Regulatory Affairs
T. +64 4 474 9028 F. +64 4 4746628
E. paul_hay@bnz.co.nz
Private Bag 39806, Wellington Mail Centre, Lower Hutt, 5045

Date 18 October 2024

Ministry of Business, Innovation & Employment
Consumer Policy
Building, Resources and Markets
Ministry of Business, Innovation & Employment
PO Box 1473
Wellington 6140
Email: consumer@mbie.govt.nz

Dear Sir or Madam

Bank of New Zealand's response to MBIE's discussion paper: open banking regulations and standards under the Customer and Product Data Bill.

1. Introduction

1.1. E mihi ana a Te Pēke o Aotearoa ki te whai wāhi ki te tuku urupare ki a Hikina Whakatutuki mō te arotake i ngā open banking regulations and standards under the Customer and Product Data Bill. Kei te mōhio mātou he mea nui tēnei kaupapa whakawhiti kōrero i te whakatakototanga o te tūāpapa mō ngā rā kei te heke mai o Aotearoa, ā, hei whakarite hoki i te pūmautanga ā pūtea.

1.2. E whakapono ana a Te Pēke o Aotearoa, e tika ana kia whai pūnaha pēke a Aotearoa, he pakari, he urutau ki ngā āhuatanga o anamata, ā, he pono, he whaitake, ā, he kōkiri hoki. E mihi ana mātou ki ngā mahi a Hikina Whakatutuki i te hanga i ngā tūāpapa mō taua whāinga. E mōhio ana mātou ki te mahi tahi me te kōkiri whakamua a Hikina Whakatutuki kia whakatairanga ai i tētahi rāngai pūtea āhua tau, rerekē, kanorau, me te auaha. E hīkaka ana mātou kia mahi tahi tonu ai tatou.

~~~~~~

1.3. BNZ welcomes the opportunity to provide a response to the Ministry of Business, Innovation & Employment on the open banking regulations and standards under the Customer and Product Data Bill discussion paper. We appreciate that this is an important discussion paper as it lays the foundation for New Zealand’s future to provide financial stability.

1.4. BNZ believes that New Zealand deserves a robust and future-proofed banking system that is reliable, efficient and inclusive. We appreciate the Ministry of Business, Innovation's help in
~~~~~~

building the foundation for this. We acknowledge the collaboration and pro-active engagement from the Ministry in ensuring that this work promotes a stable, diverse, inclusive and innovative financial sector. We look forward to further collaboration with the Ministry in order to achieve these goals.

1.5. Bank of New Zealand (BNZ) has prepared this submission in response to the Ministry of Business, Innovation & Employment's Discussion Paper: Open banking regulations and standards under the Customer and Product Data Bill (discussion paper).

1.6. BNZ is highly engaged on the establishment of a Consumer Data Right (CDR) and is an industry leader in the development of APIs through Payments NZ API Centre and welcomes the opportunity to submit on this discussion paper.

1.7. We believe the key objectives of the discussion paper are:

1.7.1. Early delivery of a wide range of trusted Open Data services to many New Zealanders through many accredited service providers as soon as possible.

1.7.2. Promote competition, including supporting smaller banks, deposit takers, and Fintechs to compete with larger banks

1.7.3. Make Open Data safe for customers, and affordable and attractive for participants to become involved.

2. Key themes underlying our submission

2.1. BNZ agrees that a well-functioning CDR is a key enabler of better financial services and a growing financial technology sector.

2.2. We have responded to each of the questions in the discussion paper. However, our response is shaped by 6 key themes that we believe the regulation should focus on. These are set out below:

1. Leverage the current API Centre Standards methods and processes: BNZ agrees that the quickest, and only practical, path to delivering Open Data services is to build on the six years of experience of the API Centre and its user community. Starting with these established standards, the process of Open Data implementation will be more efficient and streamlined. Any new standards required to be operational at the target commencement date and

introduced outside of the API Centre standards are likely to delay delivery, increase costs, and reduce affordability, especially for smaller banks. This could limit the ability for smaller banks to participate, which would disadvantage their customers by not allowing them to benefit from Open Data services. In the alternative, it could undermine the competition objectives by encouraging customers to switch to the banks that can provide Open Data services.

2. Negotiate with the API Centre to use their standards and to have them perform those tasks that they are suitable to provide: BNZ recommends that the government work with the API Centre to perform the tasks for which it is already well-suited. The API Centre operates under a pay-to-use model and should continue to derive a commercial return to provide any services under the CDR framework. We support the API Centre proposed recognition model that introduces a Recognised Standards Body. We believe this mechanism could effectively facilitate the use of the Centre's expertise and provide continuity in further standards development.

3. Phased designation for banks: BNZ supports a staggered designation for all banks. However, to meet competition objectives of the CDR, BNZ submits that all banks should eventually be designated under the CPD. We believe a phased approach is best to ensure smaller banks can participate without undue burden. It is critical that the framework remains affordable for smaller institutions to allow their customers to benefit from Open Data services within a reasonable timeframe.

4. Incentivise participation with commercial returns: BNZ believes that all API providers, including smaller banks, should have a clear commercial incentive to participate actively in the Open Data environment. Without a commercial incentive to participate, some API providers may stifle innovation by doing the minimum required for legal compliance. This could lead to sub-optimal outcomes for the Open Data ecosystem and limit the potential benefits of the CDR.

5. Product data only designated once all banks can provide it: Product data is not currently standardised across the industry which means that product data needs to go through a design, development and implementation process before it could be requested via an API. We strongly recommend that product data should only be designated after all banks are capable of providing it. Enabling requests for product data from some banks before others are ready could result in customers only receiving comparisons from banks designated at the time and skew customer behaviour towards those banks.

6. Data should only go to accredited requestors: In order to protect customers and maintain trust in the system, BNZ submits that data should only be shared with accredited requestors. This will safeguard customer interests and encourage more service providers to join the programme.

3. BNZ supports the rapid implementation of the CDR and believe it is crucial that the framework is built on existing standards, supports fair competition, incentivises broad participation, and ensures a high level of customer protection. Through addressing these key areas, BNZ believes the CDR will promote a dynamic and sustainable Open Data ecosystem that benefits all participants.

Should the Ministry of Business, Innovation & Employment have any questions in relation to this submission, please contact:

Paul Hay
Āpiha Matua: Waeture me te Tūtohu (Chief Regulatory and Compliance Officer)
Bank of New Zealand

DDI: (04) 474 9028
Mobile: (021) 159 8172
Email: paul_hay@bnz.co.nz

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?

    a. BNZ is highly engaged on the establishment of a consumer data right (CDR) framework and is an industry leader in the development and use of open APIs through Payments NZ[1]. BNZ's view is that designating banking under a CDR framework as is currently proposed via the Consumer and Product Data Bill (CPD Bill), is the best way to drive open banking and alternative payment options. The reasons for this are as follows.

    b. We appreciate the Commerce Commission is trying to support the progress of industry initiatives with its recommendation to the Minister that the interbank payment system be designated under the Retail Payment System Act 2022. However, we believe that this brings with it a high risk of duplicative regulation and creating overlapping bank workstreams. That is likely to tie up expert resources and unlikely to increase the level of uptake, or the speed at which Open Data can deliver widespread benefits, in the absence of designation under the Bill. A Retail Payment Systems Act designation would be unlikely to sufficiently facilitate Open Data due to gaps in oversight and safeguards. For example:

        i. Lack of clear standards and accountability for third-party providers: without a consumer data right structure, there is no formalised framework to define what standards and accountabilities a third-party payment provider must adhere to.
        ii. Consent management and dispute resolution: while a third-party payment provider (TPP) may gain access to customer data based on explicit consent, the Retail Payment System framework does not provide a detailed mechanism for documenting or managing this consent, which is critical in resolving disputes.
        iii. Data privacy and potential misuse: payments provide data that, when aggregated, can identify a person and could be provided by the TPP to other clients. BNZ believes compliance with the Privacy Act 2020 needs to be considered (or an alternative confidentiality regime for non-personal information).

[1] BNZ has already partnered with 14 Fintechs and sees success with customer-controlled data sharing tools.

c. While, separately, the Commerce Commission has recently authorised the API Centre to develop accreditation and partnering arrangements. In our view, it would be a more productive focus for that work to generate outputs that could be adopted for the purposes of the CPD Bill. There are number of challenges with the expectation that Fintechs and banks work together under the API Centre to develop APIs and deliver to market an accreditation and partnering framework without any regulation. BNZ submits that one of the most important challenges is how is the decision will be made on whether the accreditation body has liability if their process ends up accrediting bad actors (which banks will be obliged to connect to) who then cause widespread customer harm). This has been the model to date and not all banks have been sufficiently incentivised to develop the required APIs; there are also difficulties in setting pricing without breaching competition laws.

2. Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?

a. BNZ believes that the definition of the problem needs to be clarified in order to receive quality feedback. At a high-level, we understand MBIE views the problem as being that:

i. "Disincentives and barriers to adoption of open banking are likely to continue to inhibit its efficient and widespread use";[2] and

ii. the disincentives and barriers are comprised of:

1. the market power of major banks could hinder an effective Open Data regime;[3] and

2. Open Data implementation has been slow in New Zealand compared to the EU, UK and Australia.[4]

iii. BNZ is encouraged by recent industry movement and believes these barriers are unlikely to cause concern. As noted above, the major banks are now delivering an Open Data regime under the API Centre implementation plans. New Zealand's implementation started later than the EU, UK and Australia, as an industry-initiated initiative, and has taken a similar time to each of those jurisdictions. BNZ believes the regulator ambition for New Zealand shows greater success than the overseas examples.

[2] MBIE discussion paper, page 15.
[3] Ibid, paragraph 20.
[4] Ibid, paragraph 21.

b. In this context, BNZ's views are as follows:

i. BNZ believes a sustainable consumer data right regime is required for Open Data to flourish in NZ because it adds supporting elements beyond the reach of an approach driven by industry alone.

ii. The EU, UK, and Australia had earlier implementations which saw modest uptake. BNZ encourages MBIE to take the lessons from these jurisdictions and also look further abroad to jursidictions which have seen higher uptake. BNZ is one of the major banks who have been thoroughly engaged in Open Data. Paragraph 22 omits a key point from the historical problem definition - that banks had started the future Payments Direction work on their own initiative before that work was co-opted into a government Open Data narrative. That said, we agree with much of paragraph 23 of the discussion paper and believe that, on the current approach, APIs have not achieved the optimal level of development. In our view, in addition to regulatory uncertainty around Open Data, development has been hindered by the wide range of other financial services regulations requiring compliance and technology work to be prioritised and delivered over recent years.

iii. As per our subsequent response on potential fees, we encourage MBIE away from creating commercial disincentives that inhibit Open Data uptake under the proposed regulation.

iv. The Council of Financial Regulators regulatory reform calendar demonstrates regulators are attempting to improve coordination and regulatory cross-over. The Ministry has noted a lack of commercial incentive for banks. It does appear that MBIE is not looking to solve bank lack of commercial incentive problem but to simply make delivery compulsory despite the consequences of that observed in Australia of Open Data development becoming a regulatory compliance programme rather than creating a framework to encourage substantial innovation and uptake. There is a high-risk banks build to the minimum when given insufficient time or to too broad a scope to develop in a set time period, or are not permitted to recover fees that recover development costs.

v. If the status quo continues, the is a high potential for customer-impersonation access methods to become more widely used. The risks from this unregulated deceptive customer impersonation practice is to leave customers exposed to

poor outcomes, use of data beyond their consent and few remedies to redress. Banks are not in a position to help customers caught in this, as the whole business model is to keep the bank out of the picture and unconnected to the actors conducting the actions.

3. What specific objectives should the government be trying to achieve through a banking designation?

As noted in our opening summary, we think the government's objectives are and should be:

1. Early delivery of a wide range of trusted Open Data services to many New Zealanders through many accredited service providers as soon as possible.

2. Promote competition, including supporting smaller banks, deposit takers, and Fintechs to compete with larger banks.

3. Make Open Data safe for customers, and affordable and attractive for participants to become involved.

What needs to happen to achieve these objectives?

See our points 1 to 6 in our opening summary.

4. Do you have any comments on the criteria that should be used to assess designation options?

a. BNZ broadly agrees with the criteria set out in the discussion paper at paragraph 35.

i. We believe that designation options must build on existing industry developments and momentum to encourage efficiency. There has been considerable work done in this space and leveraging current industry momentum ensures a more seamless approach and is more likely to foster greater stakeholder engagement.

ii. We strongly advocate that the criteria provide for wide uptake and valuable use cases. We draw from the experience of Australia where it was evident that a successful consumer data right implementation requires a focus on use cases. Regulation that is grounded in well-defined use cases will drive meaningful engagement. By identifying and focusing on high-value scenarios, these use cases will build trust in the system which will incentivise wide uptake, especially

by customers where it will help explain the benefits of Open Data and help them understand consent arrangements.

iii. BNZ strongly encourages the government to prioritise providing customer trust and confidence in privacy and security when assessing designation options. BNZ believes it is essential that participants feel confident in the in the security of their data and privacy protection in order for an Open Data regime to succeed. A foundation of trust is more likely to increase the uptake of Open Data. BNZ submits that the security of data must be a cornerstone of a consumer data right framework. We believe in designation options encouraging this. Strong security measures will mitigate the risk of data breaches and help build confidence in using Open Data services. Moreover, BNZ believes it is important to address the issue of business information confidentiality as existing privacy laws will not protect that data. The Privacy Act 2020 provides protections for personal information but does not extend to non-personal business data. As part of the framework, we suggest considering the implementation of additional safeguards to protect confidential information.

iv. BNZ seeks clarification on the final point of paragraph 35 on what this means and for whom? BNZ is aware that there has been, and will continue to be, substantial investment into technology systems by banks and Fintechs to enable Open Data services. We believe that a sufficient return will encourage continued investment and enable the Open Data regime to succeed. We believe that there may be a barrier to entry banks that are not designated to become involved and offer Open Data services if they are not able to earn a sufficient return through fees.

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?

a. BNZ agrees with this proposal and submits that Kiwibank should be included in the designation from June 2026. New Zealanders banking with Kiwibank should not have to wait a full year longer than customers of the other four banks before having access to Open Data-enabled services. Similarly, Fintechs should not be hamstrung by unduly narrowing the range and number of customers they can offer such services to.

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. MBIE will be aware that customers of any banks not providing Open Data-enabled services cannot benefit from an Open Data regime. That may well prompt those customers to move at least some services to designated Open Data banks, buttressing (and perhaps increasing) their market share in the relevant underlying products. That observation provides the context for this response.

   b. Benefits:

      i. Would support Fintech investments by increasing the size of addressable market for their services.
      ii. Would enable better service offerings, such as for account aggregation (as MBIE notes) and product comparisons.
      iii. Would promote competition by increasing the ability for smaller banks to compete with designated banks. This supports the Bill's goal of promoting competition via Open Data progress.
      iv. For example, if smaller banks are not participating in any regime sharing product data for comparison purposes, then their banking products would not be presented as an option for customers looking to choose a product.
      v. Would reduce unsafe screen scraping of smaller banks.

   c. Costs:

      i. Could raise security and regulatory risks, especially if smaller banks face challenges in properly funding the necessary technology work.
      ii. Potentially disproportionate compliance costs (particularly if access fees do not enable a sufficient return for data holders)

   d. Given the points above, BNZ believes the best approach would be for MBIE to signal now that a wider range of deposit takers will be designated in future, which will be based on a size threshold.

   e. BNZ does not currently have a view on where the threshold should be set. However, the earlier that MBIE can publish one, the more time the banks above the threshold would

have to prepare for their designation – and some may voluntarily participate in the Open Data system earlier.

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?

    a. BNZ supports access being limited to accredited requestors only.

    b. Further to the reasons in the paper, BNZ considers that omitting limits on who product data must be provided could result in data holders being bombarded with requests from bad actors, which they would not be able to refuse.

    c. BNZ already offers bilateral arrangements to large customers to access APIs directly. We have a commercial incentive to make this offering available to our customers and do not believe an additional legal requirement is needed for this. We do not believe personal banking customers need access to an API to obtain their data in addition to the other channels already available for this. Accordingly, in BNZ's view, direct requests by banking customers should not be designated at any time.

8. Do you have any comments on the customer data to be designated?

    a. BNZ strongly agrees with the proposal for designated account types to align with the existing API Centre standards. At this stage, BNZ believes that designated customer data should also match the data available under the API Centre standards. MBIE should not create a different list from the API Centre if its objective is an early functioning Open Data regime.

    b. In support of that, BNZ observes:

        i. Each new type of data that must be provided requires new technology development work.
        ii. The regulations should only include data elements that are ubiquitous or aligned across the industry.
        iii. Paragraph 59 is inaccurate. Information about all accounts is available to customers through multiple channels without following Privacy Act processes.

iv. Accordingly, it is not necessary, nor optimal, for an Open Data designation to include all information that is available on bank systems.

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?

   a. We do not see any value providing product data via *public* APIs. If product data is designated it should only be provided to accredited requestors.

   b. Proposed product data looks sensible, noting that there are no standard data categories in New Zealand and no relevant existing standards. This concept will be starting from scratch. Product data needs to be designated, standardised, and stored, and pathways to deliver it to the market need to be established. Setting a timeframe of 6 months to provide product data after standards have been set is not feasible and would set the regime up for failure. The timeframe should be set after the data standards are determined – it is likely to need at least a year after any standards are published – and only after a significant degree of consultation to ensure that designating product data will bring sufficient benefits. Some product data will be easier to standardise and provide than others.

   c. The product data use case can be considered problematic until all banks are onboard because the goal is to enable comparison and competition - unless the government wants the ecosystem only to offer services from designated data holders for customers to consider.

   d. Our view is that it is imperative data is transmitted via APIs and separate rails are not required to be created for direct customer requests or product data requests. All data should flow through APIs to accredited requestors.]

10. Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?

    a. We support MBIE's proposal to begin with payments initiation (using the API Centre standards) and following the UK's lead. As well as being the only action that there are currently API standards for, we consider that it is important to build consumer trust by starting with simple actions that will likely function well.

b. Once that trust has been established, if there is then an appetite to extend action initiation beyond that, we would recommend that a robust consultation process is followed to ensure the opportunities are maximised and the risks are well understood and appropriately mitigated.

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?

    a. BNZ agrees that customers would benefit from new services that may be more convenient. In that regard, it would be helpful for MBIE to provide more details of the products have been enabled in other markets where Open Data has been introduced, giving more clarity on use cases. The idea of a budgeting tool in the abstract has its merits, but the tools associated with this could be more brought to life.

    b. Competition may be hard to improve without greater participation of the wider banking sector which includes smaller banks.

    c. BNZ believes the customer control and security objectives are likely to be undermined if, as the discussion paper proposes at paragraph 146, data can be passed from accredited requestors to unaccredited persons who will not be subject to any restrictions on the use and disclosure of that data in future (except the Privacy Act requirements for personal info). Similarly, BNZ believes designation under the Bill will not give customers greater control over their banking data in general – but for data that is transferred within the Open Data construct, and only for the initial sharing of that from a data holder data to an accredited requestor.

    d. BNZ seeks clarity on the following questions: Will data being passed from an accredited requestor to unaccredited persons be counted as Open Data activities? And if so, how? If not, does this reduce the perceived success of Open Data set out in 31 (a) (b) and (c)?

    e. The Commerce Commission is currently consulting on regulating to further lower interchange fees. Our observation is that, if that proposal proceeds, it will significantly

reduce the scale of benefits to businesses from Open Data payments as fewer Fintechs and use cases will be commercially viable. The reason for this is that, to achieve widespread uptake, the fees Fintechs charge for their services (e.g. to merchants) will need to be competitive, and likely lower, than the widespread incumbent method of paying by card.

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 Data Implementation Plan.

    a. BNZ agrees with the costs and benefits that MBIE has identified. We do not believe it is possible to quantify the potential additional costs (or benefits) to banks at this stage due to the range of potential outcomes contemplated within the discussion paper. BNZ is hopeful it will be able to provide more specific information once MBIE has progressed the shape of potential regulations.

    b. BNZ submits that if the scope of designation were to exceed the scope of the Minimum Open Banking Implementation Plan, as the discussion paper countenances, it is highly likely to significantly increase the additional costs to banks. In our view that may reduce the ability for data holders to focus on the best delivery of open requirements as the available resources would have so much work to do just to ensure the minimum requirements are complied with. We understand that challenge arose in in Australia when the CDR was introduced.

    c. BNZ also highlights that costs relate not only to developing, maintaining and operating the required IT infrastructure, but also the high security standards to mitigate risks like third-party data breaches, and man-in-the-middle attacks.

13. Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?

    a. Yes. BNZ's view is that designating banking under the CDR framework as is currently proposed is the best way to drive Open Data and alternative payment options.

b. A CDR framework managed by a central regulator with guardrails that protect and guide emerging payment types is the model for access to payment networks in markets overseas. Executed well, such regulation can provide confidence and maintain the trust and integrity of the payments system at a time when financial crime is growing around the world.

14. Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?

a. BNZ broadly agrees with the comments on the benefits and risks to security, privacy, and confidentiality, subject to the following.

b. Paragraph 82(c) states that Open Data should reduce "*instances of customers providing their bank account credentials to third parties*." We are concerned that this will not occur unless this is supported by a regulatory requirement to phase out screen scraping services and until all deposit takers are involved.

c. Paragraph 83(b) - as noted in response to question 11 above, the customer control and security objectives will be undermined if, as the discussion paper proposes at paragraph 146, data can be passed from accredited requestors to unaccredited persons who will not be subject to any restrictions on the use and disclosure of that data in future (except the Privacy Act requirements for personal info).

d. The confidentiality of business data seems to have limited protections built into the proposed Open Data regime. This sits oddly with the position for personal information about consumer customers, which also benefits from Privacy Act protections. We would be interested in understanding the rationale(s) of MBIE and the Government for this difference.

e. However, we also believe that accreditation requirements must be set correctly in order for a successful regime.

15. Are there any risks from the designation to intellectual property rights in relation to customer data or product data?

a. BNZ considers that there is a risk that the designation will impact intellectual property rights if the definition of product data is not amended to expressly exclude commercially sensitive information such as affordability calculations and shaded rates.

b. We believe the definition of "data" requires clarification. While currently undefined in the draft Bill, the discussion paper suggests that customer data is intended to include "derived data" and "data derived from derived data". An example of this might be a customer's credit assessment which is data derived from a customer's income and expenses. However, providing this would mean that a bank is also providing its affordability calculation, which could harm competition between banks.

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?

a. BNZ submits there are two factors that will significantly affect the proportion of businesses that choose to become accredited requestors:

   i. If businesses can receive data through an intermediary without being accredited, then we would expect businesses seeking accreditation to be dramatically less than if data can only go to an accredited recipient.
   ii. That accredited requestors (including intermediaries) are exposed to greater liability under the Bill than data recipients who are not accredited.
   iii. BNZ believes it is a significant omission from the Bill to not have established clear boundaries as to the point at which responsibility (and liability) for data and regulated data services shall cease to sit with the data holder and move to the accredited requestors. BNZ submits it be explicit that responsibility moves with the data: data holders who have acted appropriately and transferred data to an accredited requestor (or initiated an action) cannot be held liable for anything that happens to the data after that point and accredited requestors should (explicitly) be liable from that point. We would encourage this point to be clarified in the regulations that are made under the Bill.

b. BNZ strongly advocates against it being possible for accredited requestors to transfer the data to further recipients that are not accredited. We believe this creates significant confidentiality concerns - for small businesses in particular - that will not be covered by

the Privacy Act protections. That is, whether an entity chooses to obtain regulated data directly or via an intermediary, that entity should have to be accredited.

c. However, BNZ believes this requirement need not be the same for payments. In BNZ's view, it is appropriate for intermediaries to provide payment initiation services to other entities that are not accredited.

d. BNZ agrees with paragraph 88 of the discussion paper. However, we believe that setting high security standards for accreditation need not be framed negatively as a barrier to entry; rather, it seen as a positive. BNZ believes an entity who is serious about accessing regulated data services, should be willing to meet high security standards. This ensures customer trust in the system, which will support higher customer uptake and thereby support a more successful Open Data regime.

e. Overall, BNZ believes it is difficult to assess the number of businesses without more clarity on the actual parameters of the designation (and standards – as well as some general information on the number of Fintechs who are focused on Open Data services as opposed to other services).

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?

a. Yes and no, respectively.

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?

a. BNZ is open to deeming 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 in a to be agreed reasonable timeframe have met this requirement without further assessment. However, we encourage MBIE to check whether the standards across the three regulators (and MBIE) are sufficiently consistent and aligned to the operation of an Open Data business so as

not to undermine the effectiveness of this test.

19. Do you consider that 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?

    a. Yes. BNZ believes this is exacerbated by the Bill not being specific/explicit on where liability sits as the data is transferred (see our response to question 16 above).

    b. BNZ submits that under a properly constructed liability regime, banks should face minimal risks from any breach of obligations by an accredited requestor. Banks should explicitly not be liable to their customers after delivering the outputs of a consented instruction. In particular, the law should be clear that banks are not liable for the faults (and consequent debts) of accredited requestors to whom banks are required to provide regulated data services. We encourage MBIE to clarify this point in the regulations under the Bill.

    c. BNZ believes insurance requirements be included to ensure the accredited requestor has the financial resources to respond to claims where it is found liable for negligent acts or omissions appropriate to the type of services provided and the associated risk exposures involved in performing its obligations. Although, it is difficult to quantify the harm resulting from a data breach, insurance will at least go some way towards compensating those who have been harmed as a result. Noting that insurance is only one element of a total risk management strategy. We believe that it is best that insurance covers: (1) professional indemnity; and (2) cyber and data protection.

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?

    a. Applicants for BNZ API services have often spoken of the difficulty in finding insurers for what is a new risk category that there is little experience in rating. To an extent, this challenge could be mitigated if the proposed regime was clearer on the potential liability an accredited requestor may have (on which, please see our response to question 19 above).

21. Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?

    a. Yes in principle.

    b. In particular, BNZ agrees that this has the benefit of assessing the financial resources of the applicant.

    c. It would also enable flexibility for accredited requestors which approach to financial protection works best for their business to put in place e.g. a guarantee, further capital, and/or insurance.

22. Do you agree that accredited requestors in open banking should be required to be a member of a financial services disputes resolution scheme?

    a. Yes. In addition, businesses that use accredited requestors to facilitate payments should also be required to be a member of such a scheme (or covered by the corresponding accredited requestor's membership).

    b. This should be supported by a clear complaints regime in the Bill so that consumers understand where to complain to, including who to complain to if the Bill ends up allowing unaccredited businesses to receive information from accredited requestors or use accredited requestors to facilitate payments.

23. Do you consider that information security requirements should form part of accreditation?

    a. Yes, this is critical.

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 1: a criterion that the applicant meets information privacy principle 5 (i.e. status quo obligations)

Option 2: a criterion that the applicant meets a set of high-level principles (i.e. similar to the UK)

Option 3: a more prescriptive set of information security requirements along the lines of the Australia CDR Rules, potentially with expectations of third-party certifications against specific standards (e.g. ISO 27001).

a. We support option 3, a prescriptive approach, to provide the greatest assurance that customer data is being treated safely and securely by accredited requestors. We acknowledge that this could make accreditation more costly and less flexible initially but that is outweighed by trust and confidence that it would promote in the Open Data regime. BNZ submits, it would also make it easier for MBIE to confirm whether the required standard of information security is in place.

b. Regardless of the approach MBIE takes, we believe it is imperative that MBIE actively checks an applicant's information security capability or certification and does not rely solely on information that the applicant has self-reported.

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?

a. BNZ believes this to be a useful requirement. We can comment further after MBIE clarifies how it expects an applicant to demonstrate compliance. Presumably it would include criteria such as: showing certifications held, security audit reports, penetration test results, policy documents, how data is stored and used, how payments are monitored, and so forth.

26. Do you consider any additional accreditation criteria are necessary?

a. BNZ believes that the use cases the applicant is seeking to introduce should be part of the accreditation assessment process. BNZ's view is that where an accredited requestor subsequently wishes to introduce a new use case, it should be notified to MBIE (as the accreditation authority) in advance. This would enable MBIE to confirm that the information security standards (and financial coverage level) the requestor has in place

remain appropriate for the new use case – which may be higher risk than its existing use cases.

b. BNZ submits each accredited requestor be required to undergo follow up checks periodically to retain its accreditation. This will ensure accredited requestors are appropriate Open Data counterparties under the Bill on an ongoing basis, rather than only passing one initial set of checks.

c. Regarding paragraph 117, BNZ believes it will be important that data holders are notified immediately if there could be an issue where an accredited requestor has its accreditation suspended. In addition, the regulations should consider what actions a data holder can legitimately take to reduce access in respect of an accredited requestor's the behaviour leading up to a potential suspension. What is needed here?

d. BNZ believes that the register of accredited requestors should provide an API that can be consumed by data holders – to provide for an automated, efficient, real-time method that data holders can use to confirm that a requestor is accredited.

27. What would be the impact of requests under the Bill being free, for banking?

a. BNZ submits that there would be a reduced incentive for banks to invest. As a comparison, when banks have always provided EFTPOS at no cost to merchants; this has led to no further investment in EFTPOS, such as the absence of contactless payments that are available from credit card scheme cards.

b. We agree there is a risk of an inefficiently large number of requests being made. Fintechs would have no incentive to design applications to make an optimal, rather than excessive, number of requests.

c. A decision that would see banks required to provide CPD services for free presumably becomes a principle for all future CDR sectors as opposed to something peculiar to banking.

d. A decision to not allow banks to recover costs of setting up and providing CPD is likely to compound the problems for smaller banks to participate and therefore for their customers to gain the benefits posed in the discussion paper. Similarly, any decision

which does not support all banks becoming designated, may have the flow-on effect of pushing customers to move to banks that do enable Open Data-enabled services.

e. We believe that if an authorised requestor requires free data and payments access to make their service viable, it does not bode well for the appeal of their proposition to their customers and the value that it brings to the New Zealand economy. This could also lead to further issues as their viability would also be enhanced if they did not have to pay for electricity, rates, ACC levies, and other costs.

f. Similar to the point made in paragraph 130(b) of the discussion paper, BNZ believes an effect of making requests free would be that banks are compelled to participate in activities that are not a priority for customers. Permitting access fees for regulated data services will likely steer the ecosystem's - and accredited requestors' - focus to services that are valued by customers.

g. BNZ believes that compelling banks to deliver services that are not a commercial or customer priority should not extend to preventing them covering the costs of that compulsory participation and having an economic return incentive to be involved.

h. Section 32(1)(a) of the Bill also seems to imply that requests would not be subject to a single prohibition on charging that relates to all aspects of accessing regulated data services.

i. Regarding the advantages posited at paragraph 129(a) of the discussion paper:

    i. It is likely incorrect to say that a free or low capped approach to fees would maximise use of regulated Open Data services. It assumes that the only variable relevant to a comparison is the level of fees. However, it is unlikely that a free or low capped approach would result in an environment that delivers the same range, quality, support, promotion and usage of regulated data services as an environment that permits data holders to recover at least some of their costs through fees. This point is implicit in paragraph 130 of MBIE's discussion paper.
    ii. The logic in paragraph 129(a) (as qualified in the preceding paragraph) would also apply to any fees charged by accredited requestors. However, we are not aware of any proposal to cap such fees to maximise use of accredited requestors' Open Data services.

j. We note the potential advantage stated in paragraph 129(b) of the discussion paper. BNZ submits that the better way to address screen scraping would be regulations to require it to be phased out once regulated data services are available under the CPD.

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?

a. BNZ submits fees should be set at a fair level. Banks should be able to recover a measure of their costs, while recognising that they are making a long-term investment and will not recover all costs via fees in the short term. We believe this is integral for a sustainable Open Data regime.

b. BNZ strongly believes that the appropriate place to regulate fees for regulated data services is under the CPD regulations. We do not support just one of those fees, for payments services, being regulated separately under the Retail Payment System Act (if the interbank payment network were to be designated under that Act). We submit that regulating fees under the CPD regulations is the best way to ensure pricing remains appealing for competitors to card products.

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?

a. BNZ believes the definition of express and informed consent needs to be further clarified. This definition needs to be customer-centric as opposed to a tick-box exercise.

b. BNZ submits that this needs guidance to ensure that accredited requestors are meeting the spirit of express and informed consent when this is operationalised and conveyed to customers.

c. BNZ broadly agrees with the points made in sub-paragraphs 137(a) and (b), however we are concerned about sub-paragraph (c) and paragraph 138. We believe in the principle of data minimisation, which provides that data collection should be the minimum amount necessary to obtain the service.[5] We submit that the point in paragraph 137(c) goes against this principle because it enables data to be obtained that is not necessary

[5] Office of the Privacy Commissioner | Principle 1 - Purpose for collection of personal information

to provide the service. This could harm customer trust in the system, which is of paramount importance. We do not support accredited requestors being able to bundle both necessary and non-necessary uses of data into a single consent request (even with an opt-in option for the non-necessary uses); doing so has the potential to gain consent to uses of data that the customer may not intend or be focused on and may not be in their best interests. The proposals in these paragraphs are also contrary to submissions made for the proposed requirements of an accredited requestor's customer data policy, as stated in paragraph 180(a).

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?

    a. BNZ believes the data minimisation principle is a central tenet of Open Data. As noted in our response to question 29 above, BNZ does not believe that a bundled, opt-in / opt-out consent approach will promote trust. Instead, BNZ submits that the customer be sent a separate consent request for any other use of their data to occur and, if that consent is not granted, that use of the data must not occur. If the consent is enduring, the customer should be given the option and ability to cancel that ongoing consent.

    b. In BNZ's view, no weight should be placed on the two disadvantages put forward in paragraph 138 of the discussion paper. On 138(a), each accredited requestor's service should deliver enough value to be economic without relying on non-necessary uses of data. The appropriate consequence to 138(b) is for accredited requestors not to obtain data that it is not economic for them to handle in accordance with customer consents.

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?

    a. BNZ submits that customers should only have the ability to set an expiry on ongoing consents if this is possible under the API Centre Standards. BNZ maintains that building on the API Centre work will enable a swifter implementation. We note that customers will (and should) have the ability to end any consents that no longer suit their needs.

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?

a. BNZ agrees with intent and suggested treatment of consents that might be obtained by accredited requestors who are intermediaries. In essence the consent process for regulated data being passed on by intermediaries is the same as with direct users.

    i. The customer should clearly understand what their data is being used for and by whom and consent to that.
    ii. No more than the minimum data necessary for performing that specific service should be sought.
    iii. Any different use of that data can only happen with the express consent of the customer.
    iv. Any use of the data by another party can only happen with the express consent of the customer
    v. It should not be permissible under the regulations for the scenario in paragraph 142 of the discussion paper to occur, where the consent is too broad; the measures suggested in 143-145 address that.

b. Regarding paragraph 146:

    i. BNZ believes customer data security is paramount and submits that intermediaries should not provide data to any further recipients unless the recipient is also accredited and therefore meets the necessary security requirements.
    ii. Having no restrictions on the use and disclosure of customer data by unaccredited persons (whether designated customer data or derived customer data) would most likely lead to disastrous outcomes for customers once the data goes beyond an intermediary (or, at the least, when it goes beyond the further recipient). We strongly caution MBIE against enabling such a highly risky position in the regulations.

c. If that position were to eventuate, it would disincentivise persons from undergoing accreditation and becoming accredited requestors. The consequences of that could be that:

    i. it limits the parties that might contribute financially for the upkeep of the accreditation service; and

ii. leads to a small number of businesses becoming accredited and operating as data intermediaries, each of whom is of substantial size. Accordingly, the regulated open banking ecosystem would have a fairly narrow perimeter.

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?

a. The API Centre currently has material setting out how consents work. As MBIE intends for those standards to be used under the CPD Bill, it would seem there is no need also to address this in the regulations. Doing so would enable less flexibility, and a slower process, to update consent requirements if the best way to obtain customer consent moves on from what is in the regulations.

b. If the regulations are to include consent contents, we support those being high level requirements only, as the discussion paper suggests. The requirements in paragraph 148 do not seem to align to how open banking is currently operating. For example, where a payment services provider facilitates a payment for a merchant, to the customer it may seem from the consent that it is the merchant that will 'act on the authorisation' i.e. be paid; that is the nature of transaction the customer is intending, and the substance of what will occur, although it may in fact be the payment services provider that 'acts on the authorisation' by initiating the payment. In addition, a consent would identify the party who will be paid, but is unlikely to specify the "particular, code, reference" or 'the account that funds will be paid to'.

34. Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?

a. Broadly this looks fine. If unaccredited parties are to be able to receive data sourced or derived from regulated data services (which we oppose), BNZ supports the proposed obligations for the intermediary to ensure those parties have an equivalent consent revocation method.

b. There are two levels of consent revocation in an Open Data system:

i. revoking consent to share/request data – this can be done by cancelling consent at the data holder or the requestor, and

ii. revoking consent for a party to use a customer's data – which can only be done at the requestor (in this context). We understand it is implicit in paragraph 153 that an accredited requestor may only continue to use customer data it has already received if the customer has not revoked the consent to use it.

c. BNZ does not believe it was clear from the discussion paper how the regulations will ensure any revocation of a data use consent would be effective to prevent ongoing use of data by secondary users of customers.

d. Paragraph 152 does not appear to contemplate payments intermediaries. We would be interested in what MBIE proposes for them, noting that such an intermediary is often less visible, or not visible, to a customer making a payment to a merchant.

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?

a. The practical impact of adding exceptions would be to require new technology builds by designated banks that moves away from the idea that the existing API Centre standards will be used to speed up adoption and achievement of the benefits of Open Data. The API Centre Equivalency Principle Policy has benefited from both the extensive thought applied in preparing it and experience of operating in practice.

b. We note Australia made the treatment of joint account data unworkable.

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?

a. The default provisions look sufficient in BNZ's view.

b. The API Centre has drafted a standard for multiple-signatory one–off payments and is working its way through the complexities of creating a corresponding standard for enduring payments. When these are finalised and available, MBIE could work with API

Centre to use them for the purposes of the CPD Bill. In BNZ's view, that would be the best path for the CPD regime to follow to cater for multiple signature payments in due course. That would address the few joint accounts where two to sign is required. Given how uncommon that is, BNZ's view is that open banking under the Bill need not cater for these situations in its initial phase.

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?

    a. This should also follow the equivalency principle and is already suitably catered for in the API Centre Equivalence Principle Policy and bank practice.

    b. If a person has set up account operating authority for another – e.g. a child being given the right to assist an aged parent, or an accountant can view accounts – then they should be able under the CPD Open Data regulation to be able to make payments and share data in the same manner they can initiate other banking activities.

38. How should payment limits be set?

    a. There are so many different payment use cases that a nation-wide limit would be problematic (even if different between business customers and consumers), particularly if these are set in regulation.

    b. Banks, accredited payment initiators and customers (through an overlay service) should be able to set limits to suit the different use cases and risk levels.

    c. At present, and rightly, nothing prevents the accredited requestor setting payment limits that apply within its services. There are payment intermediaries currently that have put in place limits below the bank limits that suit their proposition.

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?

    a. For the first question - yes. However, there should be an additional, and prior, obligation that an accredited requestor reimburses the customer directly for an

unauthorised payment they have facilitated. The requestor will know which account they debited and should therefore be able to reimburse the customer directly.

b. The first obligation therefore should be for the accredited requestor to make the customer whole.

c. If the accredited requestor needs the bank to do that on their behalf (or the bank separately reimburses the customer) then the accredited requestor should make the bank whole.

40. What functionality should the register have? Is certain functionality critical on commencement of the designation, or could functionality be added later?

a. BNZ submits that the discussion paper places more emphasis on the register than we have seen it used for to date. We believe banks should be able to look up somewhere, and it may be the register, that a requestor is accredited and remains accredited.

b. In theory, a customer might want to check that a requestor is accredited but we simply do not see that happening at all.

c. It follows that, upon commencement, BNZ believes the register need not have much (if any) information beyond that required in the Bill and should not be required to have any particular functionality beyond data retrieval.

d. However, if MBIE and the API Centre were to reach suitable arrangements to facilitate the use of the API Centre's register, we believe there should be no functionality required beyond what is currently available on it plus the minimum information required by the Act. That will enable industry resources to focus on other aspects of open banking delivery. MBIE can then assess over time whether any need for additional information arises that would justify going beyond that.

e. We have the following questions arising from the proposals in the paper:

i. On what basis would the API Centre register be incorporated under the Act? Would that occur via a designation?

ii. Will the Ministry contract with the API Centre to use its services, including the standards and the register, and what would it pay for that?

iii. On what basis would the API Centre be compelled to amend its contract with its third-party supplier to add additional data categories to the register required by the Bill? Or would that be an optional commercial request?

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?

a. In line with our response to question 40, no additional information is needed.

b. The information will be of most value privately, to participants in the Open Data system. The information could be public but that would be for transparency rather than any observable public need to see the register information.

42. Is it necessary for regulations to include express obligations relating to onboarding of accredited requestors? If so, what should these obligations be?

a. In BNZ's view, it is difficult to read clause 27(a) of the Bill as requiring onboarding. The wording of the clause is focused on the capabilities that must be present in the data holder's Open Data technology system. That is evidenced by the use of the words "operate an electronic system that has the capacity" (i.e. the electronic system itself has the capacity, rather than a reference to having individuals available to assist), to "enable the data holder to receive requests for regulated data services" and provide those services (i.e. providing data or performing an action, rather than onboarding). For this to encompass onboarding would seem to require an unduly expansive reading of the word "operate".

b. Consequently, if the plan is to have additional obligations on data holders to facilitate onboarding, we would anticipate that being pursuant to a different clause of the Bill or regulations under such a clause (which we would ask to be cited specifically). However, if that were to occur, we are unclear how that would be expected to work in practice, as follows.

c. BNZ submits that we do not understand what accredited requestor software applications banks would need to onboard. In the event that MBIE believes banks should expeditiously enable the accredited requestor to connect to the bank's API end

points that it wishes to use. We submit that is a two-way process requiring skill and resources on both sides .

d. For example, if the accredited requestor lacks skills or knowledge on how to connect to APIs (which is not uncommon in our experience of this early phase of Open Data APIs being available in NZ) does MBIE anticipate banks being required to have resources available to coach them on how to do that? If so, would the requirements extend further, such that banks might also be required to bug-fix poor API coding? In this scenario BNZ submits that would:

    i. need to be pursuant to a clear section in the primary Act itself, given the nature of such an obligation; and
    ii. be remunerated on a 'time and materials' basis, and subject to appropriate advance notice being given (given the large and diverse workloads of banks' technology teams) and a maximum amount of bank resource that could be required to attend to such work at any one time.

e. In BNZ's view, data holders can be expected to provide API access keys to accredited requestors, which could usefully be clarified in regulations – and possibly to make aids available regarding API connectivity (see below). If there is an intention to impose further obligations than that, we believe that would require the above points to first be worked through and addressed in a relevant proposal.

f. There could possibly be some value in other express obligations. The regulations might oblige:

    i. accredited requestors to have or obtain suitably skilled personal to connect to Bank API end points or (subject to the points above) to pay the bank to assist them if they do not; or
    ii. banks to make aids available for parties planning to become accredited requestors, like sample code, software development kits and sandbox access to expedite connectivity.

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?

a. That seems a useful list though there is some tension between (a) *accredited requestor minimises data collection to what is necessary* and (d) *all purposes for which de-identified customer data is used, and who benefits from each purpose.*

b. The concept of (d) seems, in many cases, to be data collection and use beyond the minimum data required for the customer's need. We think (d) should be prohibited under the regulations.

44. Do you agree with the proposed standards? Should any additional standards be prescribed?

a. We are happy to use the API Centre API standards.

b. Please be aware that there is only a Minimum Open Data Implementation Plan for v2.3 and not v3.0.

c. Would it be the API Centre setting that plan and developing the standards? Or would it be the Ministry or some other body it sets up, in which case who develops the standards that will be subject to those minimum plans?

d. BNZ is fine with using the API Centre security standards.

e. In general, we are not clear on how the standard setting process under the Bill is expected to operate. For example, can more clarity be provided on which body would set standards? How involved MBIE would be in that process? Paragraph 186 does indicate the API Centre might be tasked to continue development of standards, based on needs, and of industry consultation guides. We support this in principle, although we do not currently know the arrangements that would make that possible.

45. When should version 3.0 of the API Centre standards become mandatory?

a. The industry has not yet had the conversation on the need for v3.0 APIs and thus we do not yet know the scale of the need. The two-way alerting of cancelled consents is of some use, but we do not yet know where third parties see the priority.

b. We are yet to see the need to mandate v3.0 API standards until after that conversation has been had.

c. Until any need for what v3.0 offers in addition to the prior version is confirmed as a strong need by industry we do not think it should become mandatory.

46. If product data were included in the designation, what standards should be adopted or developed for product data?

a. There are, as yet, no product standards to use or even requirements setting out what product data is required, and no bank internal mapping of that data or services to provide such data for consumption.

b. It goes without saying that there are also no standards to deliver something that neither the industry or regulation has yet even defined.

c. The fact that products are (rightly) not standardised across competing banks adds complexity to any designation of product data.

d. We question whether there is a strong enough use case to warrant developing product data APIs. If there is, then the work necessary for developing product requirements and standards, building APIs and creating service delivery looks like a multi-year development. The sequencing of that would require first agreeing what the use case is, then the data scope required to serve that, then requirements to draft into a standard, then standards drafting review and publication, then internal bank set up to make that data available, and then developing the API end points.

e. On the basis, we would suggest it is better not to designate product data at this stage.

f. Note: we anticipate that if only designated banks need to provide product data, and the use of product data is to inform customers of best available solutions to meet their needs then that will drive business to designated banks and pull it away from non-designated banks.

g. The implication of that might be to not designate product data under the CPD Act until all banks are designated and thus able to benefit from product comparison services or, alternatively, accept as an intended consequence of designating product data that designated banks will gain market share.

47. Do you have any comments on performance standards that should apply?

a. BNZ submits MBIE outsource that to the API Centre and use those that have been under discussion and development for months.

b. As a principle, an Open Data API service should perform as well as a bank provides to its customers directly.

48. How can MBIE most effectively monitor performance?

a. Contract the API Centre to collect and share data on performance with MBIE. Again, leveraging an existing structure would be quicker than trying to create a new API to be used from inception of the legal regime.

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?

a. The API Centre is a proven model and fit for purpose. We would recommend that MBIE contracts with the API Centre to provide a range of services to underpin the delivery of Open Data under CPD. We have no guidance to offer on how to govern other sectors as they are bought into the CPD.

b. We would be interested in how MBIE would propose to achieve the various options set out in paragraph 207, and under which legal powers.

c. There has been a recent commentary on perceptions of too much control of outcomes from the Payments NZ Board and the banks that own it. We are not aware of any examples of that, and the Commerce Commission has also noted that it is not aware of the Payments NZ Board blocking API Centre proposals[6]. We suggest that the industry follow the path set down of making the decisions of the API Centre and the Payment NZ Board on API Centre matters transparent. From that, interested parties (including MBIE) can assess the facts to determine if any problem exists that requires fixing.

[6] paragraph 166 of the Commerce Commission Payments NZ Limited Final Determination 20 August 2024. "While we understand that there have to date been no reported instances of the Payments NZ Board not approving recommendations made by the API Council or other existing working groups in the counterfactual,..."

d. We believe that the Government could also play a very useful role in the general promotion of open banking.

Funding the API Centre to provide services under the Act

i. The API Centre operates a cost recovery model, and we believe this should continue.
ii. Banks presently provide the bulk of the funding, which is because in the early lifecycle of Open Data there are relatively few third parties to contribute. With a thriving Open Data ecosystem, the mix of funding would change.
iii. We also recommend that one of the consequences of becoming an accredited recipient should be paying a fee to contribute to the operating costs of the API Centre. On a cost recovery basis, all other things being equal, the more accredited recipients there are, the lower the individual fees would be.

e. MBIE should become immediately involved with the API Centre Accreditation and Partnering Working Group

i. BNZ strongly suggests MBIE become involved in the work the API Centre is conducting to design the accreditation regime under the Commerce Commission authorisation while it is being developed.
ii. We recommend that work be conducted with the up-front aim of it being adopted and underpinned by MBIE, rather than building an API Centre accreditation process and a different MBIE accreditation process. Again, we anticipate this would be done with the agreement of the API Centre and, presumably, the Commerce Commission.
iii. The benefit of that would be that the Ministry can listen to the discussion of the options and, if thought appropriate, give input on whether the form of accreditation being developed is one it would be happy to adopt without further rework.