Akahu submissions

Open banking regulations and standards under the Customer and Product Data Bill

10 October 2024

Responses to questions

The Consumer Policy team welcomes your feedback on as many sections as you wish to respond to, please note you do not need to answer every question.

Status quo and problem definition	
1.	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?
	We agree with the issues that MBIE has described in section 2 of the discussion paper. We estimate that well over 1 million customers use unregulated forms of open banking in New Zealand each year, enabled by services like Illion, Credit Sense, POLi, Windcave, Yodlee, and Akahu. This existing unregulated open banking activity demonstrates customer demand for open banking (even despite the current unregulated nature of the dominant connectivity methods). Accordingly, this existing activity provides a clear benchmark on which to measure successful customer adoption of purpose-built APIs through the voluntary delivery by banks. When we refer to "purpose-built APIs", we mean APIs that are developed specifically for third party consumption, either on a voluntary basis or to comply with regulatory requirements. Akahu would strongly prefer to use purpose-built APIs if they offer a viable alternative to our current connectivity methods. However due to a combination of the limited functionality of the APIs that have been delivered, and the terms that are being offered to access those APIs, and in one case the refusal of a bank to provide access to its purpose-built APIs, the purpose-built APIs that have been delivered so far have not provided a viable alternative for any of the 56 third party services that are accredited to use Akahu's API in production environments. It is clearly evident that designation is required in order to develop a thriving open banking ecosystem in New Zealand.
2.	Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?
	We agree with MBIE's view that the risk of continued suboptimal development and uptake are high. There are many issues that have emerged from the bank-led work that will be difficult to resolve adequately without regulatory intervention. For example: 1. **Payee restrictions**: Some banks are applying restrictions to open banking payments that are not applied to payments that are made in bank-owned channels. For example, a customer of Bank A may be able to pay Merchant X in Bank A's web app or mobile app. But that same customer is unable to pay Merchant X via Bank A's open banking API. These restrictions are anti-competitive because they prevent third party services from competing on an even playing field.

2. **Payments from multi-signatory accounts**: The API Centre standards do not currently support payment initiation for multi-signatory accounts. This prevents many businesses and charities from using open banking payments, which prevents the APIs from being viable for some use cases.
3. **Data sharing from joint and multi-signatory accounts**: The API Centre standards currently allow banks to apply an "equivalency principle" to determine how a data sharing authorisation is granted for joint and multi-signatory accounts. This approach was agreed over two years ago, but third party services are still waiting for one of the major banks to confirm how it will apply the equivalency principle. If that bank does not enable a single customer to grant a data sharing authorisation (as was expected when the equivalency principle was agreed), there are no standards to support the granting of an authorisation from this type of account. This would mean that the new APIs will not work for many types of accounts, which would prevent the APIs from being viable for some use cases.
4. **Account type coverage**: We understand that banks have different interpretations of the types of accounts that are required to be supported through the existing implementation plan. We're aware of some use cases that will not be possible to support through the new APIs due to limitations on the types of accounts that banks intend to support.
5. **Confirmation of payee**: We understand the banks are intending to deploy a confirmation of payee system in New Zealand before the end of 2024. This system will need to be interoperable with open banking payments. Despite repeated requests, the banks have not shared details on how the confirmation of payee system will work, meaning that third party services do not know whether there will be breaking changes for open banking payments when the confirmation of payee system is deployed.
6. **Payment limits**: Banks impose different limits on the value of a payment that can be initiated via open banking APIs, and some banks impose a low limit. Open banking payments typically incur a small fixed fee, rather than a percentage fee, making them well suited to higher value payments. The average value of an open banking payment initiated via Akahu during September 2024 was $2,028.05. If one or more banks have low payment limits, then a product like automated payroll payments or automated tax payments will not be viable. In our experience, the bank-imposed open banking payment limits can be significantly lower than payment limits for other bank channels, which is anti-competitive and limits the viability of open banking payments.
7. **Bundled authorisations**: 46% of the customers that have an active ongoing authorisation via Akahu have granted access to both payment initiation and account information. These authorisations were granted through a bundled authorisation flow. In contrast, the API Centre standards currently require separate authorisation flows for payment initiation and account information. Duplicating the authorisation

	process creates unnecessary friction for customers, and will decrease adoption. 8. **Authentication options**: Two large banks decided not to deliver browser-based authentication as part of the 30 May 2024 deliverables in the API Centre's implementation plan. If authentication options are restricted, customer uptake will decrease. 9. **Data holder authentication and authorisation experience**: There are no requirements in the standards regarding customer experience. Based on the bank authentication and authorisation flows that we have observed, we are concerned that they are visually unappealing and overly complex for customers of some banks. This will decrease adoption. 10. **Conformance and performance**: Banks are not bound by meaningful commitments in relation to the conformance and performance of their APIs. For example the current implementation plan has a non-binding target API availability of 99.5%-99.9%, which is far too low for a payment service and would not be acceptable for a bank's own channels. This constrains competition and innovation because third party services may be unable to compete on a level playing field. 11. **Fees**: We are contractually restricted from sharing specific information about fees, but can state that some banks are charging fees that are not viable for many of the existing use cases in market. These fees would prevent customers from accessing the benefits of purpose-built APIs. 12. **Bilateral agreements:** A third party service currently needs to execute a bilateral agreement with each bank in order to access purpose-built APIs. Third party services have very little negotiating power, particularly if the proposed service is competitive with a bank's services, and therefore the incentive for the bank is to block access. Even if the API Centre's work to centralise some of the accreditation process was successful, third party services would still need to execute a bilateral agreement with each bank to govern fees and potentially other matters, leaving banks with control over which third parties and use cases are feasible. We think it's critical for these types of issues to be addressed in order to enable existing unregulated open banking activity to migrate to purpose-built APIs. We think that regulatory intervention is clearly necessary to resolve issues that remain unresolved through the bank-led work.
3.	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
	We broadly support the objectives that MBIE has described in the discussion paper. We have the following specific comments. **Inefficient investments** The discussion paper proposes that a designation should not require inefficient investments.

	We believe that the issues raised by banks regarding the costs of delivering purpose-built APIs are overstated. For example, to try and accelerate the delivery of purpose-built APIs, we have been offering to build and maintain purpose-built APIs for banks that are compliant with the API Centre standards for $10,000 per month. We think that the cost of delivering purpose-built APIs will be clearly justified if the existing unregulated open banking activity is able to migrate across to the purpose-built APIs. So the onus should be on banks to deliver APIs that provide a viable alternative to current connectivity methods. Further, we think that consumer data rights are fundamental. The proposed purpose-built APIs should be considered part of the social contract of being a bank, rather than seen as a standalone investment that needs to be justified on its own terms.
4.	Do you have any comments on the criteria that should be used to assess designation options?
	We broadly support the criteria that MBIE has described in the discussion paper. We have the following specific comments. **Privacy and security** The discussion paper proposes a criteria of providing customer trust and confidence in information privacy and security. The Bill is focussed on data *sharing*, and largely relies on the Privacy Act for data *protection*. We strongly support this approach. It simplifies participation in the CDR regime and will significantly help to increase adoption, because data collected via CDR can be treated in largely the same way as data collected through other methods. We strongly encourage reliance on the Privacy Act for data protection in the proposed regulations.
The Scope of an open banking designation	
5.	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?
	We note that the timeframes in the implementation plan were arranged by asking the relevant banks to nominate their preferred dates for delivery against the proposed requirements. So the timeframes have come from the banks themselves, rather than being influenced by customer or third party preferences. However if we ignore the slow industry-led progress over the previous 7 years, and solely consider the timeframes going forward, we are supportive of the proposed dates.
6.	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?

A mixture of connectivity methods will co-exist

We expect that CDR will offer the most compelling open banking environment for third parties services over time, and that existing open banking activity will migrate to the CDR regime once it is established and mature enough to handle each existing use case.

In the meantime, existing unregulated connectivity methods will co-exist alongside purpose-built APIs that come online. These existing methods will be required to support connectivity with banks that haven't delivered purpose-built APIs, and where purpose-built APIs are not yet viable for a particular use case.

We think that MBIE's commentary in paragraphs 11-15 of the discussion paper applies equally to deposit takers outside of the largest 5 banks. The only difference is that those deposit takers have fewer customers. We support designation of a broader range of deposit takers so that their customers can enjoy the benefits of the CDR regime.

Encouraging migration to CDR

As the open banking ecosystem first developed in the UK, open banking regulation gave certainty to third party services in two ways. First, by setting API delivery dates for banks. And second, by requiring each bank to support alternative connectivity methods if that bank's purpose-built API was unavailable or insufficient[1].

We suggest the following similar rules for New Zealand:

1. **Accredited requestors**: An accredited requestor must migrate to a bank's purpose-built API within a reasonable timeframe once that purpose-built API is proven to be viable for the relevant use case.
2. **Banks**: Until a purpose-built API is proven to be viable for a given use case, a bank must not block competition and innovation by restricting other connectivity methods for an accredited requestor.

We think that these rules would create good incentives for stakeholders:

- Third party services would be incentivised to become accredited requestors in order to have regulatory cover for existing unregulated open banking activity.
- Banks would be incentivised to deliver functional and performant APIs in order to be in a position to set sunset dates for use cases that can migrate away from unregulated methods. This incentive would apply equally to banks that fall outside of the proposed designation, and therefore may encourage voluntary participation.
- Third party services would be incentivised to migrate to purpose-built APIs as they become viable for each use case, otherwise they risk their existing activities being blocked.

[1] The UK implementation of PSD2 acknowledged that fallback methods are necessary until purpose-built APIs are proven to be effective. These fallback methods have been important in the UK due to poor performance of purpose-built APIs. Paragraphs 17.85 to 17.97 of this FCA guidance contains some requirements that could be considered in New Zealand.

	We think it's critical to retain this market-based pressure in order to promote competition and innovation, to continue informing future versions of API standards, and to benchmark the capabilities of purpose-built APIs that are delivered pursuant to the CDR regime.
7.	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?
	We expect that intermediaries will adequately address demand from customers that want direct access. For example Akahu provides "personal apps" free of charge to customers that want API access to their own accounts. We expect to continue providing customers with this type of direct access (provided that the costs of doing so via the CDR regime are not prohibitive). We think it's useful to retain the flexibility to include direct access in a designation, but we think that power should be used carefully to avoid delaying the rollout of higher priority functionality.
8.	Do you have any comments on the customer data to be designated?
	Account type coverage We understand that banks have different interpretations of the types of accounts that are required to be supported through the existing implementation plan. We're aware of some use cases that will not be possible to support through the new APIs due to limitations on the types of accounts that banks intend to support. We recommend that the designation aligns with MBIE's commentary in paragraph 55, which relates to data that customers already have access to through internet banking. This "equivalency" approach will enable third party services to compete on an even playing field. **Authentication** Two large banks decided not to deliver browser-based authentication as part of the 30 May 2024 deliverables in the API Centre's implementation plan. If authentication options are restricted, it will negatively affect customer uptake of the CDR regime. We think that the designation should impose authentication requirements. Similar to above, we recommend an "equivalency" approach so that banks have the flexibility to update their authentication methods over time, but they must be prohibited from making the open banking channel a more frictionful or degraded experience compared with their online banking channel. That will enable third party services to compete on an even playing field.
9.	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?

	We support the proposals regarding customer data. We think it's useful to retain the flexibility to include product data in a designation, but we recommend focussing on customer data until the majority of existing unregulated open banking activity has migrated to the CDR regime.
10.	Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?
	We consider it critical that payment initiation is included in the designation. Around half of the consumers that currently use Akahu have included payment initiation authorisation. It's important that these use cases are able to migrate to the CDR regime. We recommend including the flexibility to require other types of action initiation in the designation, but focussing on payment initiation until the majority of existing unregulated open banking activity has migrated to the CDR regime.
The benefits, costs and risks of an open banking designation	
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?
	We agree with MBIE's assessment of how the designation will affect the interests of customers. **Scale and timeframes for benefits** While we agree that the scale of benefits and the timeframe over which they are delivered are uncertain, we think that existing unregulated open banking activity provides a clear baseline for the numbers of customers that should benefit from the CDR regime. We discuss this baseline in more detail in our response to question 1. **Specific aspects that are needed to maximise the benefits** The discussion paper requests comments on the "specific aspects of the open banking designation, regulations, and standards that are needed to maximise these benefits." As discussed above, we think that the largest opportunity by far is to migrate existing unregulated open banking activity across to the CDR regime. CDR provides two key advantages for third party services in comparison to existing unregulated connectivity methods. The first is that the customer will authenticate with their bank directly, rather than entering their login credentials into a third party screen. The second is that the scope of authorisation that is granted by the customer will be technically restricted by the bank, meaning that it will not be possible for a third party to access data or initiate payments that are outside the scope of the authorisation.

These two advantages are important, and they make the CDR regime immediately more appealing than unregulated forms of open banking. But these advantages are not enough by themselves. There are a range of prerequisites that need to be met before a third party service can migrate from unregulated methods across to CDR:

1. **Functionality**: A portion of the existing use cases in market use open banking functionality that is not yet supported in any version of the API Centre standards, let alone in the versions of the APIs that banks have committed to delivering through the existing implementation plan. These use cases will be unable to migrate until the standards and APIs catch up.
2. **Performance**: Unregulated open banking methods are typically interfacing with the APIs that power the web and mobile apps of the banks. Given that these APIs are powering a bank's own products, they are highly performant. The CDR regime should ensure "equivalency" in performance between a bank's internal APIs and the regulated APIs that are made available to third party services. That will ensure that third party services have an even playing field to compete and innovate.
3. **Data quality**: In the UK and Australia, there have been material issues with the quality of data provided via regulated APIs. For example, here is commentary from PocketSmith after switching from unregulated forms of open banking to the CDR regime in Australia. If the data quality is poor, it will not be feasible for third party services to migrate to the CDR regime.
4. **Ability to support an entire use case**: The purpose-built APIs need to support an entire use case (rather than parts of a use case) before it makes sense for a third party service to migrate to CDR. For example if a third party service requires access to both identity information and PDF bank statements to support its use case, but PDF statements are not supported via CDR, then the customer would have to use both an unregulated method and a regulated method to use the third party service. In that scenario there would be no customer benefit to using the CDR regime.
5. **Costs**: The levies, fees, liability allocation, accreditation process, and other costs like insurance must be feasible to encourage third party adoption of CDR.

In our response to question 6, we propose an approach to incentivise this migration of unregulated open banking activity to the CDR regime once the purpose-built APIs offer a viable alternative. We strongly encourage a rollout that enables and encourages this migration in order to support the CDR regime.

For businesses

18 of our accredited app customers offer services that are designed specifically for business consumers. These include payroll services, accounting and tax services, and other SaaS products that harness unregulated forms of open banking.

	We consider that businesses are amongst those with the most to benefit from open banking, and we think it's critical that business use cases are supported in the CDR regime.
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.
	We agree with MBIE's assessment.
13.	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
	We strongly agree with MBIE's commentary in this section. In particular, centralised accreditation will give third party services certainty of access to the purpose-built APIs, as opposed to the current bilateral relationships which can be terminated or modified by each bank in its sole discretion with little or no notice period.
14.	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?
	We agree with MBIE's assessment. We note an additional benefit of purpose-built APIs, which is that the scope of authorisation that is granted by the customer will be technically restricted by the bank, meaning that it will not be possible for a third party to access data or initiate payments that are outside the scope of the authorisation.
15.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	We agree with MBIE's assessment.
Accreditation criteria – what specific criteria should business need to meet before they can become accredited to make requests on behalf of consumers?	
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?
	Open banking and intermediaries In our observation of countries like the UK, Australia, and the US, the vast majority of open banking traffic is facilitated by intermediaries.

	Using an intermediary enables a third party service to outsource the "infrastructure layer", and focus instead on delivering value to customers at the "experience layer". Akahu operates exclusively in the New Zealand market. We process over one million API calls each day in relation to customer data and payment initiation requests. We currently provide open banking API services to 56 Government, corporate, and fintech organisations (including MBIE, which uses Akahu to support identity verification processes within Business Connect). These organisations have all been accredited against our security and consumer protection requirements to use Akahu's open banking API services in production environments with New Zealand customers. We also provide API services to more than 300 "personal apps", which are used by individuals or businesses that access our open banking API for programmatic connectivity with their own bank accounts. For an intermediary to justify its role, we consider that the intermediary must be both better and cheaper than the third party service choosing to participate directly in the CDR regime: • **Better**: An intermediary will have specialists with deep experience at integrating with bank systems, working with the raw data, and delivering a highly performant API. Even if purpose-built APIs are "standardised", there are always issues and edge cases that need to be worked around, and a dedicated team can address those matters. In addition to connectivity, an intermediary will often provide ancillary services such as transaction enrichment that make it much simpler for a third party service to use purpose-built APIs. • **Cheaper**: An intermediary is able to spread its fixed costs across all third party services that it works with. Using an intermediary should be significantly cheaper than a third party service hiring its own team to build and maintain a web of open banking integrations. **Intention to use the CDR regime** Akahu intends to be a major user of the CDR regime. We think that the Bill has been largely well designed. And we're pleased to see that MBIE has given significant thought to making the CDR regime workable for intermediaries. In section 5 of our submission on the Bill (pages 10 to 13) we made suggestions that we consider critical to our ability to migrate existing unregulated open banking activity to the CDR regime. We would welcome the opportunity to discuss these matters in more detail with MBIE.
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?
	We support this proposal.

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?
	We generally support this proposal for efficiency purposes. However we note that many licensed entities such as banks have been subject to enforcement action in recent years for relevant conduct, such as making false and misleading representations to customers, and for poor management of data systems that have led to overcharging customers. If licensed entities such as banks are being given automatic approval for the "fit and proper test" despite these track records, then we question whether the test will be proportionate.
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?
	We agree with MBIE's assessment.
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 our experience, cyber and professional indemnity insurance has been difficult to obtain and expensive. We do not feel certain that we would be able to obtain similar cover from an alternative provider if our existing insurer decided to withdraw cover at some point in the future. We also consider that our existing cover is tenuous. For example if another open banking intermediary (either in New Zealand or in another country) makes a significant claim, and the insurer adjusts its risk model as a result, we think that could impact the cost or availability of our cover.
21.	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
	Relevant cover In our experience, professional indemnity cover is largely irrelevant to the risks that we manage. We consider cyber cover to be far more relevant to the risks that we manage. We support the approach of allowing an applicant to have discretion over the insurance that is relevant to meet principles-based requirements. **Flexible requirements** A prescriptive approach is likely to favour large incumbents. We support the flexible approach suggested in the discussion paper so that any requirements can respond to the commercial availability of relevant cover.

22.	Do you agree that accredited requestors in open banking should be required to be a member of a financial services disputes resolution scheme?
	We agree with this proposal.
23.	Do you consider that information security requirements should form part of accreditation?
	Options 1 and 2 are suitable We think that both option 1 and option 2 are suitable approaches. Both options would be achievable for any organisation that has adequate people and resources to be handling sensitive data.
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?
	Option 3 is well-intentioned but would cause issues We caution against any approach, like option 3, that creates materially different requirements than status quo obligations under the Privacy Act. Under option 3, we think that many organisations would be incentivised to remain outside of the CDR regime in order to avoid the costs and time involved with meeting prescriptive requirements. Further, if a third party service was required to handle CDR data in a different way to data collected through other methods, it would create significant operational complexity and costs. That would create a perverse disincentive to use the CDR regime. If there is reason to raise the level of protection for personal information in New Zealand, we think those changes should be made in the Privacy Act so that they apply regardless of the method of collecting that personal information. **Akahu's approach to accreditation** Akahu requires accreditation of a third party service before that service is approved to use Akahu's API in production environments with customers. Our accreditation requirements depend on whether the third party service is requesting one-off or ongoing connectivity from customers, and whether the third party service is requesting "read" or "write" access from customers. Our requirements include a mix of principles-based obligations (similar to the UK), and certain prescriptive requirements (similar to Australia). We would welcome the opportunity to discuss our experience with accreditation in more detail with MBIE.
25.	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?

	We support the proposals.
26.	Do you consider any additional accreditation criteria are necessary?
	No, we think that the proposed criteria are sufficient.
Fees – what restrictions should there be on fees for providing customer data or initiating payments?	
27.	What would be the impact of requests under the Bill being free, for banking?
	Centralised accreditation is critical The discussion paper includes an option where API requests are free to a certain limit, with any extra requests being handled pursuant to a bilateral agreement with each bank. We consider it critical that third party services do not require bilateral agreements with banks in order to access and use purpose-built APIs. Any system that requires bilateral agreements will make third party services dependent on the goodwill of banks. This would increase uncertainty for the third party service, decrease the ability to access capital, and decrease customer adoption because fewer third party services would use the CDR regime. **Access to customer data should be free** We think that a customer should be able to access their data for free. When a customer gives their consent to a third party service to access their data, the third party service is acting as an agent of the customer, so it should still be free. To align with the Privacy Act, a data holder should generally not be charging a customer to access their data. **Payment initiation should also be free or equivalent** Banks don't charge fees for payment initiation on most retail customer accounts. Instead, banks profit from depositor customers by paying a low (or zero) rate of interest to depositors. These customer deposits can be held in a Reserve Bank ESAS account which pays interest at the Official Cash Rate ("OCR"). So at a minimum, before taking any risk with the deposits through investing or lending them out, banks generate net interest of OCR less the rate of interest paid on deposit accounts. According to the Commerce Commission's market study, the five largest banks have a total deposit balance of $395b. The income from these deposits provides an enormous incentive to provide depositors with good payment functionality in order to continue attracting those cheap deposits.

	We think that the cost of providing open banking payment initiation must be seen in this broader context of how banks cross-subsidise the cost of payment functionality through deposit income. In order to compete and innovate, third party services need equivalency with bank-owned channels. For payments, this means: ● **Equivalency**: If a bank does not charge a customer a fee to initiate a payment from a particular account through its web or mobile channels, then the third party service should not incur a fee from that bank for initiating the same payment through an open banking API. ● **No extra fees**: If a bank does charge a customer a fee to initiate a payment from a particular account through its web or mobile channels, there should not be an extra fee charged to a third party service for initiating the same payment via an open banking API. These rules would give banks the flexibility to choose whether to charge customers for payments on each type of account. And they would ensure that third party services are not disadvantaged when providing payment services that use open banking APIs. **Promoting migration to the CDR regime** More generally, we consider it important to incentivise migration of existing unregulated open banking activity across to the CDR regime. Any fees would create a disincentive for existing activity to migrate.
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?
	We provide our comments in the response above.
The detailed rules for open banking	
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?
	We support the proposals.
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?
	Reliance on the Privacy Act wherever possible The discussion paper proposes that "customers should be required to opt in to specific uses that are not necessary to provide the service." We're unclear on how this proposal would be practically applied.

	We think that obligations in the Privacy Act should be relied upon wherever possible to inform the purpose for collection and what to tell the customer. That will ensure that any future changes to the Privacy Act are applied to data collected through the CDR regime. And it will ensure that third party services are not incentivised to collect data through other methods in order to avoid specific obligations in the CDR regime.
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?
	Using notifications for non-expiring consents In the absence of a regulatory framework for open banking, Akahu developed our own rules around ongoing consents that we enforce with third party services that use our API. These rules evolved over time, and during 2022 we landed on an approach that now gets high satisfaction from both customers and third party services. We initially imposed a 12 month maximum duration for ongoing consents. This led to a high dropoff when the consent expired, because a significant portion of customers did not quickly reconnect their accounts following expiry notifications. Customers and third party services were both frustrated by this dropoff, and it was difficult for services like accounting software and household budgeting tools to synchronise data seamlessly when accounts were reconnected. Based on customer and third party service feedback, we no longer impose a maximum duration for ongoing consents. This policy matches the concept of non-expiring consents in scenarios like direct debit and tax agent authorisations. To ensure that customers remain aware of the ongoing consents that they have granted, we send an annual notification to customers regarding their active ongoing consents. The annual notification provides customers with a 1-click option to login to my.akahu.nz, which is our tool to give customers visibility and control of their ongoing consents. We see a very small dropoff (less than 2%) in the month after an annual notification is sent to a customer, implying that the vast majority of customers want to keep their non-expiring consents active. **Non-expiring consents are important for adoption of the CDR regime** We believe that enabling non-expiring consents is important to encourage uptake of the CDR regime. For example, if a merchant such as an energy retailer is comparing direct debits which don't expire, versus a CDR consent that will expire each year, we think it's highly unlikely that the energy retailer will choose to use the CDR regime for customer payments. We believe that the Privacy Act contains the necessary countermeasures to protect customers from over-collection of data via a non-expiring consent. **Ability to override a consent with an expiry date**

	Based on our experience with customers using unregulated forms of open banking, we don't consider it important that customers have the ability to override a consent with a fixed expiry date. There are three key reasons for this: • **Privacy Act**: Under the Privacy Act, a third party service needs to have a valid purpose for collecting data. If the initial purpose is no longer relevant, for example because the customer is no longer using the service, then the third party service has a default obligation to discontinue collecting data. • **Ability to withdraw consent**: Customers have the ability to view and revoke an ongoing consent at any time. As discussed above, this is similar to ongoing direct debit or tax agent authorisations that are non-expiring by default. • **Appropriate access request**: In our experience, customers must be convinced of the value they'll receive in order to grant a third party service with access to their bank account. So the third party service is naturally incentivised to scope the access request based on the principle of least privilege. If a third party service does not have a valid purpose to request non-expiring access, we think that the natural incentive is to request one-off access or access with a fixed expiry in order to gain support from the customer.
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?
	We support the general principles, but have some specific clarifications and suggestions that we consider critical to make the CDR regime workable for intermediaries. **Third party should be able to provide consent details instead of the intermediary** The customer's primary relationship is with the third party service that is requesting access, rather than the intermediary. Accordingly, we consider it important that the third party service is able to provide the consent details to the customer, rather than requiring the intermediary to provide those details. This scenario has been addressed in the API Centre rules by enabling an intermediary to fulfil its consent obligations if a downstream service complies with the rules. We think it's important for the CDR regime to enable this type of intuitive consent flow. **"Pure" intermediaries shouldn't duplicate consent details** When Akahu is acting as an accredited requestor intermediary in the CDR regime, we intend to act as a "pure" intermediary, meaning that we will carry out the customer's instructions and facilitate access only to the specific third party service that has redirected the customer to Akahu.

	In this scenario, there is no other person that we will disclose customer data to. And therefore it would create unnecessary friction if the third party service describes the access request to the customer, and then we are required to duplicate that same information to the customer. This scenario has been addressed in the API Centre rules by enabling a "pure" intermediary to not duplicate the consent details if the intermediary is not collecting the data for a different purpose. We think it's important for the CDR regime to enable this type of intuitive consent flow. **A general point to make the CDR regime workable for intermediaries** To avoid any unintended consequences, we think it should be clear that an accredited requestor can satisfy relevant CDR obligations (for example the obligations in clauses 39 and 40 of the Bill) through fulfilment by a downstream service. In the previous draft of the Bill, this ability for an accredited requestor to delegate obligations was potentially facilitated through the "outsourced provider" provisions. Now that the outsourced provider provisions have been removed, we consider it critical that either: • New provisions are added to give accredited requestors a mechanism for satisfying relevant CDR obligations through fulfilment by a downstream service; or • There is clear guidance that the current wording in the Bill enables accredited requestors to satisfy relevant CDR obligations through fulfilment by a downstream service. We note that these recommendations align with the API Centre rules, which give an intermediary the ability to delegate relevant obligations to a downstream service (referred to as a "Permitted User" in the API Centre standards). **Consent and consent management with an intermediary** We consider it critical that consent and consent management are intuitive for customers when an intermediary is involved: • **Consent**: An intermediary should be able to refer to a relevant downstream service, instead of the intermediary, when providing details of the consent request to a bank. In this scenario, the bank should display the name of the downstream service on the consent screen. That would lead to a much more intuitive consent screen for the customer. • **Consent management**: A bank should show the name of a relevant downstream service, instead of the intermediary, in the bank's consent management dashboard. That would enable the customer to properly identify and manage each consent.
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?

We generally support the proposals, but have some specific comments.

Maximum amount

In some scenarios it may be appropriate for a maximum amount to be defined in an enduring payment consent.

However in many scenarios, the merchant needs the flexibility to charge a highly variable amount based on the customer's use of a service. In this type of scenario, the maximum amount would need to be high in order to be effective, and we think that if this field was mandatory it may scare customers from using open banking as a payment method.

We think that the maximum amount field should be optional so that open banking payments are not disadvantaged in comparison to other payment methods such as card scheme and direct debit.

Payment frequency

In some scenarios it may be appropriate for the payment frequency to be defined in an enduring payment consent.

However in many scenarios, the merchant needs the flexibility to charge on a variable frequency. In this type of scenario, we think that a mandatory payment frequency field would prevent merchants from using open banking as a payment method.

We think that payment frequency should be an optional field so that open banking payments are not disadvantaged in comparison to other payment methods such as card scheme and direct debit.

Defining the account that funds will be paid into

In some scenarios it's appropriate to define the payee account in an enduring payment consent.

However in many scenarios, the third party service needs the flexibility to initiate a payment to different accounts. For example:

- **Payroll services**: Payroll services are the largest users of Akahu's payment initiation API. These services enable a customer to automate payments from within the payroll software, instead of downloading a payment file, logging into the bank, uploading the payment file, and authorising it. The customer (an employer) will pay different employees or contractors over time, so the consent needs to be flexible to support this payment automation.
- **Bill payment services**: Some services enable a customer to view and approve bills for payment, and then the service initiates the payment on the due date. The customer will pay different suppliers over time, so the consent needs to be flexible to support this payment automation.
- **Peer to peer services**: A peer to peer payment service enables payment directly from one customer to another. This type of service will naturally require a flexible payment consent.

Some of the services offering these use cases could support similar functionality by directing all payments to a trust account, and then distributing

	to the relevant payee from that trust account. However many services find that banks will not allow them to open and use a bank account for this purpose. We recommend that the requirement to specify a payee account in the consent details is removed in order to provide flexibility to support relevant use cases. This is similar to how banks will enable a customer to appoint a "technical service provider" to initiate payments on the customer's behalf without specifying any payee accounts at the time of authorisation.
34.	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?
	Intermediaries should be able to delegate the responsibility to provide a consent dashboard Section 39(2) and (3) of the Bill describe scenarios in which an accredited requestor must enable a customer to view or end an authorisation. Intermediaries typically represent the vast majority of traffic in an open banking ecosystem. To support adoption of CDR, it's important for the regime to work smoothly for intermediaries. We strongly support the simple accreditation framework, which does not create a special tier for intermediaries. However this could lead to potential issues where an intermediary (as an accredited requestor) is required to carry out all obligations of an accredited requestor, even if certain obligations would be better delivered by a downstream service. In the context of clause 39, an intermediary should not be required to provide a dashboard to enable customers to manage ongoing authorisations. Instead, the intermediary should be responsible for the clause 39 obligations, but be allowed to delegate the fulfilment of those obligations to a downstream service. Here is a description of how Akahu currently requires a downstream service to provide these customer controls. This would have two important benefits: • **Customer understanding**: The customer's primary relationship is with the downstream service rather than the intermediary. So the customer will be expecting to manage an ongoing consent with the downstream service rather than the intermediary. • **Minimising friction for customers**: If an intermediary was required to provide functionality for customers to manage consents, the intermediary would need to collect and verify information about each customer so that it can authenticate the customer when granting subsequent access to the dashboard. This would add significant friction and would reduce uptake of the CDR regime. This friction would be avoided if the downstream service can authenticate the customer and provide functionality to manage consents. **Banks should describe the downstream service rather than the intermediary**

	As discussed above, a bank should show the name of a relevant downstream service, instead of the intermediary, in the bank's consent management dashboard. That would enable the customer to properly identify and manage each consent because each consent will be labelled as the downstream service, rather than having multiple consents all labelled with an intermediary like Akahu. In addition, we do not think that the purpose of each consent should be specified in the dashboard, because the bank will have (and will not need) access to that information in order to provide consent management functionality.
Joint customers	
35.	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?
	We support the equivalency principle in relation to joint accounts.
36.	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?
	We think it's critical that open banking payments support accounts with multiple authorisers. In our experience, these types of accounts are common with small businesses, charities, body corporate managers, and other customer segments that want to use open banking-enabled services. In order to drive customer uptake of the CDR regime, accounts with multiple authorisers should be supported.
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?
	We support the proposal.
Payment limits	
38.	How should payment limits be set?

	We think that the equivalency principle should be applied so that each bank has the flexibility to set payment limits for security purposes, but the open banking channel cannot be degraded by imposing a lower limit in comparison to the web and mobile channels of that bank.
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?
	We generally support the proposal. However the bank should be prohibited from reimbursing the customer unless it would reimburse the customer in an equivalent scenario if the payment was initiated in the web or mobile channel of the bank.
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?
	The proposed register is very simple to create and maintain. There is almost no efficiency or cost advantage to utilising the existing API Centre register. We think that the register should be maintained by MBIE: • **Centralised accreditation**: We understand that MBIE will be responsible for accrediting applicants. Therefore, it would be natural for MBIE to also manage the register of participants, otherwise there would be costs of coordination with external parties. • **Multiple designations**: Given the potential for multiple sector designations under the CDR regime, we think it's appropriate to maintain a centralised register for all CDR participants. • **Avoiding conflicts**: Given the purpose of promoting competition and innovation, we consider it inappropriate for any aspects of open banking to be managed by an organisation that is owned by the incumbent banks.
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?

	The register should enable participants to digitally verify the identity and status of a participant, and carry out any other processes required by the "security profile". This information should only be available to participants. We think that public access to information on participants should be enabled through a website similar to https://www.cdr.gov.au/find-a-provider.
42.	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?
	Yes, we think it's worth including express obligations relating to onboarding of accredited requestors in order to prevent any unfair delay. We think that an obligation to provide access within 5 business days would ensure that accredited requestors can confidently plan their workstreams and timing.
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?
	We strongly encourage reliance on the Privacy Act instead of creating additional requirements for data collected via the CDR regime. If there is reason to raise the level of protection for personal information in New Zealand, we think those changes should be made in the Privacy Act so that they apply regardless of the method of collecting that personal information. In addition, we expect that most third party services will access CDR data via an intermediary, meaning that any obligations that apply exclusively to accredited requestors will not apply to the primary service that the customer is engaging with.
Standards for open banking	
44.	Do you agree with the proposed standards? Should any additional standards be prescribed?
	We support the proposal.
45.	When should version 3.0 of the API Centre standards become mandatory?
	We think that version 3.0 should become mandatory on 30 May 2026.

46.	If product data were included in the designation, what standards should be adopted or developed for product data?
	We recommend delaying the development of standards for product data until the majority of existing unregulated open banking activity has been able to migrate to the CDR regime.
47.	Do you have any comments on performance standards that should apply?
	We think that open banking APIs should have equivalent performance to the APIs that serve a bank's own web and mobile channels. This will ensure that third party services do not have a degraded performance.
48.	How can MBIE most effectively monitor performance?
	We think that conformance and performance monitoring should be conducted by the regulator. This will give the regulator the ability to understand any blockers to migrating existing unregulated open banking activity, and to consider whether any enforcement action is required for non-compliance.
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?
	We're deeply concerned about delegating any aspects of open banking regulation to an organisation that is owned by the incumbent banks. In our response to question 2, we detail issues that have persisted through the bank-led work on open banking. These issues would have been resolved long ago if a regulator was setting the rules instead of leaving it to the banking sector. Below we describe other reasons why delegating authority would restrict the potential of the CDR regime. **Ownership and funding** A key purpose of the CDR regime is to promote competition and innovation. Given that purpose, we think it's untenable for an organisation which is owned and funded by the incumbent banks to be responsible for the development of open banking standards. **Third party participation** Standards development requires informed engagement from banks, third party services, and other groups that have a detailed understanding of customer implications. We're concerned that this level of high quality third party engagement will be lacking in an industry body environment for the following reasons:

- **Participation**: There are 19 third parties that are listed as members of the API Centre on its website. Some of these third parties are disengaged and do not contribute to API Centre working groups. Others attend existing working groups sporadically, and may not be reliable as a source of meaningful third party participation. So the onus would be on a small number of third parties to provide consistent engagement.
- **Attrition**: Some third parties have discontinued API Centre membership for a variety of reasons, including becoming disillusioned with slow progress, and being unable to launch a viable service due to lack of delivery of APIs. Even some large third parties, such as Datacom and Equifax, have discontinued third party membership recently. Some of these third parties would provide valuable engagement, but we think it would be difficult to entice them back into API Centre membership if they have previously decided to leave.
- **Conflicts**: Some third parties, like Visa and Mastercard, have existing high value commercial relationships with banks. Despite technically being "third parties", the importance of these existing commercial relationships may affect participation in favour of bank interests in order to protect existing commercial interests.
- **Resources**: It's difficult for many third parties to justify the time involved with deep engagement in API Centre working groups.

The majority of third party services and other relevant stakeholder groups would prefer to engage directly with a Government entity that is responsible for standards development.

Bank participation

There are 6 banks that are listed as members of the API Centre on its website, after Heartland Bank and The Co-Operative Bank discontinued their membership. One of the current member banks, TSB, does not actively participate in API Centre forums.

So the banks that are actively participating are New Zealand's 4 largest banks, which the Commerce Commission has described in its market study report as a "stable oligopoly", along with Kiwibank, which has questioned the benefit of the CDR regime in its public submissions. As further described in the market study report, the large banks "put more focus on maintaining profit margins than seeking to gain market share".

The banks that would be participating in the industry working groups are naturally incentivised to maintain the status quo and slow the development of a thriving open banking ecosystem.

Natural incentives for banks

Given that incumbents benefit from the status quo, their natural incentive is to slow and restrict the ability for open banking to increase competition.

We have observed a consistent pattern of the banks wanting to stay just ahead of regulation - retaining the ability to "hold the pen" and control the rules for open banking. For example:

- The API Centre standards are largely based on the UK open banking standards. Despite this existing body of work, after more than seven

years there is still very limited delivery of APIs and ability for third party services to access those APIs. As the likelihood of regulation increased, banks reacted by agreeing to an implementation plan.

- The banks historically promoted the view that open banking regulation was unnecessary due to the industry work being facilitated by Payments NZ. This view recently softened, then flipped into support for CDR once the CDR regime became more certain.
- With Payment NZ's authorisation application to the Commerce Commission, we understand that banks would like to control the rules for accreditation instead of these rules being developed by the Government pursuant to the CDR regime. This work could have been done years ago if there was genuine desire to make it simpler for third party services to access APIs.

High quality consultation is essential for delivering public benefits

High quality consultation on standards is essential for delivering the potential benefits of the CDR regime.

Given the issues described above, we don't think that a bank-owned forum is the right environment to enable high quality consultation on the development of open banking standards.

MBIE will need a centre of excellence for CDR

Even if standards development was delegated to an industry body, MBIE would still need the in-house expertise to provide high quality oversight of the standards and other aspects of the CDR regime. This would require employees with the skills, experience, and mana to make important decisions. For example:

- Whether to approve, reject, or modify standards recommendations from a delegated body.
- Whether to extend, modify, or revoke any delegated authority.
- Whether to grant any new delegated authority.
- Whether to create or modify any standards if there is no current delegated authority.

Given the need for a centre of excellence even if standards development is delegated, we don't consider that delegation would provide a significant cost saving.

Our recommendation

MBIE should not delegate authority for developing open banking standards.

Instead, we think that MBIE should develop an internal centre of excellence for managing the CDR regime. That would avoid conflicts of interest, and ensure that standards are customer-centric and aligned with the purposes of the CDR regime.

General Comments: