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?
	Slowly. We have only recently engaged with the API Centre (in August 2024), but feedback we've gotten from other Standards Users is frustration around how long it has taken to get to this point. We think the threat of designation under the Bill is one of the things spurring "voluntary" action by banks in this space so that they can build their preferred Open Banking framework which, they hope, would be adopted by the CDR regime. We think the absence of designation under the Bill would significantly erode current incentives for banks to continue progressing their Open Banking capabilities. As a financial services startup, our view is that the current barriers to entry for third parties to engage in the Open Banking ecosystem are far too high. Just to find out what price API Providers (banks) are charging for access a Third Party would have to: • Join the API Centre • Contact API Providers (banks) and indicate an interest in negotiating bilateral agreements • Complete security and due diligence checks by the bank • Finally get to the point where most banks will discuss their API pricing (which may vary significantly in both pricing model and cost from other providers) This is a huge barrier for small companies and startups and makes it nearly impossible to determine the commercial viability of new product offerings without significant upfront investment. This means that many prospective Third Parties are simply not interested in engaging with the current Open Banking framework. We believe that, in the absence of designation under the Bill, the uptake of Third Parties utilising Open Banking APIs would slowly increase, but that we'd be building a walled garden that would inhibit growth and lock many new entrants out of the market.
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 think the problem definition is fairly accurate. The only additions we would suggest are: * The risks associated with only implementing Open Banking among the largest 5 banks * A lack of transparency around the cost to access these APIs. This lack of transparency can be viewed from two perspectives:

	1) Consumers should have a right to know the costs associated with their bank accounts. Banks are required to disclose any fees related to the account, surely they should be required to disclose any fees charged for a consumer to access their account information via API? 2) As a Third Party looking to develop a useful product on top of these APIs, it is crucial to know what the cost to access will be. This would allow prospective Third Parties to have a good understanding of the costs which allows them to quickly determine if their idea is commercially viable. This early understanding of commercial viability is pretty critical for any business, but especially small businesses and startups, and greatly impacts their ability to raise capital. How significant are the risks of suboptimal development and uptake under the status quo? Pretty significant. New Zealand is well known to have one of the least competitive banking sectors in the developed world and we don't think the progress we're seeing under the status quo will have any meaningful impact on that. ComCom has really leant on the promise of Open Banking as a means of increasing competitiveness in the banking sector, but the status quo would likely shift New Zealand in the opposite direction. If only the largest 4-5 banks have Open Banking capabilities that enable novel products from Third Parties, that would seem to incentivise consumers to move away from smaller banks without Open Banking API capability and result in further market consolidation. Similarly, with the current barriers to entry we're likely to see more large, incumbent Third Party providers utilising Open Banking APIs and fewer small/startup providers developing new and novel solutions for consumers.
3.	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
	This discussion paper is on the money here. We want to use existing efforts as springboard rather than trying to build something new from scratch. The key here being that we want to identify which aspects of the current regime are working and which aspects aren't. We would also like to emphasise that that this needs to drive not only Third Party update, but also uptake among a much greater number of potential API Providers in New Zealand (smaller banks, credit unions, etc). Increased adoption is, of course, the goal but we also need to look around the world and be realistic as to what the adoption rates will likely be. Especially initially. Progress around areas like Open Banking is like a snowball. Uptake starts slow but as a wider array of products utilise Open Banking APIs uptake will steadily increase. With lower barriers to entry for Third Parties, we'll have a wider range of apps available to consumers and a greater likelihood that some of these apps will become increasingly popular and significantly drive adoption.
4.	Do you have any comments on the criteria that should be used to assess designation options?

	We think these designation options are good, provided the scope applies to all banks.
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?
	The timeframes are good. We think that the accelerated timeframe for Kiwibank's implementation is good. Kiwibank needs to get onto the same footing around Open Banking as the 4 largest banks as soon as possible to remain competitive.
6.	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?
	As discussed in our response to Question 2, we believe it is vitally important to have as many financial institutions participating in Open Banking as possible. Applying the requirement to just our 5 largest institutions runs the risk of reducing the competitiveness of smaller banks and robbing the customers of those banks of their right to access their data. This would seem to be counter to the concept of a Consumer Data Right, which implies there should be an equal right of access to all consumers, regardless of their financial institution. We would strongly recommend the option in point 50, where a wider range of deposit takers is designated now. Giving them a 6 month window for designation after Kiwibank seems reasonable, with the ability for deposit takers to apply for an additional 6 months if circumstances require. There seems to be some concern that designation may be overly burdensome to new entrants. This seems unlikely for two reasons: 1) New entrants are more likely to see Open Banking as a potential competitive advantage and embrace it. 2) Most prospective new entrants are likely to have a tech focus (such as Dosh & Emerge). These companies will be utilising APIs and the underlying infrastructure required already so extending this functionality to Open Banking should evoke minimal cost.
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 think that there are some areas where requests should be limited to accredited requestors, especially around the areas of payment, changes & update to their accounts, etc. But there is also a lot of read-only data that can be made accessible direct-to-customer with fairly low risk (transaction data, etc).

	The way to encourage the creation of new products that can take advantage of Open Banking APIs is to ensure that there is a pathway for people to easily play around with these APIs and realise what they can do. Allowing individuals safe access to their own data is a great way to enable this. Risk of misuse or customer harm is low, as authentication would be required to access the API. If the API is limited to read-only, it mitigates much of the harm that can be done. And any nefarious party that can use a customer's banking credentials to access the API, would also just be able to log into their Online Banking where they could cause significantly more harm.
8.	Do you have any comments on the customer data to be designated?
	We would recommend that IRD, GST, and/or NZBN numbers be added as information identifying the customer. These are definitive identifiers that allow Third Parties to ensure that the customer they're connecting to is the customer they expect. Additionally, adding which IRD, GST, and/or NZBN numbers are associated with each account will be important. For example, if a person has access to accounts for multiple entities that bank with Bank A, it is common for Bank A to make them accessible to that person from within the same Online Banking account. So it is important for Third Parties to be able to differentiate between the many different kinds of accounts that may be tied to a person's Online Banking: * Is it a personal account? What are the GST number(s) of the account holders? * Is it a business account? What is the IRD/NZBN number of the business holding that account?
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?
	No feedback
10.	Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?
	We strongly support designating payments under the Bill. One-off payments will naturally feed into automatic payments and direct debits, which should be covered. The ability to open & close accounts would be significantly impactful in terms of allowing for greater competitiveness in the banking space as this would encourage products that could reduce the barriers for consumers to switch. The ability to apply for credit would be a good thing to designate. It would also be good to designate the ability to interact with supported card features in the same way consumers can via online banking or their bank's mobile app (lock card, set spending limits, block paywave, request new card, etc).

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 generally agree with the assessment – the benefits of Open Banking will far outweigh the costs. Allowing fintechs to provide over-the-top services with less concern about winning over bank relationships is a big one, and one that still very much exists under the current Open Banking regime. Personally, our focus is on access to real-time transaction information allowing us to help businesses have a better understanding of their financial position and obligations in real-time. Among New Zealand businesses in the current economic environment there is currently a huge issue with late filing and/or payment of GST obligations. Allowing businesses to better understand their obligations and plan for payment can have a significant positive impact on the small businesses that are the backbone of the New Zealand economy. As discussed in our response to Question 3 we believe benefits will accrue slowly at an accelerating pace over time. It will take time for banks to implement the proposed changes, Third Parties to develop products to utilise the APIs, and consumers to gain confidence in their use. We would expect a minimum 5 year horizon to seeing significant uptake (of 20%+) barring a wildly popular integration that drives adoption.
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 generally agree with the assessment – although we think the costs to banks are overstated and the potential benefits much greater than discussed. For example – banks with online banking capability and mobile apps will already have internal APIs that these use for access. Tech savvy banks looking to make the most out of their IT investments should utilise the new APIs and infrastructure they're building for Open Banking for their own online banking and mobile app access. Consolidating this capability will significantly reduce the complexity of their own internal systems while utilising standardised APIs will significantly increase the pool of companies, contractors, and potential employees who can develop further products for the bank on top of these APIs. This has the potential to be one of the largest uplifts of internal bank systems across all banks for decades. And banks get to blame the regulators for the cost when reporting to their boards. Win-Win.

13.	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
	We agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services.
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 that the designation will significantly benefit the security, privacy, and confidentiality of customer data. One of the biggest advantages is that, under the accredited requestors scheme, banks will now have a very good idea of who has what access to customer data whereas under the status quo there is very little knowledge of who has accessed what customer data via screen scraping and other techniques. Specific knowledge of the Third Parties access this data allows banks and regulators to hold those Third Parties accountable should any issues arise, whereas there is little accountability with the status quo. It is our strong recommendation that there is a requirement for Third Parties currently accessing bank data via insecure means (screen scraping, etc) be required to transition to access via secure Open Banking API over a period of time. Otherwise incumbent providers with existing systems that have little oversight may not be incentivised to seek accreditation and access to the new, secure APIs.
15.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	No, we completely agree with MBIE here.
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?
	We are very likely to seek accreditation given that we already participate in this scheme via the API Centre. The criteria in 86 seem reasonable, however there needs to be some pathway for existing API Centre Third Parties to smoothly transition to being accredited requestors in the proposed regime. We would suggest that, in order to help reduce the barriers to entry, different levels of requirement may be applied to requestors accredited to different levels of access.

	For example: there is far less risk associated with an accredited requestor that is only accredited to access account and transaction data than an accredited requestor who is utilising the payments APIs. This could be the good basis for a "tiered" approach to accredited requestors where there are lower tiers that provide accredited access to low risk information and come with lowered barriers in terms of insurance & security requirements with higher tiers being able to access increasingly sensitive or risky data/actions requiring greater barriers to accreditation. This would allow a natural pathway for new and emerging participants to utilise Open Banking APIs in their products while ensuring requestors undertaking high risk activities are more stringently vetted. While we understand an accredited intermediary ecosystem will necessarily develop we think it is best to encourage businesses to become accredited requestors themselves as this will give banks and regulators the best understanding of who is actually utilising this banking data. This significantly reduces the risk to consumers while ensuring banking data is held by a minimum number of entities.
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 agree that there needs to be a "fit and proper" person test. We would strongly recommend that this is limited to insolvency, criminal offences, and more general tests of fitness. Specific requirements around professional body memberships or experience in banking will be too onerous for most businesses and startups that have the potential to be accredited requestors and result in a significant barrier to entry. That kind of professional membership or experience in banking may have no relevance to the products being built to utilise these APIs. We believe the tests here should be more character based than experience based as the concern should be whether directors and senior managers are trustworthy. Technical fitness for a potential accredited requestor to handle the data should be assessed at the business level rather than the director/senior manager level.
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 agree that directors and senior managers already meeting a "fit and proper" test by Reserve Bank, FMA, or ComCom should be deemed to meet this requirement.
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?

	It really depends on the accredited requestor and loss potential of the APIs they're accessing/banking data they're holding. In general, we believe it would be prudent to require accredited requestors to hold insurance commensurate to their level of risk. We believe that it is important to note, however, that risk should not be fully borne by the accredited requestor. We would expect that the bank would be evaluating all API requests for fraud, misuse, and risk in the same way that it evaluates the riskiness of changes and transactions processed via online banking or their mobile app. So there needs to be a clear understanding of in what instances and actions liability falls on the accredited requestor, in what instances it falls on the bank, and in what instances it is apportioned between the two.
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 general we have found professional indemnity insurance fairly reasonable to acquire (as it is a requirement of our participation in the API Centre) and the cost has not been overly prohibitive to us as a start up (compared to other participation costs). However I think it would be important that MBIE keeps an eye on this cost to ensure that this does not become overly burdensome for new entrants. Regarding cyber insurance, our experience is that this is not a cost effective form of insurance. Cyber-related risk and mitigation is an area that changes extremely fast and currently actuaries have struggled to appropriately assess risks posed. This means that the costs of cyber insurance fluctuate quite a lot in short periods of time and claims are often disputed. We would not recommend cyber insurance as a requirement to participate as an accredited requestor.
21.	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
	We would agree that a principles-based approach is an appropriate insurance measure, *however* we would strongly recommend that some general guidelines are developed and published to allow new entrants an understanding of the likely insurance obligations required prior to their application to become accredited requestors. Many established businesses will likely already have professional indemnity insurance sufficient to cover this requirement.
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 do not agree that accredited requestors should be required to be a member of a financial services disputes resolution scheme. As it is not a requirement for accredited requestors to have financial services as their core product offering (or even any product offering) it seems clear that there

	will be situations in which the dispute between accredited requestors and customers will involve products that may not fall neatly into "financial services" and so dispute resolution via a financial services disputes resolution scheme may make little sense. In addition, the cost of participating in financial services disputes resolution schemes may be overly burdensome for new entrants and small companies as some have annual levies and costs of thousands of dollars per complaint. MBIE notes that there is a filing fee for the Disputes Tribunal, however this is between $59-$234, which is at least an order of magnitude less than the cost per complaint of some external disputes schemes. This seems like a good opportunity for MBIE to assess the riskiness of applicants and engage in a discussion with them about whether they should be required to participate in an external financial services disputes resolution scheme or not. This goes hand in hand with requirements around insurance and the "tiered" approach to accredited providers we discussed in our response to Question 16. IE lower tier accredited requestors with low risk access may have lower insurance requirements and are not required to participate in the relevant external disputes scheme. Whereas higher tier accredited requestors with higher risk access may have commensurate insurance requirements and requirements to participate in the relevant external disputes scheme.
23.	Do you consider that information security requirements should form part of accreditation?
	We think that information security requirements should be a key aspect of accreditation, as this will be necessary to provide assurance to banks and consumers that their data is being appropriately handled by accredited requestors.
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?
	We would recommend a more principle-based approach as described in Option 1 or Option 2. We would further recommend that level of information security requirement is commensurate to the level of risk associated with the banking data that the accredited provider will be accessing/actioning. We would recommend discussing recommended security requirements with other government departments that are already implementing such requirements. For example: the IRD has information security requirements for providers that access sensitive IRD information via its APIs. This would seem to be roughly equivalent to banking data in terms of sensitivity and impact and so evaluating the IRD's guidelines and their effectiveness may be a good starting place rather than re-inventing the wheel.

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?
	Yes, but we would strongly recommend that “the person” be replaced with “the applicant” in these recommendations to make it clear that it is not an individual person being evaluated but rather the organisation applying to be an accredited receiver.
26.	Do you consider any additional accreditation criteria are necessary?
	No.
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?
	We have actually gone around and asked about 50 members of the public about this, and of them 49 people expected that there would be no cost associated with accessing their data via Open Banking. The idea that there might be a charge for requests didn’t even occur to the vast majority of people. We strongly believe that fees for accessing customer data via Open Banking APIs should be the same as the fee for that same customer to access their data via online banking or their bank’s mobile app. If that access is free then Open Banking access should be free in order to allow equivalent access to accredited requestors.
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?
	If requests under the Bill were not free, then it should be charged at a flat subscription model with a single monthly fee. This fee would have to be quite low, no more than $2/month. This fee should cover **any** open banking access to a consumer’s account. IE connecting to Open Banking products via multiple accredited providers should not attract any additional fee. We would strongly recommend against fees for account information & transaction history access. For most people the term “Open Banking” means that their banking data is *freely* accessible so if there is a plan to charge then there needs to be considerable consumer education about this from both the regulator and the banks. It seems more reasonable that there might be some small fee related to payments

	actions, in which case a fixed fee that is somewhere on the order of $0.05-$0.10 per transaction may be reasonable. This fee should be at least an order of magnitude less than listed higher cost alternatives. We understand that fees can incentivise investment into banking systems, however it is difficult to see why charging fees would provide any additional incentives to banks when this investment is already a regulatory requirement. We would strongly recommend that the performance of Open Banking APIs should be equivalent to the performance of access via a bank's online banking portal or mobile app. And if this is the case, then it is unlikely fees would provide any additional performance incentives. In terms of competitive incentives, it would seem to make far more sense to allow banks to develop voluntary "premium" APIs that can allow access to value-added information and services that falls outside regulatory requirements. This would provide banks a significant incentive to go beyond the bare minimum required and provide additional APIs where there may be market demand. We understand the concern on the part of banks that a lack of charges may result in an inefficiently large number of requests being made to banks, negatively impacting their performance and requiring disproportionate resources. We would suggest that this would best be addressed by a disputes resolution process for disputes between accredited requestors and API providers (banks). This would need to be overseen by a regulator with the power to enforce outcomes as there will be a significant power differential between most accredited requestors and banks (in favour of the banks). Accredited requestors that are seen to be abusing the APIs could be warned in the first instance and other action may be taken against them (such as their accreditation being revoked). We view such a disputes process as key to the success of an Open Banking regime.
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 agree with 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?
	This is a tough one. Theoretically yes, but there are many use cases where allowing customers to opt our of specific uses of their data that are not necessary to provide the service may undermine the entire commercial model of that service provider.

	There are plenty of companies where the service is offered to the customer for free and the commercial model is to utilise that data for other commercial purposes. While we don't necessarily support this commercial model, it is a common model that is popular with consumers and would be completely undermined if consumers could opt out of that data use. In this case would that mean that this use of their data actually *is* necessary to provide the service (as that provides the funding to keep the service running)? Unclear. We think it is more realistic to encourage accredited requestors to provide the option for customer to opt out of specific uses of their data that are not necessary to provide the service where it is feasible. At the very least all accredited requestors should clearly state the specific uses of a customers data that are not necessary to provide the service when gaining consent. It is then up to the customer to make an informed decision around whether are willing to accept that use or not.
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?
	For the vast majority of ongoing use-cases having ongoing authorisations with reminders at least every 12 months seems like a good middle ground. Some use cases, like one off payments, should allow single-use consents or provide more options for consent to expire after a certain period of time. Again, this would lend itself better to a tiered approach where consents regarding low-risk data (account information, transaction history, etc) could operate with regular annual reminders rather than expiry dates and ongoing consents for higher-risk actions (payments, etc) may offer customers the option to set expiry dates (we'd recommend allowing options like 1 month, 3 months, 6 months, 1 year) where the accredited requestor can send reminders to renew the consent. The details here seems like a great area for further discussion and exploration with existing players in this space.
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?
	Mostly, it makes sense that each disclosure to an unaccredited entity would require its own consent. We do have some slight concerns around 146 around data handling by unaccredited entities (please stop using "person(s)"). Surely there should be some requirements around unaccredited entity use that exceeds the requirements in the Privacy Act? IE limitations on utilising the banking data expressly for the purposes authorised in the customer consent? Do we plan to have any information security requirements regarding how unaccredited entities treat customer banking data? We assume it would then be up to the accredited intermediary to conduct the appropriate due diligence.

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?
	Yes. We also would recommend, as discussed in our response to Question 31, that ongoing payment consents have (at least) the option of setting an expiry date as these are much higher risk than data consents. We think that authorisations should be collected through the accredited requestor if that is where the liability is retained. A good example of this are the workflows that Stripe allows for credit card payments – an "unaccredited" business simply embeds their payment workflow seamlessly into the "unaccredited" business' app or website. We would envision a similar flow for accredited requestors to collect payment consents on behalf of an unaccredited entity. We think that it is fine that an unaccredited entity instructs payments via an accredited requestor. Obviously the payment would have to meet the scope of the authorisation/consent.
34.	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?
	We agree with most of the proposals a customer dashboard for viewing and withdrawing consent, although we believe that accredited requestors should also provide a functionality for customers to request that the consent is terminated. So a customer should be able to end a consent from either end of the relationship – the bank or the accredited requestor. However, this section raises the concept of a "secondary user", which we oppose. The customer is the customer – there should be no "secondary users". Open Banking data and payments APIs should confer on a customer the same access that they have view and change data and authorise payments via their existing online banking & mobile app channels.
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 strongly agree that joint customers should be able to access account information and authorise payments based on the "equivalency principle" in accordance with the API Centre's Equivalency Principle Policy. We are not currently aware of the need for any additional exceptions.

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'll leave this one to the banks. Our preference would be the recommendation described in 158.
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?
	The entire concept of "secondary users" is an unnecessary complication. Any customer should be able to authorise data and payment consents commensurate with their Online Banking access and all customers should be treated the same from the Bill's point of view. The better question is should there be some functionality in joint and/or multi-signatory accounts to be able to view and withdraw authorisations created by other joint/signanators on those accounts. And the answer to that is "yes".
Payment limits	
38.	How should payment limits be set?
	Option C is the best option as it follows the equivalency principle. If there is an ongoing issue around limits being too low, there should be a provision to review this and potentially set minimum limits.
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?
	No, we do not agree that accredited requestors should remediate banks for unauthorised payments. Banks already have sophisticated systems in place to help determine if a requested transaction is fraudulent or not, have much greater resource devoted to this, and have much more experience in detecting fraud.

	Our position is that it is up to the bank to assess any transaction for fraud in the same way that it would for any online banking payment transaction. The bulk of this fraud detection & risk also aligns with whether the customer's authentication that authorises the payment authority (ie signing in with their online banking details) is deemed risky and again banks bear the responsibility of determining whether this authentication is genuine or fraudulent. An accredited requestor has nearly no ability to determine the relative riskiness of a customer's authentication using their online banking details whereas banks have sophisticated systems and significant knowledge of a user's prior behaviour to judge the riskiness of that authentication. Only in cases where an accredited requestor, through negligence or mishandling, requests a payment via a consent that was using a valid consent but not authorised by the customer, should they be liable to reimburse the bank. We would expect issues of this sort to be covered by the accredited receiver's professional indemnity insurance. In this instance, there may need to be some provision in terms of timeframes for the payout depending on the size of the reimbursement and whether the accredited receiver needs to wait for their insurance to provide the payout.
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?
	We believe the functionality describe here to be sufficient with the understanding that additional functionality can be added later as required.
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?
42.	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?

	No, although it would be good for the register to move towards a more streamlined and automated approach to on-boarding, we don't believe that this needs to be mandated by regulation.
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?
	Yes, we agree with the proposed content of the accredited requestor customer data policies with the understanding that accredited requestors may change and update these policies as required.
Standards for open banking	
44.	Do you agree with the proposed standards? Should any additional standards be prescribed?
	We agree with the proposed standards.
45.	When should version 3.0 of the API Centre standards become mandatory?
	The functionality for banks to notify requestors of changes to consents is critical, so this should become mandatory as soon as is practicable.
46.	If product data were included in the designation, what standards should be adopted or developed for product data?
	This should be the subject of future discussion.

47.	Do you have any comments on performance standards that should apply?
	We strongly believe that performance and uptime via Open Banking API channels should be equivalent to the performance and uptime via a bank's Online Banking and mobile app channels.
48.	How can MBIE most effectively monitor performance?
	Yes, we would recommend a similar API based performance metrics system to be instituted. We would also recommend that MBIE institutes its own API testing regime so that it can run (at any time at its discretion) tests against the live APIs to test their performance. These tests should be run regularly and taken in conjunction with bank reported statistics to determine performance.
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?
	This is clearly an issue that should be discussed in conjunction with the API Centre. As a private company it seems clear that MBIE would have no power to mandate changes to their institutional arrangements without their willing participation and consent. We think that trying to rebuild this functionality outside of the API Centre is likely untenable and would set back the Open Banking project by, at minimum, years. Therefore MBIE should seriously consider and engage the API Centre in discussions around their proposed recognition model for CPD standards management. We believe the Recognised Standards Body model would be a good fit for Open Banking / the API Centre and provides a flexible model for other designated sectors going forward. There would need to be some questions answered around funding and governance of the API Centre. Obviously there is a current perception of bank control which is a concern we believe is justified. Governance of the API Centre would need to be balanced and insulated from the undue influence of banks and other large participants. The current membership would need to be considered as it poses a large barrier to entry for small companies, startups, and those who are trying to test/develop a new product and determine its commercial viability. It is possible this could be achieved with levies but we strongly believe that the API Centre, if it becomes the Standards Body, should play a key role in determining this.
General Comments:	

The Bill should include a requirement for review. If the API Centre's Recognised Standards Body (RSB) model then review on a 5 year basis (to align with renewal of a RSB's renewal) would make the most sense.

Other issues we'd like to raise:

API Centre participation – many of the questions raised here have already been discussed within the API Centre and may be moot if the decision is made to adopt the API Centre as the Open Banking Standards Body. We would strongly recommend that this decision is made before the details are regulated as it would behove the entire ecosystem to ensure that MBIE and the API Centre do not have overlapping and/or conflicting advice in this space.

As we mentioned previously, it does not seem feasible to force the API Centre's participation and so, if we wanted to adopt the API Centre's standards, this would need to be approached in partnership with the API Centre. In order to effectively achieve this MBIE would have to seek and participate in a much closer partnership with the API Centre than it currently undertakes (to the best of our knowledge).

MBIE's role as the regulator – in the instance where the API Centre becomes the Standards Body we would need roles and responsibilities that clearly define and delineate the requirements of the Standards Body and MBIE.

For instance, we believe that the regulator should have responsibility for:
- Mandating entry, participation, and accreditation in the scheme
- Mandating scheme coverage
- Mandating, testing, and enforcing API performance and ensuring service volumes
- Mandating implementation and timeframes
- Escalated disputes resolution and enforcement action

Proposed fines – we believe the fines listed in the current Customer and Product Data Bill need to be adjusted. Specifically most fines for data holders are far too low to provide an effective disincentive (especially in the case where the data holders are large banks) whereas the fines and punishments for customers & accredited requestors (as described in Clause 43) are far too high. These should be discussed further with industry with greater input from Third Parties (we're happy to participate) and the API Centre. It would also be good to look at other jurisdictions and the files levied there, my understanding is that there have been some large fines levied against data holders that have provided strong incentives for compliance.

Thank you for receiving our feedback and we would like to continue to engage with MBIE directly to provide feedback on this with much smaller/faster feedback loops. Feel free to reach me using the contact details listed on this submission.

Thank you

We appreciate you sharing your thoughts with us. Please find all instructions for how to return this form to us on the first page.