entitlements.
Approver	The individual can create payments and approve payments created by others, but they might be subject to approval limits and cannot change entitlements.
Administrator	The individual has full access and can add or remove users, assign authorisation roles and permissions, and set transaction and approval limits.

13. There is a discrepancy of views on how banks should treat individuals who are able to view data, but not to make payments. In the list above, this would be the ‘view only’ entitlement and the ‘prepare transactions’ entitlement.

    a. Some stakeholders, primarily fintechs, have expressed that if a customer is able to download PDF bank statements and share them with a third party (for example, via email), then they should be permitted to approve data sharing requests. They consider that open banking is a more secure way to share this kind of data than the status quo of downloading and emailing.

    b. Other stakeholders, primarily banks, have expressed that since data-sharing is an action, these customers, who do not have the entitlement to undertake other types of actions on the account such as approving and releasing payments, should not be able to authorise data-sharing via open banking. For example, an individual may use their ‘view only’ entitlement to download bank statements for internal filing and audit purposes, with no intend beyond internal capture. These stakeholders consider that even if the individual is technically able to screenshot transactions and download PDF statements, their organisation (the customer) might not approve them to share those documents externally. The organisation may have an internal policy requiring signing of a contract before sharing bank account data with a third party, and individuals with these lower-level entitlements may not have seniority to sign those contracts.

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

14. Related to Issue 2 above, some banks have indicated that where a customer has specified that multiple authorisers are needed to make payments, multiple authorisers would also be needed to confirm data-sharing authorisations.

15. New Zealand’s open banking regulations and standards do not yet support multiple authorisers. Without a mechanism for a customer to approve a single individual to confirm data-sharing authorisations, these customers have no way to share data through open banking.

Current approach to addressing these issues

16. When drafted in late 2025, Regulation 6 was intended to empower the customer to decide what kind of entitlement to authorise open banking the individuals associated with the customer should have. Therefore, the current drafting of Regulation 6 intends for businesses to be given the option of approving an individual just to authorise sharing of customer data (potentially bundled with other activities such as viewing and downloading data), which will usually be lower risk than approving an individual to make payments. Regulation 6 provides an opt-in mechanism for a customer to approve individuals to confirm data sharing authorisations, but does not address the ‘default’ entitlements of those individuals. MBIE considered this approach to be a middle ground between the views expressed above.

Concerns with current approach

17. During consultation in April 2026, submitters had concerns that the way Regulation 6 is currently drafted could result in unintended consequences in practice. Both banks and fintechs were concerned that the current drafting could unintentionally result in banks requiring *all*

individuals associated with the account to have their entitlement confirmed through this system (including those who already have entitlement to act on the account and make payments) which could create significant friction and reduce uptake. This is not the policy intent of Regulation 6, but because it is silent on default entitlements, it is possible that this practice could develop.

18. Submitters also expressed concern that operating a separate set of entitlements relating to data sharing under open banking creates complexity for banks and could be unnecessarily confusing or burdensome for customers.

Proposed approach

Proposal

19. To address these concerns, we propose that regulation 6 is replaced with the following three-part requirement:

    a. **Part 1: System to verify identity**

        i. To enable a data holder to confirm that a requested service is within the scope of the authorisation given by the customer as required by s 39 of the *Customer and Product Data Act 2025* (the Act), a data holder must provide a system for the customer (if the customer is an individual), or an individual acting on behalf of the customer, to verify their identity.

        ii. This system must be provided to any individual who has access to data about the account through an electronic facility.

        iii. If the customer is an entity with access to data about the account through an electronic system, the system must be accessible by at least one individual acting on behalf of the customer.

        iv. This system must be the same as, or no more onerous than, the system used to verify the identity of the individual when accessing data about the account through the electronic facility.

    b. **Part 2: Policy for default access**

        i. The data holder must have a policy that sets out which individuals may, on behalf of the customer, confirm an authorisation in respect of a request to share data under section 15 of the Act.

        ii. In developing this policy, the data holder must take into account:

            (1) the extent to which the individual is entitled to view and download data about the relevant account from the electronic facility according to their existing online banking entitlements,

            (2) the extent to which the individual can share data (previously downloaded or otherwise) with another person, and

(3) the complexity of the customer's banking arrangements, including the complexity of the online banking authorisation entitlements held by individuals acting on behalf of the customer.

c. **Part 3: System to approve individuals to act on behalf**

i. The data holder must have a system in place to enable a customer to do the following:

(1) approve an individual (acting alone) to act on the customer's behalf to confirm an authorisation in respect of data-sharing requests under section 15 of the Act, including the ability to specify limits, conditions, or duration applying to that approval, and

(2) view, amend or revoke that approval.

Explanation

20. This means that banks would need to enable the following:

a. **Part 1:** As at present, banks would need to enable individuals with access to a customer's account on online banking to authenticate themselves. This mechanism could continue to use online banking login systems, or banks could develop a separate system.

b. **Part 2:** Banks would need to design and implement a default access policy that sets out which individuals, based upon their level of online banking access, are able to confirm data sharing authorisations on behalf of customers. Further detail on the rules for how default access settings are designed and applied could be supported through standards or guidance.

c. **Part 3:** Similar to existing regulation 6, banks would also need to provide a system for customers to amend individual access rights if the bank's default policy is unsuitable for them, including by setting or changing limits, conditions or duration.

Other factors for the default access policy that we considered

21. In preparing the proposal for the default access policy described at Part 2, we considered whether other factors should be taken into account by banks in determining the default access policy, such as the likelihood that the customer approves of the individual sharing data through open banking. The difficulties with including this factor are:

a. Banks have limited information about what a customer has approved its employees and agents to do on the customer's behalf, such as entering into contracts with accredited requestors, or share data with accredited requestors.

b. These matters may be more effectively addressed by customers through their own internal policies, rather than by banks. Customers' internal policies already need to address these matters outside of open banking: 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.

Discussion questions

22. We invite responses on the following questions in relation to Regulation 6:

Problem definition

a. How does the problem definition align with your experience in practice? Are there aspects of the problem that have been underemphasised or overlooked?

b. What additional issues or edge cases should be considered to fully understand this problem? Are there distinct sub-problems affecting different user groups?

Proposed approach

c. Do the factors outlined at Part 2 – and in particular, the third factor relating to the complexity of the customer's banking arrangements – provide the right level of flexibility?

d. Should Part 3 specify that banks should offer the option of a specific entitlement role whereby an individual would be permitted to authorise open banking data-sharing on behalf of a customer, but not to authorise payments?

e. Does the proposed approach provide enough clarity for banks, fintechs and customers? If not, how could more clarity be provided?

f. Are additional safeguards needed to prevent inappropriate delegation within organisations (e.g. junior staff overreach and fraud risks) or can this be managed by the customers' in-house policies? If additional safeguards are required, what should these be?

g. How will the proposals affect small vs large businesses, and Māori organisations?

h. Are there international models or best practices that could inform New Zealand's approach?

Implementation, standards and guidance

i. Do you foresee implementation challenges for banks, fintechs, and/or customers (including business customers, and customers that are Māori organisations)? If so, what transitional arrangements or guidance would help ensure a smooth rollout?

j. Should MBIE provide more standardisation of open banking entitlement options (e.g. baseline rules or model policies) or leave flexibility to banks?

Professional trust accounts

Background

23. Some bank customers hold professional trust accounts, which enable them to manage funds on behalf of multiple clients. ANZ, ASB, BNZ and Westpac offer these types of account.[3]

24. Examples of banks' customers that might hold a professional trust account include:

a. Solicitors, who use the accounts to hold clients' money for business transactions, or for conveyancing purposes

[3] The service offerings are ANZ 's Trust Management Services, ASB's FastNet Business Professional Trust, BNZ's Client Fund Service, and Westpac's Multi-Deposit Scheme.

b. Body corporate managers, who use the accounts to hold body corporate funds on behalf of the different body corporates that they manage

c. Property managers, who use the accounts to hold different rental income on behalf of different landlords

d. Non-bank financial service providers, who use the accounts to hold client funds for purposes such as investment or deposit-taking

e. Māori organisations such as Post-Settlement Governance Entities and whānau trusts, who hold funds for multiple beneficiaries, such as individual hapū, whānau or descendants.

25. Professional trust accounts consist of a single **umbrella account** (sometimes called 'source account'), within which are multiple **client accounts** (sometimes called 'sub accounts' or 'virtual accounts'). The client accounts function as separate ledgers and allow the professional to keep different clients' money separate within the same overarching umbrella account.

26. Holders of professional trust accounts are subject to trustee duties set out in the *Trusts Act 2019*, which mean they face legal obligations relating to the way they manage clients' funds. Additionally, some holders are subject to industry-specific requirements, such as the requirements in the *Lawyers and Conveyancers Act (Trust Account) Regulations 2008*.

27. Online banking (via mobile or internet) for these accounts is accessed through each banks' business electronic facilities.[4] These facilities will be included in the Regulated Open Banking system from 1 June 2027. This means that from 1 June 2027, banks must enable professionals to access regulated open banking from the umbrella accounts for professional trust accounts. This includes:

a. Sharing of customer data that can be viewed in the electronic facility, for example, the overarching balance of the umbrella account

b. If relevant, payments where only a single authoriser is required (however, many professional trusts will be out of scope for payments, because their payments require dual authorisation. This is where one individual initiates the transaction and another individual authorises it).

Problem definition

28. In consultation on the draft amendments banks raised concern about the imposition of open banking requirements on these accounts.

Inclusion of umbrella accounts

29. Regarding the inclusion of umbrella accounts, interested parties expressed concern that:

a. **Dual-authorisation data-sharing**: Because many professional trust accounts have dual-authorisation requirements for payments, some banks have indicated that they would set a

[4] These electronic facilities are ANZ Direct Online, ASB FastNet Business, BNZ Internet Banking for Business, and Westpac One Business.

default position that multiple authorisers would also required for data-sharing, which, because multiple authorisers are not supported by the open banking regulations and standards, would result in account holders being unable to access open banking-enabled service unless this issue is addressed through the system described at Regulation 6.

b. **Use cases:** there are few known use cases for open banking for these accounts; which could mean that open banking will not deliver sufficient benefits to the holders of these accounts to justify the cost to banks of providing open banking technology.

Inclusion of client accounts

30. Regarding the inclusion of the client accounts, interested parties expressed uncertainty about whether the client accounts are also included within the requirements.

31. Interested parties expressed concern that if the client accounts are to be included:

    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

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

    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.

    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.

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

Proposed approach

32. Our understanding is that:

    a. the umbrella accounts **do fall within scope** of the open banking requirements, because they are a type of call debt security as set out in regulation 4(a)(i) of the *Customer and Product Data (Designations for Banking and Other Deposit Taking) Regulations 2025.*

    b. the client accounts **do not independently fall within scope** of the open banking requirements, because, as we understand it, they are not a call debt security or any other type of relevant account as listed in the regulations.

33. We propose that with respect to this issue, the regulations remain unchanged, and MBIE issues guidance that while the umbrella accounts fall within scope, the client accounts do not. The exclusion of client accounts could be revisited at a future time alongside the development of standards specifically for these types of account if demand emerges.

34. With respect to payments from the umbrella accounts, as with any other type of designated bank account, banks would only be required to enable open banking payments that require a single authoriser.[5]

35. With respect to data-sharing from the umbrella accounts, banks would be subject to the requirements of the delegation system outlined in the first part of this proposal document. This means that banks will be required to enable the holder of the account, in the case of an account where multiple authorisers are required to make payments, to authorise an individual, acting alone, to authorise data-sharing.

36. An alternative option for consideration is for the regulations to be amended to exclude professional trust accounts entirely. We seek feedback on potential use cases for open banking for professional trust accounts, and the potential impact of excluding the accounts.

Discussion questions

37. We invite responses on the following questions in relation to professional trust accounts:

Problem definition

a. How well does our description of professional trust accounts (both the umbrella accounts and the client accounts within them) reflect how they operate in practice? Please highlight any inaccuracies, gaps, or areas that require clarification.

b. Do you agree with our understanding that while the umbrella accounts are call debt securities, the client accounts are not?

c. What are the potential benefits and use cases for enabling open banking for:

   i. the umbrella accounts (payments and/or data-sharing)?

   ii. the client accounts (payments and/or data-sharing)?

d. What are the potential costs and risks of enabling open banking for:

   i. The umbrella accounts (payments and/or data-sharing)?

   ii. The client accounts (payments and/or data-sharing)?

Proposed approach

e. To what extent does our proposed approach strike the right balance between our intended objectives outlined at the beginning of this proposal document?

f. Would excluding professional trust accounts in their entirety enable us to better achieve these objectives? What are the trade-offs?

g. Are there international models or best practices that could inform New Zealand's approach?

[5] As set out in Regulation 8 of the *Customer and Product Data (Designations for Banking and Other Deposit Taking) Regulations 2025*.