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 do not have a view on this point.
2.	Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?
	The discussion paper suggests that the set of services in open banking has been defined based on the API Centre Minimum Open Banking Implementation Plan. However, we are not sure (and we have not seen any evidence) that these are the services that would benefit the New Zealand market the most. We believe that an evidence-based approach to open banking would require particular steps to identify and implement those services that would have the greatest impact on competition in the New Zealand market and bring the most value to New Zealanders. We think the regulator should be guided by the following questions: • What is the evidence or market research regarding the most potentially attractive use cases for consumers in open banking/finance? (For example, moving a mortgage loan to another bank might be highly attractive to Kiwi customers, and unlocking that use case could have a significant pro-competitive effect.) • How could those most attractive scenarios be realised using existing API standards? We noted three API standards: payment initiation, account information, and event notification (https://www.apicentre.paymentsnz.co.nz/standards/available-standards/). These standards limit the number of scenarios to services that analyse customer account information and initiate payments. However, given the limited uptake of these services in Australia, we think this may be insufficient to realise more impactful scenarios. • What additional standards (API and others) and/or regulations are needed to foster more competition in the market for these scenarios?
3.	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
	We do not have a view on this point.
4.	Do you have any comments on the criteria that should be used to assess designation options?

	We do not have a view on this point.
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?
	As mentioned in our response to question 2, if the business cases supported by the current API standards are unlikely to generate consumer interest, this approach may not be optimal and could discourage fintech and customer uptake. Instead, it risks reinforcing the status quo in the market, as it might direct market players' efforts toward less effective business cases. We also note that a future 'open finance' designation could offer a broader range of scenarios that may be more successful in fostering competition and innovation.
6.	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?
	We do not have a view on this point.
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 do not have a view on this point.
8.	Do you have any comments on the customer data to be designated?
	We do not have a view on this point.
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 note that product data could be crucial for comparison scenarios, especially when the details of market players' offers are not publicly available. This could occur when such offers are customised for specific groups or personalised for individual customers. In such cases, without access to the parameters of particular product arrangements, it would be impossible to make reliable comparisons between offers for customers.

10.	Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?
	We do not have a view on this point.
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 note that the document outlines only the benefits for consumers. However, we believe the Ministry should also consider potential costs. These could include the availability of products that may be phased out due to regulation, compliance costs that might be passed on to consumers through higher prices, and possible delays, such as during the adaptation period.
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 do not have a view on this point.
13.	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
	We see the potential for implementing better and more widely available data services, but we do not have the expertise to form a definitive view on this matter.
14.	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?
	The central importance of customer confidence to the success of open banking services means that **privacy and trust** must be embedded in every aspect of the Consumer Data Rights scheme. For this reason, we submitted to the Select Committee that the Customer and Product Data Bill should establish several key consumer data rights. Regardless of the statutory regulations, the designation must ensure that privacy risks are minimised by: - Limiting the sharing of customer data with third parties unless expressly authorised by the customer (see also response to Question 32 below). - Mandating the erasure of customer data when consent is withdrawn to mitigate risks such as spam, scams, or unwanted marketing. - Enforcing stricter rules around authorisation/consent (see responses to Questions

	29-31 below). The overall goal should be to minimise customer risks and concerns, which may otherwise prevent them from choosing to use alternative services. It is also essential that the designation regulations not only minimise risks for customers but also ensure appropriate responses when these risks materialise. For example, if a data holder experiences a notifiable privacy breach, the regulations should stipulate that their accreditation is suspended pending an investigation. Accreditation should only be reinstated once any necessary remedial actions, as required by the Ministry and/or the Privacy Commissioner, have been completed. In our view, serious failures in risk management—such as failing to notify a privacy breach as legally required by the Privacy Act—should generally lead to suspension and potentially the cancellation of accreditation.
15.	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
	We do not believe that the designation strikes the right balance between intellectual property rights and privacy rights. In our view, customer data should not be limited to information that customers already have access to through internet banking, bank websites, and statements. As technologies evolve, there are growing opportunities to generate derived data by combining data from various sources to make inferences and decisions about individuals. This derived data is often extracted or extrapolated from existing customer data, in combination with other data (including opinions, inferences, and possibly inaccurate information). It may include details unknown to the customer or information they would not have chosen to disclose (e.g., false opinions), as well as data used by organizations to tailor products and services to customers. We believe that excluding derived data from the scope of designation creates a loophole that will undermine customer confidence and trust. Accredited requestors and/or data holders may generate derived data that incorporates customer information, which could then be processed without the customer's consent and outside their control. It is important to note that derived data, if it pertains to an individual, is considered personal information and can have as much impact as direct customer data, potentially leading to harm for customers.
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 do not have any insights on this point.
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 any requirements that promote transparency, fairness, and skill & competence in services, as these will contribute to increasing consumer trust and improving the system as a whole.
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 do not have a view on this point.
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 do not have a view on this point.
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?
	We do not have a view on this point.
21.	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
	We do not have a view on this point.
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 have no experience with that dispute resolution scheme and are unable to provide specific insights on it. However, we would like to highlight that it is likely that market players from other countries may wish to extend their services to New Zealand, especially if these services are globally available (e.g., as internet services or mobile apps). Such players could offer alternative services and enhance competition in the New Zealand market. Therefore, the set of requirements for accredited requestors should be achievable for these market players while still ensuring robust dispute resolution processes and maintaining consumer trust.
23.	Do you consider that information security requirements should form part of accreditation?

	We believe that information security requirements should be an integral part of the accreditation process to ensure that the data of users within the accredited scheme is adequately protected. Additionally, we would like to highlight that the Privacy Act 2020 does not apply to non-personal data, meaning that customer data for entities that are not natural persons may not be fully protected under its provisions. Specifically, it is unclear whether Information Privacy Principle 5 and the privacy breach notification scheme under the Privacy Act 2020 would apply to such data. This potential gap in protection may need to be addressed through robust information security requirements.
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?
	Given that the open banking scheme cannot fully rely on the Privacy Act 2020 (see response to question 23 above) and assuming the Customer and Product Data Bill is not enhanced in this regard, we believe that the designation should establish security principles for accredited requestors to follow. We do not have a specific view on imposing particular information security standards, such as ISO 27001 (as in Australia). However, we note that such standards cannot substitute the liability imposed by the designation regulations, nor can they be used to fulfil transparency obligations (or notification obligations). These elements need to be clearly defined within the designation regulations.
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, we support this as it may enhance customer trust. We believe that the designation regulations should include minimum requirements for the complaint process.
26.	Do you consider any additional accreditation criteria are necessary?
	We do not have a view on this point.
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 also consider this aspect critical. We believe that future data holders, given their market position and the advantages of scale, are well-positioned to provide these services free of charge.
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 believe that any charges, if applied, should not be based on data holders' initial infrastructure investments, as this would unfairly burden new market entrants with the cost of recouping those investments. Additionally, the Ministry should ensure that inefficiencies in data holders' costs are not passed on to new entrants. In other words, any fees should be based on efficient, long-run incremental costs. We also note that under the Privacy Act 2020 (see s 66), private sector agencies may only impose charges for making information available or providing assistance, and all such charges must be reasonable.
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 view customer consent as a critical element in ensuring that individuals maintain control over their data and in fostering trust. We note that the consultation document uses the term "consent," where the Bill uses "authorisation." Individuals need assurance that their personal data (e.g., financial information, private life details, payments, secrets) is well-protected, and that if their choice of an accredited requestor proves to be a mistake, they can withdraw their authorisation and request the erasure of their data, including any downstream data held by secondary users or third parties. This minimises the risk of harm from the use of their data. To be valid, authorisation/consent should be: - intentional, - informed, - specific (which could be included under informed), and - free from controlling influence. For consent to be informed and specific, the authorisation request must clearly identify the customer data, the purposes for which authorisation is sought, the intended recipients of the data, and the purposes for which the data may be used under that authorisation. The requirement for consent to be intentional means that the customer must explicitly confirm their desire to participate. Authorisation should not be assumed,

	for example, as part of general terms and conditions. This also means that consent must be “opt-in.” Customers should separately agree to the use of data necessary for providing the service and to any additional uses of the data that are not essential (this also addresses question 30 below). This ensures that the customer truly agrees to those additional uses, without bundling consent into a single line that covers additional risks that the customer is unaware of. Additionally, the customer should not only be reasonably informed about the subject matter requiring authorisation but also about the authorisation process itself. Customers should be informed about the duration for which the authorisation is active and how to revoke it if they wish to do so.
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?
	We do not think that bundling additional uses of data under a single, combined consent can result in truly valid consent, minimising customers’ risks and engendering their trust in the system. This issue is addressed in more detail in the response to question 29 above.
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?
	Yes, customers should have control via a dashboard to manage who has access to their data and for how long. Ending authorisation should be as easy as granting it, which would help maintain New Zealand's adequacy with the European GDPR (see Article 7(3) of the GDPR). Given the issues customers face with "dark patterns"—deceptive practices that discourage, among others, the termination of services—it is crucial that the regulation prioritises customer trust. Furthermore, as mentioned earlier, accredited requestors should be required to erase customer data upon request when authorisation ends, unless there is a clear lawful reason for keeping the data. These measures should set the necessary standards to foster customer trust.
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 believe that approving the business model of intermediary “data aggregators,” which combine data from multiple sources, process it further, and repackage it, poses significant risks to customer trust and creates strong disincentives for customers to engage with accredited requestors. In short, it opens a Pandora’s Box. Downstream users of data may ignore the limits of customer consent and share that data with unauthorised third parties, claiming it was collected with consent. This could result in New Zealand customer banking data being sold on shady “data markets.” We do not believe that compliance with the Privacy Act 2020 will sufficiently deter

	these “data aggregators,” as it has not prevented foreign companies like ClearviewAI from collecting and using data of New Zealanders. Therefore, we propose that anyone receiving customer data (whether designated customer data or derived from it) should be required to become accredited and subject to the restrictions of the Customer and Product Data Act.
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 agree with this. We also acknowledge that payment authorisation raises distinct issues related to maintaining customer control over their funds. We believe the industry will be the best source of expertise in this area. A potential approach could involve setting limits on merchants and unaccredited parties collecting authorisations or instructing payments. Additionally, customers may want transparency on which account the funds will be drawn from.
34.	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?
	Yes, we submit that the dashboard should include an option to withdraw authorisation directly from it. Additionally, there should be a clear principle that withdrawing consent must be as easy as granting it. This would ensure that service providers do not use "dark patterns" to discourage customers from opting out.
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 agree with the "equivalency principle," provided customers are informed that other joint customers may not only access account information but also request that it be shared with third-party providers. In our view, this may require additional information to be provided to ensure customers are fully aware of new services and associated risks.
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 believe that any designation (or broader regulation) preventing customers who use multi-signature authorisation from accessing new services offered by competitors would be flawed and should be revised. While we do not have data on the prevalence of multi-signature authorisation in New Zealand, gathering this information would help assess the potential negative impact of such regulation.

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 believe that the definition of secondary users in the Bill is too broad and should be carefully narrowed by the designation. Limiting secondary users to authorised signatories on a customer's account would provide a reasonable restriction.
Payment limits	
38.	How should payment limits be set?
	We do not have a view on this point.
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 do not have a view on this point.
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?

	A publicly available register of accredited requestors could significantly enhance customer trust. In our view, this register should include not only the details of these businesses but also information useful from a customer's perspective, such as: - how to lodge a complaint, - contact details for customer support, - the type of services offered, - whether the requestor provide reimbursement for errors, - whether the requestor is insured, or - whether the requestor acts as a "data aggregator".
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 information directed towards customers, as described in the answer to question 40, above, should be publicly available.
42.	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?
	We do not have a view on this point.
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 agree with that list. We think that those policies should also list all the recipients of customer data.
Standards for open banking	
44.	Do you agree with the proposed standards? Should any additional standards be prescribed?

	We do not have a view on this point.
45.	When should version 3.0 of the API Centre standards become mandatory?
	We do not have a view on this point.
46.	If product data were included in the designation, what standards should be adopted or developed for product data?
	We do not have a view on this point.
47.	Do you have any comments on performance standards that should apply?
	We do not have a view on this point.
48.	How can MBIE most effectively monitor performance?
	We do not have a view on this point.
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 do not have a view on this point.
General Comments:	

Thank you for the opportunity to make a submission on the proposed regulations.

Privacy Foundation New Zealand supports the designation's goals of facilitating competition, enabling innovation, and promoting secure, standardised, and efficient data services. We encourage the Ministry to consider our proposals above to find the best path to foster customer trust and encourage the swift uptake of these services.

We also note that consulting on secondary regulation without the relevant statutory law (as the Customer and Product Data Bill has yet to be enacted) may lead to gaps, where the consultation cannot account for changes in the Bill. Therefore, we urge the Ministry to consult on a more finalised version of the designation regulation once the legal foundation is stable.

About the Privacy Foundation
The Privacy Foundation New Zealand Inc was established in 2016 to protect New Zealanders' privacy rights, by means of research, awareness, education, the highlighting of privacy risks in all forms of technology and practices, and through campaigning for appropriate laws and regulations. Its membership has a diverse range of professional, academic and consumer backgrounds and the Foundation regularly lends its collective expertise to comment on proposed regulation or programmes in the media or by participating in consultation processes.

This submission was prepared on behalf of the Privacy Foundation New Zealand by Dr Marcin Betkier and Maria Tenorio from the Foundation's Privacy in the Digital Economy Working Group.

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.