Customer and Product Data Regulations

Akahu submissions

29 August 2025

Customer and Product Data (General Requirements) Regulations 2025

Clause 6(1)

We think that a data holder should be able to check an official resource to verify that the requestor has been accredited.

We think this could be achieved by MBIE hosting a webpage with a list of accredited requestors.

Clause 6(2)

We think that the proposed timeframe of 5 working days is reasonable, because the data holder is simply configuring technical access for the accredited requestor, rather than carrying out due diligence or other onboarding activities.

We suggest the following additional regulatory obligations in order to clarify expectations for data holders and accredited requestors:

- A data holder must specify the information that is required to configure technical access for an accredited requestor, and this information must be available through a public resource.
- A data holder must not require information that is not reasonably necessary in order to configure technical access for an accredited requestor.
- The 5 working day period begins after the accredited requestor has provided all information that is reasonably required by the data holder to configure the technical access.

Customer and Product Data (Banking and other Deposit Taking) Regulations 2025

Clause 7

General requirement regarding designated data

Alternative connectivity methods, like screenscraping and reverse engineering mobile APIs, have worked effectively and have seen high customer uptake because the customer data is the same as what's available via a bank's electronic facilities.

To date, the data available from official open banking APIs has been lower quality. For example the transaction data available from official open banking APIs can often lack the detail that is available via electronic facilities, making that data unusable for use cases such as accounting and tax solutions, personal financial management services, and credit applications.

We consider it critical that the regulated regime is very clear on the designated data requirements. This would enable data holders to be certain about their compliance obligations, it would enable accredited requestors to develop their product roadmaps with confidence, and it would enable the regulator to enforce compliance against clear obligations.

With the current wording in clause 7, we're concerned that there will be gaps between the data that is designated in the regulations and the standards that are made pursuant to section 138 of the Act.

We consider it critical that there is a general requirement that a data holder must provide at least the same information as required by standards that are made pursuant to section 138 of the Act, including optional fields if those fields are relevant for the particular account or transaction.

This type of general requirement is the most effective way to ensure that high quality data is available via regulated open banking APIs, and that accredited requestors can use the regime to deliver the intended innovation and competition benefits.

Without this type of general requirement, we expect there to be a prolonged period of disputes about whether specific data fields are designated, and delays in compliance and enforcement. If this dynamic emerges, it would erode trust in the regulated open banking regime and reduce customer uptake.

Data sharing from jointly held accounts and accounts that require multiple authorisers for payment initiation

In API Centre forums, the largest 5 banks each confirmed they would apply the "equivalency principle" to data sharing requests.

In this context, the equivalency principle means that if a single user can access and download account information to share that information manually with a third party, that single user can consent to a data sharing request via open banking APIs. This principle stands even when the account is jointly held or is configured to require multiple authorisers for payment initiation (because a single user can still access and download account information via a bank's electronic facilities in these scenarios).

However we're aware that not all data holders currently enable a single user to consent to a data sharing request if the account is configured to require multiple authorisers for payment initiation.

We recommend making it clear in the regulations that either:

- A single customer can consent to a data sharing request, even when the account is jointly held or requires multiple authorisers for payment initiation; or
- Each data holder must apply the equivalency principle, meaning that if a single user can access and download account information to share that information with a third party manually, that single user can consent to a data sharing request via regulated open banking APIs.

Payment obligations, authorisations for transactions, and payees

MBIE's open banking information page indicates that designated data will include "payment obligations" and "authorisations for transactions given in respect of accounts, such as automatic payments and direct debits" and "payees".

We could not see this information defined in clause 7. This information included in version 2.3 of the API Centre standards, so may be included at a later date by reference to standards pursuant to clause 138 of the Act, but we wanted to note that this data is not currently designated.

Clause 7(1)(a)

Account holder

We recommend including data that allows accredited requestors to unambiguously determine whether the customer is a holder of the account. This is necessary for bank account verification use cases.

We note that the person authorising the accredited requestor to access data may have "delegate" access, so their name alone is insufficient to determine whether they are a holder of the account. Additionally, the API Centre standards have different rules for accounts held by individuals compared to accounts held by businesses. Because of this, information about whether the account holder is an individual or business must also be supplied to ensure that accredited requestors can accurately determine account ownership in all scenarios.

Date of birth

We recommend including the date of birth of the customer.

This is useful for lending use cases, where the lender needs to verify an applicant's identity, and can also use this personal information to request data about the applicant that is held by a credit reporting agency.

Clause 7(1)(b)

Product name and and name of the account

The data requirements in this clause should clarify that both of the following values are available:

- The product name or name of the account; and
- The customer-assigned nickname or name for the account (if applicable).

Both values are necessary for accredited requestors to surface relevant information about each account to customers.

Type of customer

We think that clause 7(1)(b)(iv) may be intended to require the type of customer, such as individual, trustee, or company.

If so, we support that requirement, and consider it necessary for bank account verification use cases.

If this clause was intended to be interpreted differently, we recommend adding an explicit requirement for the type of customer.

Clause 7(1)(d)

We suggest changing "particulars of each transaction" to "all relevant particulars of each transaction" to define the requirement more clearly.

We understand that bank transactions are diverse, which makes it challenging to be prescriptive about required elements. However, we believe that it is crucial to remove ambiguity where possible to avoid disputes and non-compliance.

We suggest that the regulation should specify that the following data fields are required for each transaction:

- The value date and time of the transaction.
- The booking date and time of the transaction (or expected booking time if the transaction is pending).
- The status of the transaction.
- The amount and direction of the transaction.
- The currency of the transaction.
- Codes or descriptions that identify the type of transaction.
- Other data elements that are equivalent to the information that is available through the data holder's statements, exports, and electronic facilities.

In addition to required data for all transactions, we suggest explicitly specifying that the following data elements must be provided when relevant to the transaction:

- The counterparty's name (for example the merchant's name if the transaction relates to a purchase or refund, or the payee's name for a bill payment or transfer, or the payer's name for a direct credit).
- The counterparty's account number (for example the merchant's account number if the transaction is a direct debit or bill payment).
- User-provided reference information (for example the particulars, code, and reference fields provided for a bill payment).
- Currency exchange information including source currency, destination currency, and rate.

The requirements above would address known deficiencies in the API Centre standards, where there is currently inconsistent interpretation and data availability from data holders (described in our general comments above in relation to clause 7).

Clause 7(1)(e)

We note that this provision includes information relating to rates. If the account relates to a credit contract, we also recommend including the following requirements (if applicable):

- Whether the rate is fixed or floating.
- The repayment structure.
- The expiry date for any fixed term.
- The maturity date or end date.

This information is important to support refinancing use cases, but these data fields are not available for loan accounts in the API Centre standards, so we think it is important for these data fields to be described in the regulations.

Clause 7(1)(e) and (f)

Period of statement history

Some existing market activity requires more than 6 months of statement history. For example some lending use cases require at least 12 months of statement history.

We acknowledge that some data holders have adapted their systems in order to support the statement-related functionality that is described in the API Centre standards, and that it's much simpler from a technical perspective to support statements-related functionality from the time that those system changes were made.

As a compromise, we propose setting the minimum statement history availability based on:

- 12 months prior to the consent date; or
- 1 June 2025.

This will provide time for data holders to build up the relevant statement history after their system changes have been made, and to have that data available to share via regulated open banking APIs.

Official bank statements

We assume that clause 7(1)(f) is referring to the official statement type that is sent to the customer and made available in a bank's electronic facility.

However we think there is room to interpret these clauses in a way that refers to a different type of statement. We think the wording should clearly state that official statements, in the same format as is provided to the customer directly in the data holder's electronic facilities, form part of the designated data in these provisions.

Clause 8(2)(d)

We note that the API Centre standards do not currently support payment initiation from accounts that require multiple authorisers for payment initiation.

We support the clarity that these types of accounts are not currently required to be supported via regulated open banking APIs.

However we note that other payment methods like cards and direct debit do not have this same constraint with accounts that require multiple authorisers for payment initiation. This constraint has a major impact on customer uptake of open banking payments, and we encourage MBIE to set a deadline for regulated open banking APIs to support this functionality.

Clause 8(3)(b)(i)

Equivalency with electronic facilities

Banks often have different payment limits between their online banking channel and their mobile channel. This means that there is room for different interpretation of whether to apply equivalency to the limit of the online banking channel or the mobile channel.

We don't currently have a specific recommendation on this point, but want to note the potential for different interpretation of this provision by each bank.

We are also aware that some banks apply a multi-tiered approach to payment limits in their electronic facilities, where payment amounts beyond a certain threshold require step-up authentication (such as a one-time passcode sent via SMS). We think that the regulation should clarify how limits are applied in this scenario. Our recommendation is that the uppermost limit should be applied to open banking payments, and that step-up authentication required to unlock this limit is applied (if relevant) during the consent process based on the consent parameters.

Payment limits for registered bill payees

We support the equivalency approach towards payment limits in clause 8(3)(b)(i).

However we note that even with equivalency, payment limits will prevent open banking payments from working well in many scenarios.

For example, in the UK, tax payments have emerged as an important use case for open banking payments. If banks apply the same payment limits to open banking as they apply to their mobile apps, the New Zealand open banking regime will not support this use case effectively because tax payments are often for amounts that are much larger than the limits that are applied in mobile apps.

As another example, unregulated forms of open banking are commonly used in New Zealand to initiate payroll payments and fund investment accounts, and these payments are often for large amounts (we discuss these use cases in pages 19-21 of our 2025 open banking report).

High value payments are very well-suited to open banking, given the low cost of initiating an open banking payment. But the current approach to payment limits will prevent uptake in important scenarios.

We recommend using the existing registered bill payees system to define an exception to normal payment limits. When an organisation registers as a bill payee with their bank, that information is shared with the other banks, so that customers of all banks can search for the registered bill payee when making a bill payment. This means that each bank holds information about registered bill payees.

We recommend requiring that, when an accredited requestor is initiating a payment to a registered bill payee, a data holder cannot apply a lower payment limit to that payment request than it applies to that customer in its internet banking system.

This recommendation would have a major impact by enabling open banking to become a payment option for registered bill payees that often receive high value payments.

Clause 9(2)(a)(ii)

This clause describes a specific scenario where the customer is using a service "B", and consents to the intermediary initiating a payment to B's account. This scenario accurately describes many relevant use cases for open banking payments.

However there are many scenarios where the payment is not being made to B's account. We recommend that this clause is revised to enable an intermediary to initiate a payment in accordance with the customer's consent, even when the payee is not B.

We think that the existing wording at the start of clause 9(2)(a) provides the necessary context about the relationship between the intermediary "A" and B by stating: "...A provides a service to B under which—". This relationship is further described in clauses 9(2)(b) and (c).

So we think that the following revised wording in clause 9(2)(a)(ii) would resolve the issue: "A facilitates a payment from an account of a customer (C) (by way of A making a request under section 19 of the Act); or".

Support for business customers

We note that the Act is designed to apply to a range of customers, including businesses as described in section 24 of the Act.

However we're aware that not all data holders currently enable their business customers to use official open banking APIs. For example:

- Business login credentials: 3 banks only support login via personal login credentials. There is no way for a user to authenticate with their business login credentials in order to use open banking in relation to a business account.
- Accounts with multiple authorisers: At least 2 banks do not support data sharing for accounts that are configured to require multiple authorisers for payment initiation.

Support for business accounts is critical for many use cases, including accounting and tax solutions, payroll services, bank account verification, tax payments, and a broad range of SaaS products. These use cases cannot migrate to the regulated system until business accounts are well-supported.

We recommend making it clear in the regulations that data holders must support access to business accounts.

Authentication options

Equivalency with authentication options

The API Centre standards define multiple methods for a user to authenticate with their bank during an open banking connection flow. The intent was to provide a range of options so that users can successfully complete the connection flow using the device they're using and a familiar login flow.

However 2 banks currently require a user to log in to the mobile app of the bank as part of the authentication flow. This decreases customer uptake of open banking for multiple reasons:

- Mobile banking registration: This approach forces the user to be registered for mobile banking in order to use open banking. Some customers prefer not to use mobile banking, and many business users are not registered for mobile banking because they solely use online banking services for their business banking requirements.
- Mobile device on hand: In order to complete the authentication flow, the user must have a mobile device on hand with the bank's mobile app installed and registered on that device.
- Overseas users: Some banks prevent their mobile app from being downloaded from app stores if the user is located in a different country. This has the effect of preventing those users from using open banking.

We think it would be unreasonable for the regulation to dictate each bank's authentication processes, because these processes should be able to adapt to evolving security threats and technology developments.

However we recommend requiring equivalency with authentication options, which would ensure that a user has the same ease of authenticating in an open banking connection flow as they do when accessing their bank's electronic facilities.

Notifications

We're aware of some bank authentication processes which do not provide an obvious screen or notification regarding the open banking consent request after the customer has authenticated.

This behaviour decreases customer uptake, because the customer can get lost and abandon the connection flow.

We recommend requiring immediate redirects to the consent request or obvious notifications so that the customer does not have to navigate through a bank's electronic facility in order to locate the open banking consent request.

Disclosures with payment consent flows

The API Centre standards require that the maximum payment amount (per specified period) must be prominently disclosed to the user at the time of setting up an enduring payment consent.

This means that when an accredited requestor is requesting an enduring payment consent for variable amounts, for example an energy retailer where the amount will vary month-to-month, or an investment platform where the user will fund their account with different amounts over time, the accredited requestor will need to disclose a high limit in the consent to allow for this variability.

We expect that this prominent disclosure will be confronting for a user when they see a high number on the open banking consent, and that this will reduce uptake of open banking payments.

With competing payment methods like cards and direct debit, there are no equivalent disclosure requirements. There is no evidence of customer harm from the lack of these disclosure requirements with these other payment methods.

We recommend that the requirements for an enduring payment consent are modified in two ways:

- Change to disclosure requirements: The maximum payment amount and specified period should not be disclosed on the consent screen that is presented by the accredited requestor and the bank during an open banking connection flow; and
- Unlimited amount and frequency: Giving accredited requestors the flexibility to request, when relevant, an enduring payment consent that is not limited to a specific amount

for a specified period. Akahu has supported this option for the last 4.5 years without any evidence of customer harm.

These modifications would enable open banking payments to function effectively for a broader range of use cases, and to compete on a level playing field with other payment options.

Liability

We support the approach to rely on general law where possible, rather than creating specific rules that apply to data sharing and payment initiation via the regulated regime.

We acknowledge that many data holders, accredited requestors, customers, and other stakeholders would like clarity around how liability allocation works in the regime.

Our expectation is that liability will follow cause, meaning that data holders and accredited requestors are responsible for accurately processing requests and responses, and for complying with relevant obligations of the regime. If a direct participant inaccurately processes requests or responses or does not comply with a relevant obligation of the regime in a way that causes loss, we expect that direct participant to be liable for such loss to the extent it was caused by that participant.

If this is the intended approach to liability allocation, we recommend considering how to communicate these principles to stakeholders.

There is one specific liability point that we think is worth clarifying. An important attribute of open banking payments is the ability to report a terminal payment status within seconds, meaning that the counterparty can rely on that status in order to release goods or services to the customer. We think the regulations should clarify that accredited requestors can rely on payment statuses provided by data holders.

Quality of regulated open banking APIs

The draft regulations specify designated data and actions, but we note that there are no obligations in relation to the quality of regulated open banking APIs.

We consider that the quality of regulated APIs will be a critical enabler of customer uptake, because accredited requestors will wait until the regulated APIs are working as expected before releasing products or features that rely on those APIs.

Our specific quality-related comments are below.

Rate limiting

As an intermediary, Akahu provides an API service that is similar to the API service provided by data holders. Our rate limiting policy is documented here. The key points are:

- Account information: We don't impose a rate limit on requests to our account information API endpoints.
- Payment initiation: We impose a rate limit of 200 requests per user per minute to our payment initiation API endpoint. (A "user" is equivalent to a specific bank customer, rather than a third party service.)

In our experience, some use cases require high frequency refreshing of account information and payment initiation, while other use cases work fine with low frequencies.

We think that the regulations should impose a reasonableness requirement on accredited requestors, so that an accredited requestor must have a reasonable justification for the volume of API requests on a per-customer basis.

This type of obligation would strike an appropriate balance between reducing unnecessary load on data holder APIs, while supporting innovation and competition by enabling use cases that require a high volume of API requests in order to work well.

API performance

There are existing non-binding performance requirements that form part of the API Centre's implementation plan, and performance requirements that are specified in the API Centre's draft performance standard.

These performance metrics are inadequate. For example, the availability requirements would be unacceptable in any enterprise contract, there are no requirements regarding payment processing times, and there are no requirements regarding accurate processing of requests.

We recommend that MBIE develops performance requirements, rather than leaving this to industry to arrange itself due to the inherent conflicts of interest.

API performance

Non-conformance with API standards is an issue that has significantly slowed customer uptake of regulated open banking regimes in other countries.

We think that the regulations should clearly describe the consequences of non-conformance, and that MBIE should be well-resourced to investigate and enforce any non-conformance that emerges in the regulated regime.

We think it's critical that this responsibility sits with the government, rather than the industry. And we think it's critical that non-performance is managed immediately in order to avoid the regulated system getting a poor reputation, and to encourage fast customer uptake.

Confirmation of payee

In our experience, confirmation of payee results are not displayed to the customer during an open banking payment consent flow. This makes each open banking payment more susceptible to fraud and less appealing to customers than initiating the payment in a bank's electronic facilities.

We think the regulations should require that, when a customer is authorising a single-payee payment consent with their bank, the bank must display the confirmation of payee match result.