MINISTRY OF BUSINESS, INNOVATION & EMPLOYMENT
HIKINA WHAKATUTUKI

Discussion paper

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

August 2024

newzealand.govt.nz

Permission to reproduce

Important notice

The opinions contained in this document are those of the Ministry of Business, Innovation and Employment and do not reflect official Government policy. Readers are advised to seek specific legal advice from a qualified professional person before undertaking any action in reliance on the contents of this publication. The contents of this discussion paper must not be construed as legal advice. The Ministry does not accept any responsibility or liability whatsoever whether in contract, tort, equity or otherwise for any action taken as a result of reading, or reliance placed on the Ministry because of having read, any part, or all, of the information in this discussion paper or for any error, inadequacy, deficiency, flaw in or omission from the discussion paper.

ISBN: 978-1-991316-18-9

Submissions process

The Ministry of Business, Innovation and Employment (MBIE) seeks written submissions on the issues raised in this document by 5pm on **Thursday 10 October 2024**.

Your submission may respond to any or all of these issues. Where possible, please include evidence to support your views, for example references to independent research, facts and figures, or relevant examples.

Please use the submission template provided at: ***https://www.mbie.govt.nz/have-your-say/exploring-a-consumer-data-right-for-the-banking-sector***. This will help us to collate submissions and ensure that your views are fully considered. Please also include your name and (if applicable) the name of your organisation in your submission.

Please include your contact details in the cover letter or e-mail accompanying your submission.

You can make your submission by:

- sending your submission as a Microsoft Word document to ***consumer@mbie.govt.nz***.
- mailing your submission to:

  Consumer Policy
  Building, Resources and Markets
  Ministry of Business, Innovation & Employment
  PO Box 1473

  Wellington 6140
  New Zealand

Please direct any questions that you have in relation to the submissions process to ***consumer@mbie.govt.nz***.

Use of information

The information provided in submissions will be used to inform MBIE's policy development process, and will inform advice to Ministers on open banking. We may contact submitters directly if we require clarification of any matters in submissions.

Release of information

MBIE intends to upload PDF copies of submissions received to MBIE's website at www.mbie.govt.nz. MBIE will consider you to have consented to uploading by making a submission, unless you clearly specify otherwise in your submission.

If your submission contains any information that is confidential or you otherwise wish us not to publish, please:

- indicate this on the front of the submission, with any confidential information clearly marked within the text
- provide a separate version excluding the relevant information for publication on our website.

Submissions remain subject to request under the Official Information Act 1982. Please set out clearly in the cover letter or e-mail accompanying your submission if you have any objection to the release of any information in the submission, and in particular, which parts you consider should be withheld, together with the reasons for withholding the information. MBIE will take such objections into account and will consult with submitters when responding to requests under the Official Information Act 1982.

Private information

The Privacy Act 2020 establishes certain principles with respect to the collection, use and disclosure of information about individuals by various agencies, including MBIE. Any personal information you supply to MBIE in the course of making a submission will only be used for the purpose of assisting in the development of policy advice in relation to this review. As indicated above, MBIE intends to publish submissions. Please clearly indicate in the cover letter or e-mail accompanying your submission if you do not wish your name, or any other personal information, to be included in any publication of submissions or a summary of submissions.

Contents

List of acronyms and abbreviations

API	application programming interface – a set of routines, protocols, and tools for building software applications. An API specifies how software components should interact.
the Bill	Customer and Product Data Bill
DISTF Act	Digital Identity Services Trust Framework Act 2023
Fintech	Financial technology company
MBIE	Ministry of Business, Innovation and Employment

Ministerial Foreword

Giving New Zealanders access to their banking data – open banking – is a key enabler of better financial services and a growing financial technology sector. Your views are important, and I want to hear how we can unlock consumer data effectively in the banking sector.

Applying the Customer and Product Data Bill to the banking sector would give customers the right to share their banking information with third parties and make payments through new payment services. Customers would benefit from more convenient, innovative and secure financial services. These could include applications that assist decision-making, such as budgeting tools and streamlined loan approvals, and safer and more secure alternatives for making payments. Unlike some existing services, open banking does not require customers to disclose their online banking login credentials to third parties. Use of open banking over risky alternatives will better protect New Zealanders and help them avoid potential scams.

A robust and accessible open banking regime will attract financial technology companies to develop and offer their services in New Zealand. This will not only facilitate overseas investment, but it will also have tangible benefits for customers who can benefit from the new products and services that are created.

This proposal builds on lessons of what's worked, and what hasn't, in other countries such as the United Kingdom, Australia and Brazil.

At the core of the Customer and Product Data Bill is trust and consent. I want to ensure that standards are set so that customers can be sure that their data is safe, and the parties that are accessing it are accredited as trustworthy, competent, and secure.

The Government is committed to ensuring that consumers are informed, empowered and protected in their interactions with businesses. To ensure that we properly consider the proposed application of the Customer and Product Data Bill to the banking sector, it is important we hear the valuable perspectives of all interested parties.

As the Minister of Commerce and Consumer Affairs, I am pleased to present this discussion about the potential application of the Customer and Product Data Bill to the banking sector.

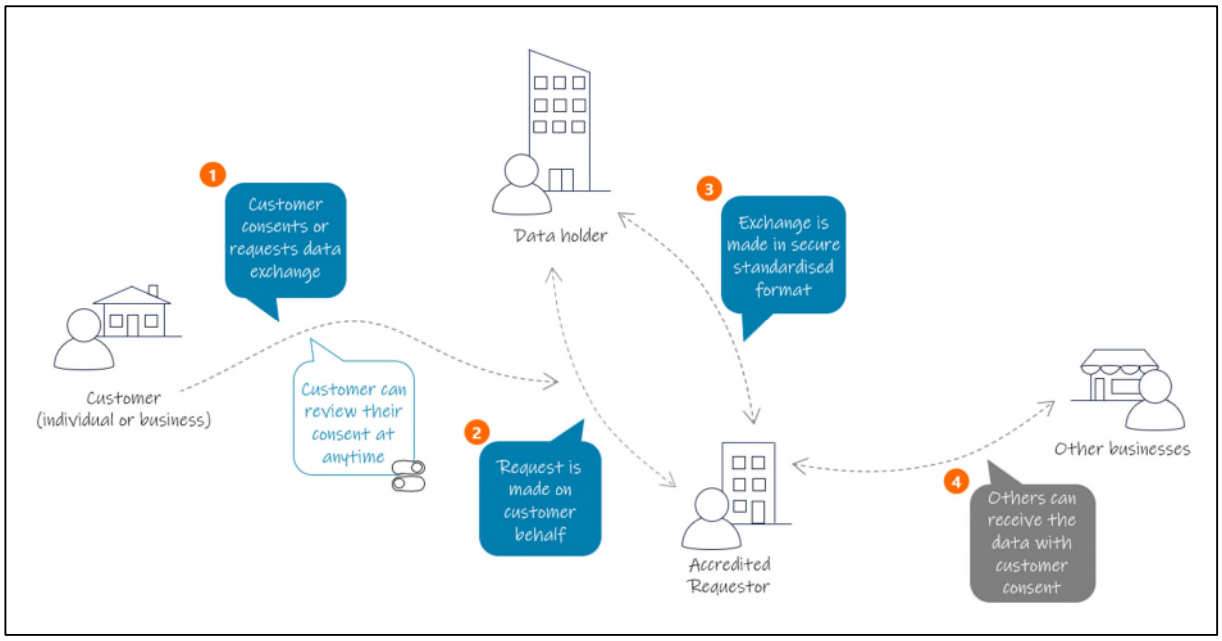
Hon Andrew Bayly
Minister of Commerce and Consumer Affairs

1 Introduction

This discussion paper seeks feedback on proposals to implement open banking under the Customer and Product Data Bill

1. The Customer and Product Data Bill (**the Bill**) is currently before Parliament and aims to establish an economy-wide framework to enable greater access to, and sharing of, customer and product data between businesses. This is commonly referred to as a 'consumer data right'. The intention of the Bill is to give customers (including both individuals and entities) in designated sectors greater control over how their customer data is accessed and used, promote innovation and facilitate competition, and facilitate secure, standardised, and efficient data services.

2. Individual sectors are designated by regulations. The Bill requires businesses that hold designated customer data (**data holders**) to provide that data to the customer and, with the customer's authorisation, to accredited third parties (**accredited requestors**). The Bill will require data holders to perform actions in response to electronic requests from customers and accredited requestors. For more about the Bill, see ***mbie.govt.nz/cdr***.



3. The purpose of this discussion paper is to seek feedback on proposals to designate the banking industry under the Bill, once it is passed. This would require banks to implement **open banking**, which means that:

   a. Banks would need to provide electronic systems and standardised application programming interfaces (**APIs**) that enable accredited requestors, with the consent of customers, to access customer data held by the bank and to perform actions (in particular, payments) on behalf of customers.

b. Accredited requestors would have automatic access to APIs, on terms and conditions provided by the Bill and the open banking regulations and standards, without the need to negotiate with individual banks for access.

c. Customers would benefit from more convenient, innovative and secure services, provided by accredited requestors. These include applications that assist decision-making, such as budgeting tools and streamlined loan approvals, and new payment services, potentially with lower fees and surcharges.

d. Customers would have greater control over their banking data, including who is it shared to and for what purpose. Banking data will be shared under the Bill only with the informed and express consent of the customer, and the customer can easily withdraw consent at any time.

4. Open banking is not new. It is operating in many countries overseas, including Australia, the United Kingdom (**UK)** and Singapore. In New Zealand, some banks have voluntarily developed open banking, under the auspices of Payment NZ's API Council and API Centre. An open banking designation under the Bill would complement these efforts to accelerate adoption and ensure that open banking is delivered efficiently and effectively.

What does this discussion paper do?

5. This discussion paper provides proposals and options, and seeks feedback on:

a. the scope of an open banking designation – which banks should be covered, and from when? What customer data must be shared, and what actions can be requested?

b. the costs, benefits and risks of an open banking designation under the Bill – is it really a good idea? What needs to be taken into account?

c. accreditation criteria – what specific criteria should businesses need to meet before they can become accredited to make requests on behalf of bank customers, and what should we consider when setting these?

d. fees – what restrictions should there be on banks charging fees for providing customer data or making payments?

e. the detailed rules for open banking – while the Bill provides high-level obligations around how requests are made and received, it leaves many aspects to secondary legislation. What happens with joint customers, or company bank accounts operated by employees? What specific steps need to be taken to ensure that customer consent to data sharing is informed? How can consents be withdrawn and should they automatically expire? What do banks and accredited requestors need to do when things go wrong?

f. standards for open banking – which technical standards do bank systems need to implement? What requirements are there for system availability and timeliness of responses?

g. institutional arrangements – how should open banking be delivered, both in the short term and longer term?

Process and timeline

6. Consultation on this discussion paper closes at 5pm on Thursday 10 October 2024.

7. The Bill is expected to be passed in early 2025.

8. Once the Bill is passed, and if the proposals in this discussion paper are advanced, regulations and standards would be made under the Bill to designate and give effect to open banking. After a transition period (which is part of the proposals being consulted on) designated banks would need to implement open banking in accordance with the Bill, regulations and standards.

Relationship with the Digital Identity Services Trust Framework Act 2023

9. On 1 July 2024, a complementary piece of legislation, the Digital Identity Services Trust Framework Act 2023 (DISTF Act), came into force. The DISTF Act establishes a legal framework that will regulate providers of digital identity services, which will support the development of trusted identity services that enable New Zealanders to safely prove who they are digitally and share their personal and organisational information. This will make it easier and safer for users to access their data under the Bill.

10. Officials from the Department of Internal Affairs and the Ministry of Business, Innovation and Employment are working together to ensure alignment between the DISTF and the Bill to fully realise the benefits of both initiatives and minimise compliance costs for system participants.

2 Status quo and problem definition

Banks are custodians of a customer's data and access to payment systems that could be used by third parties to provide services

11. Banks hold large amounts of customer data. This includes information identifying customers, the customer's bank account details and transaction records. In addition, banks are part of the inter-bank payment network, which allows customers to make payments from their bank accounts to other persons.

12. Customer data could be of significant value to customers, if they were able to share it in real time in appropriate forms with third parties, who could make use of this data to provide services to customers. For example, businesses have been established overseas, and to a lesser extent in New Zealand, to use customer data to assist decision-making, such as budgeting tools and streamlined loan approvals.

13. There are also considerable opportunities for third parties to make use of the inter-bank payment network to provide bank customers with new payment services. These could compete with established payment networks (e.g. Visa and Mastercard schemes), potentially with lower fees and surcharges, or could provide functionality that is not currently available.

14. There are two main methods for sharing customer data and enabling third party access to the inter-bank payment network:

    a. Open banking – using secure APIs that enable third parties, with the consent of customers, to access customer data held by the bank, and to perform actions (such as payments) on behalf of customers.

    b. Screen scraping (or alternatively reverse engineering of mobile banking interfaces) by third parties who impersonate customers in order to obtain customer data or make payments using banks' internet and mobile banking interfaces.

15. However, impersonated access techniques are inherently insecure, as they rely on customers providing their bank credentials (e.g. user names and passwords) to the third party. This creates a risk of misuse or unauthorised disclosure of the customer's banking credentials and also violates the bank's terms and conditions of service – potentially leaving the customer liable for any loss they suffer as a result. These techniques are also limited to the data and functionality available to customers through internet and mobile banking, and requires third parties to stay up-to-date with changes made by banks to their web sites or mobile apps.

16. This leaves open banking as the preferred solution globally for bank data sharing and new payments services.

Development of open banking in New Zealand

17. Open banking is currently being progressed by the banks and a range of third parties under the auspices of Payments NZ and its API Centre. The five largest banks are developing open banking in accordance with the API Centre Minimum Open Banking Implementation Plan.[1]

18. The API Centre Minimum Open Banking Implementation Plan sets minimum requirements and timelines for ANZ, ASB, BNZ, Westpac and Kiwibank to implement standardised APIs that are technically and operationally ready for use by the API Centre's third parties. Key requirements of the Minimum Open Banking Implementation Plan include:

    a. providing account information for transaction accounts, credit cards, savings accounts and lending accounts, and payments from transaction accounts

    b. banks are implementing specific API versions by specific dates (from 30 May 2024 through to 30 November 2026)

    c. banks to have prepared agreements that can be entered into by third parties to receive data and make payments, alongside staff and technical support for third parties

    d. target performance requirements for APIs and system monitoring.

19. On 20 August 2024, Commerce Commission granted authorisation to Payments NZ under the Commerce Act 1986 for a 'partnering framework' that would involve the joint development of:

    a. an accreditation scheme (including accreditation criteria) for third parties

    b. default standard terms and conditions on which banks would contract with third parties that meet the accreditation criteria.[2]

20. However, despite this progress, we are concerned that the market power of major banks and their advantages as incumbent holders of customer data and participants in existing payment networks will undermine the effectiveness of open banking. In particular, there are risks that further voluntary implementation of open banking may be too slow, may fail to meet desirable use cases, and the conditions for accessing customer data and payments may be too restrictive and the costs imposed on third parties may be too high. Together these create a risk that open banking uptake is low, and the potential benefits of open banking (see section 4) are largely foregone.

[1] ***https://www.apicentre.paymentsnz.co.nz/standards/implementation/minimum-open-banking-implementation-plan/***

[2] ***Payments-NZ-Limited-Final-Determination-20-August-2024.pdf (comcom.govt.nz)***

The implementation of open banking in New Zealand has been slow

21. Compared to a number of other countries, the implementation of open banking in New Zealand has been slow. The European Union amended its Payment Systems Directive in 2015 to facilitate open banking, and the Competition and Markets Authority in the UK issued a regulatory direction in 2016 to require the nine biggest UK banks to implement open banking. The UK system went live in January 2018, and now has over 300 participants. In the developing world, mobile payments powered by APIs dominate the payment systems of some countries. Open banking went live in Australia over 2019 and 2020 – though only for customer data and not action initiation.

22. Meanwhile in New Zealand, initial developments were promising. In August 2017, Hon Jacqui Dean, the former Minister of Commerce and Consumer Affairs, wrote to Payments NZ encouraging it to advance its *Payment Direction* initiative to enable 'a platform for viable alternatives to existing payment options in the New Zealand market', while noting that it 'will need to be accompanied by willingness by the banking sector to provide reasonable access to their systems and customer account data'.[3] In March 2018, Payments NZ indicated that it was focussed on a shared API framework and API standards. By March 2019, the first version of the Payment Initiation and Account Information APIs were released, and the API Centre was launched shortly afterwards.[4]

23. However, in the following four years, only two banks completed implementation of the APIs, only one engaged in significant partnering with third parties, and consequently uptake appears to have been minimal. Lack of commercial incentives for banks to roll out open banking, and potentially also regulatory uncertainty have contributed to slow implementation.

24. The Minimum Open Banking Implementation Plan has advanced implementation and uptake, with the four largest banks having now implemented payments APIs and bilateral partnering frameworks. However, despite the plan, some banks have still not fully implemented agreed standards, or have sought exemptions, indicating disagreements with the previous consensus. This makes third party and customer adoption more difficult, and may even make some use cases impossible.

25. Experience over the past five years is not a promising indicator of the likely pace and extent of future developments.

Conditions for accessing customer data and payments may be too restrictive, and the costs imposed on third parties too high

26. Even if banks fully implement current and future versions of open banking APIs, there are significant barriers to customers making full use of their data under open banking:

---

[3] ***https://www.mbie.govt.nz/assets/c974492a99/annex-to-cabinet-paper-update-on-retail-payments.pdf***
[4] ***https://www.paymentsnz.co.nz/resources/articles/making-payments-innovation-easier/***

a. At present, prospective requestors need to negotiate terms of access with each bank separately. This is costly, and a failure to agree on terms with any one bank could undermine the requestor's business.

b. Prospective requestors have expressed concerns about the conditions being placed on them by banks, such as security and insurance requirements that are perceived as onerous, which make access expensive or impossible. This may reflect bank risk aversion, and concern about the financial and reputational impacts of third parties disclosing customer data or being compromised.

c. Banks may set excessive fees for data and action initiation requests, above efficient long-run costs. This is a particular risk for large banks that have sticky customer bases and significant market power.

27. We understand that third parties have already run into difficulties with only being able to negotiate commercially viable deals with some banks and not others, undermining the overall viability of their products.

28. All of these barriers are impacted by weak incentives for banks to open up access to customer data and payments on terms that could compete with existing arrangements and payment networks.

Disincentives and barriers to adoption of open banking are likely to continue to inhibit its efficient and widespread use

29. Overall, we consider there is a high risk that lack of incentives and barriers to adoption of open banking will continue to inhibit its efficient and widespread use. While progress has been made recently, there is a risk that, over time, banks lose interest in further developing and expanding access to open banking, focussing on other activities.

30. An open banking designation under the Bill would attempt to address the above problems, as set out in the following sections.

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

3 Objectives

31. The purpose of designating banking under the Bill would be to address barriers and disincentives to further development and deployment of open banking-enabled services, and over the next five years support an open banking system that:

    a. has a substantially greater level of third party uptake (as measured by the number of participants and API calls), compared to the counterfactual

    b. provides valuable services to a substantial proportion of banking customers – and ideally most digitally active banking customers[5]

    c. incentivises further development and implementation of standards that support the most valuable use cases

    d. encourages fintechs to operate in New Zealand.

32. At the same time, a designation should not require inefficient investments, or inhibit entry or competition in banking.

33. These objectives are challenging, given that adoption has been relatively slow in a number of international markets. In the UK, only 13% of digitally active customers[6] are regular open banking users, although usage has almost doubled over the past two years. 8.2% of digitally active consumers made an open banking-enabled payment in January 2024, and 7.2% had an active data connection.[7] Australia is yet to proceed beyond data connections, and usage statistics are sparse, but most commentators consider uptake to have been disappointing – and far below the levels seen in the UK.[8]

34. Higher uptake has been seen in markets such as Singapore and Brazil. Singapore is considered one of the world leaders, with a largely market-driven approach to open banking, supported by the Monetary Authority of Singapore. In Brazil, Banco Central do Brasil's (Central Bank of Brazil's) Open Finance initiative saw rapid growth after its launch in 2020 and 2021, and now has 45 million active consents.[9]

---

[5] 55% of banking customers used online banking in the six months from July 2023 to December 2023. 71.1% were registered for online banking, and 77.1% of those customers used online banking over the six-month period. See New Zealand Banking Association (2024) Retail Banking Insights July 2023–December 2023, ***https://www.nzba.org.nz/wp-content/uploads/2024/04/Retail-banking-insights-July-to-December-2023.pdf***.

[6] Defined as those who have used digital banking in the past month.

[7] Open Banking Limited, *Open Banking Impact Report*, March 2024, ***https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-2024-march/adoption-analysis***

[8] By way of rough comparison, UK API calls in April 2024 were 48.7 million per day, compared to 3.3 million per day in Australia.

[9] ***Dashboard do Cidadão - Open Finance (openfinancebrasil.org.br)***

35. To achieve these objectives, we propose to consider designation options against the following criteria:

    a. builds on existing industry developments and momentum

    b. provides for wide uptake and valuable use cases

    c. provides customer trust and confidence in information privacy and security

    d. provides for efficient investment and does not pose a barrier to entry in banking.

36. We would welcome feedback on these objectives and criteria, and the settings needed to achieve the objectives.

3	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
4	Do you have any comments on the criteria that should be used to assess designation options?

4 The scope of an open banking designation

38. Clause 100 of the Bill provides that designation regulations may set out the persons, customer data, product data and actions to be designated.

39. We propose that the open banking designation will cover, in the first instance, the same persons as the API Centre Minimum Open Banking Implementation Plan, and the same basic categories of customer data and actions as API Centre standards. This aims to ensure that the Bill applies to agreed functionality, and is delivered within a framework that encourages fintech and customer uptake.

40. While the scope of the designation sets the outer perimeter of who the Bill applies to and what data and actions are required, much of the specific functionality to be delivered will be specified in standards that are updated more frequently (see section 9). This will be critical to evolve open banking functionality to support new use cases, focussed on applications with the highest economic or social value.

Designated persons

41. We propose that designated persons will be, to begin with, the four largest banks:

    a. ANZ Bank New Zealand Limited

    b. Bank of New Zealand

    c. ASB Bank Limited

    d. Westpac New Zealand Limited.

42. The designation, and other regulations and standards, would commence on 1 December 2025. This reflects both the time needed for government to make the necessary regulations and set up a regulator, and any additional work that banks need to complete beyond the Minimum Open Banking Implementation Plan.

43. From 1 June 2026, the designation would include Kiwibank Limited, the fifth largest bank (total assets $33.8b in 2023[10]), in respect of payments. Kiwibank will be required to provide customer data from 1 December 2026. This aligns with the timeframes in the Minimum Open Banking Implementation Plan.

[10] KPMG (2024) *Financial Institutions Performance Survey 2023 – Banks Review of 2023*, p. 50, ***https://assets.kpmg.com/content/dam/kpmg/nz/pdf/2024/03/fips-2023-banks-review.pdf***

44. The Commerce Commission's draft market study report suggested that open banking, including Kiwibank, be fully implemented by June 2026.[11] This would mean that Kiwibank would be required to provide customer data six months ahead of the timeframe in the Minimum Open Banking Implementation Plan. We would welcome feedback on the costs and benefits of an accelerated timeframe for Kiwibank.

45. Other banks and deposit takers would be invited to opt in to the designation.

46. We would welcome feedback about whether and when smaller banks and other deposit takers should be required to implement open banking. If smaller banks were required to comply, a size threshold could be imposed based on, for example:

    a. total assets – e.g. over $2 billion (corresponding to Groups 1 and 2 of locally incorporated deposit takers under the Reserve Bank's Proportionality Framework[12]) or over $5 billion

    b. number of customers with open banking products (defined below) or accounts – e.g. over 50,000.

47. We have not considered options to designate financial institutions outside of deposit-takers, as these would be covered by a wider 'open finance' designation that sought to address different problems and enable different opportunities.

Pros and cons of the proposed scope of designated persons

48. The advantages of the proposed designated persons scope are:

    a. It is the lowest cost option, covering banks that have already committed to implementing open banking.

    b. It covers the vast majority of bank accounts and credit cards. The five largest banks covered by the proposed designation scope cover 92% of main banking relationships. [13]

    c. By limiting the scope on incumbents, it does not impose compliance obligations on new entrants, and therefore should not impose any direct barriers to entry for new entrants. The ability for other banks to opt in to the designation or to otherwise make use of API standards means that they would not miss out on the competitive benefits that may come from providing open banking.

---

[11] Commerce Commission, *Personal banking services market* study, p. 251, ***https://comcom.govt.nz/__data/assets/pdf_file/0027/347373/5BPUBLIC5D-Draft-report-Personal-banking-services-market-study-21-March-2024.pdf***.

[12] ***https://www.rbnz.govt.nz/-/media/project/sites/rbnz/files/regulation-and-supervision/dta-and-dcs/the-proportionality-framework-under-the-dta.pdf***

[13] Verian (2024), *Personal banking services market study: Research report,* p. 14, ***https://comcom.govt.nz/__data/assets/pdf_file/0030/347376/Verian-Personal-Banking-Survey-Report-February-2024.pdf***.

49. However, some disadvantages of the proposed scope of designated persons are that:

    a. They exclude a small but significant number of customer bank accounts. 11% of customers hold transaction accounts with a smaller financial institution, 13% hold savings accounts, 16% hold credit cards with a smaller institution. [14] This means that applications that seek to gain a full picture of a customer's transactions (e.g. for the purposes of credit assessments or budgeting) would not be able to do so for a significant number of customers, and would need to rely on other information sources for accounts held with smaller institutions.

    b. As the scope is focussed on banks (or deposit takers) rather than other kinds of financial institutions, it would also miss a significant component of non-bank credit. For example, 44% of people have a personal loan with a financial institution other than the five largest banks. [15]

Other options for the scope of designated persons

50. Another option would be to designate a wider range of deposit takers now, with commencement at the same time as Kiwibank, or 6–12 months later. This would ensure that open banking covered almost all banking customers, maximising uptake.

51. However, requiring deposit takers to implement open banking could result in disproportionate compliance costs, which may impact their competitive position, and discourage entry.

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?
6	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?

Designation to only cover requests by accredited requestors

52. We propose that, to begin with, only requests by accredited requestors on behalf of customers be designated under the Bill. That is, we do not propose to enable requests to be made directly by customers without the involvement of an accredited requestor. This reflects the way open banking operates in other markets.

53. At present, customers can manually download their account transactions in various formats (e.g. CSV, or accounting software formats) through bank web sites and sometimes mobile applications.

[14] Verian (2024), ibid.
[15] Verian (2024), ibid.

54. The Australian statutory review of the consumer data right recommended against enabling direct-to-customer data sharing on the grounds that the limited use cases were outweighed by the greater risk of consumer harm.[16]

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?

Designated data

55. The designation must specify the data that designated banks will be required to provide through APIs. We have focussed this on data that customers already have access to through internet banking, bank websites and bank statements.

Customer data

56. We propose that designated customer data will be as follows:

    a. information identifying the customer, such as the customer's name and customer number

    b. information identifying the type of customer, such as whether the customer is an individual or company

    c. the customer's contact details

    d. information about the customer's eligibility for services and offers provided by the data holder

    e. information about the following aspects of the customer's use of **designated accounts** (defined below):

        i. information identifying the account, such as the account name and account number

        ii. information about the type of account, such as the currency

        iii. account balances

        iv. transactions

        v. bank statements

        vi. interest charges and credit fees

[16] Australian Government, *Statutory Review of the Consumer Data Right*, p. 25, ***https://treasury.gov.au/sites/default/files/2022-09/p2022-314513-report.pdf***.

vii. payment obligations

viii. authorisations for transactions given in respect of accounts, such as automatic payments and direct debits

ix. payees

x. information about offers available to the customer in respect of the account, such as balance transfers and promotional interest rates.[17]

57. We propose that the designated account types initially align with API Centre standards for customer data being: transactional accounts, savings accounts, credit card accounts and lending accounts.

58. The designation would apply to retail and business customers who have digital access to designated account types, including via bank websites and mobile banking applications. It is not proposed that designation includes open banking requirements for how banks authenticate their customers. This ensures bank authentication methods are consistent between open banking and other banking activities, and allows banks to upgrade authentication methods over time.

59. Information about other accounts would be accessible through ordinary Privacy Act processes.

60. Designated customer data is proposed to be set relatively broadly by the designation, as the more specific information that can be requested will be specified by standards.

61. We propose that accredited requestors will be able to request transactions up to 7 years old. This compares to Australia, which requires data to be provided back to 1 January 2017.[18]

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

Product data

62. Product data refers to generic information about open banking products, which is not tied to any specific customer. This can include fees and interest rates, features or benefits of the product, the terms and conditions associated with the product, or the eligibility criteria a person must meet in order to acquire or use the product.

63. At this stage, standards for product data have not yet been developed.

[17] Compare to ***Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019***, sections 6 & 7.

[18] ***https://cdr-support.zendesk.com/hc/en-us/articles/900002535683-Historic-Records-Oldest-time***

64. Information about products is currently available from bank web sites, and we understand that some banks have private APIs for accessing certain product data (e.g. mortgage and term deposit interest rates).

65. We would welcome feedback about the value and importance of providing product data through public APIs, and the specific use cases that this would enable. We would be particularly interested in any planned uses of account information or payments APIs that would be enhanced by the availability of product data APIs.

66. If product data were designated, two key issues are:

    a. The products for which product data is provided. One option would be to provide product data for the same accounts as customer data (i.e. transaction and savings accounts and credit contracts), where those accounts are available to the public.

    b. The specific information that would be provided about each products. For example:

        i. information identifying or describing the product

        ii. charges or rates associated with the product

        iii. features or benefits of the product

        iv. the terms and conditions of the product

        v. the eligibility criteria a person must meet in order to acquire or use the product.

67. We would be interested in feedback on demand for other types of product data, such as banks' foreign exchange rates.

68. Standards would need to be developed and implemented before any designation for product data could come into force. Therefore we propose that, if product data is designated, the requirement to provide it come into force six months after our proposed dates for customer data and actions.

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?

Designated actions

69. We propose that, to begin with, the only designated action will be payments initiation, from accounts where customers can transact electronic credit domestic payments in New Zealand dollars. This includes payments initiated through an enduring payment consent.

70. Payment initiation is the only action that there is currently API standards for within New Zealand, and the only action currently supported in UK open banking.

71. APIs could be developed for other actions, like making and cancelling automatic payments and direct debits, opening and closing accounts, amending limits, etc. For example, open

banking APIs in Singapore include a range of additional functionality.[19] The Commerce Commission's draft market study report suggested that implementation include other actions where these address use cases that promote competition, and mentioned opening and closing accounts (which might rely on other things such as digital identity services trust framework, and influence AML/KYC) as potential examples.[20]

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

[19] See, for example, ***https://www.dbs.com/dbsdevelopers/discover/index.html***, ***https://developers.uobgroup.com/en/apis-documentation***

[20] Commerce Commission, *Personal banking services market* study, p. 252, ***https://comcom.govt.nz/__data/assets/pdf_file/0027/347373/5BPUBLIC5D-Draft-report-Personal-banking-services-market-study-21-March-2024.pdf***.

5 The benefits, costs and risks of an open banking designation

72. The Bill requires that, before designating a sector under the Bill, the Minister must have regard to a range of factors:

    a. the interests of customers, including Māori customers

    b. any likely costs and benefits for the person or class of persons that are proposed to become data holders

    c. whether the regulations promote the implementation of secure, standardised, and efficient regulated data services

    d. the likely benefits and risks associated with the proposed designation regulations in relation to:

        i. the security, privacy, confidentiality, or other sensitivity of customer data and product data

        ii. any intellectual property rights that may exist in relation to customer data or product data.

73. Below, we set out our understanding of these matters, and invite comment on anything that is missing or incorrect.

The interests of customers

74. As discussed in the introduction, we consider the implementation of open banking through the Bill will benefit customers, as:

    a. Customers would benefit from new services, and more convenient, innovative and secure services, provided by accredited requestors. These could include applications that assist decision-making, such as budgeting tools and streamlined loan approvals, and new payment services, potentially with lower fees and surcharges. A wide range of new products have been seen in other markets where open banking has been introduced, such as the UK.

    b. Customers would benefit from greater competition for banking services. The Commerce Commission's draft market study report on personal banking states that open banking can facilitate consumers' ability to search and compare personal banking services, support digital challengers in overcoming the advantages of customer data

held with incumbent providers, and facilitate fintechs in providing over-the-top services that are less dependent on winning over main bank relationships.[21]

c. There are benefits in relation to security, privacy and confidentiality of customer data, which are discussed in more detail below. In summary, customers would have greater control over their banking data, including who is it shared to and for what purpose. Banking data shared under the Bill will require the informed and express consent of the customer, and the customer can easily withdraw consent at any time. Accreditation and security standards help to ensure that disclosure of customer data is secure.

75. The scale of the above benefits and the timeframe over which they are delivered are currently unclear. We would welcome feedback on this, particularly from businesses with an interest in delivering open banking-enabled services. We would also like to better understand the specific aspects of the open banking designation, regulations and standards that are needed to maximise these benefits.

76. The open banking designation poses risks to security, privacy and confidentiality of customer data, discussed in more detail below. These include that customer's banking data will be held by a wider range of persons, giving rise to risks of data breaches or misuse.

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?

Costs and benefits for banks

77. Implementing open banking is expensive for banks, due to the costs involved in developing, maintaining and operating the required IT infrastructure and associated services. Given that major banks have already committed to implementation of open banking, and the proposals in this paper are largely aligned with those commitments, we consider that the additional IT implementation costs imposed by the designation are comparatively low.

78. However, there are likely to be significant additional costs imposed on banks due to:

[21] Commerce Commission (2024), *Personal banking services market study: draft report*, 21 March 2024, ***https://comcom.govt.nz/__data/assets/pdf_file/0027/347373/5BPUBLIC5D-Draft-report-Personal-banking-services-market-study-21-March-2024.pdf***

a. prohibitions and limits on charging fees for designated customer data and designated actions

b. banks may need to make additional investments to meet availability and reliability requirements imposed under the Bill. However this may not be necessary if the API Centre Minimum Open Banking Implementation Plan includes standards on these matters (currently these are non-binding guidelines).

c. if product data is required to be provided, participation in the development and maintenance of new standards for product data, and implementation of system changes

d. costs of ensuring general compliance with the Bill, complying with additional obligations, and responding to requests from the regulator. For example, banks will be required to publish, implement and maintain policies relating to customer data, product data and the performance of actions.[22]

79. There are also potential benefits to banks from implementation of open banking under the Bill. These may include:

a. As potential recipients of customer data, being able to receive customer data in standard formats from other banks in relation to new or existing customers makes it more efficient to onboard new customers, customise product offerings and process loans.

b. Having customers use secure sharing methods reduces risk of security problems and the costs of managing and responding to these.

80. Further discussion of the benefits and risks in relation to security, privacy, confidentiality etc, is provided below.

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.

Promotion of the implementation of secure, standardised, and efficient regulated data services

81. We consider the designation will promote the implementation of secure, standardised, and efficient regulated data services in banking. This is because banks will be required to provide regulated data services to a wider range of third parties, in accordance with

[22] Clause 47

security and API specification standards. We consider that implementation will be more efficient than under the status quo. This is because accreditation will reduce the costs of negotiating bilateral contracts between banks and requestors, and accredited requestors will incur lower costs in requesting data and actions.

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

Benefits and risks in relation to security, privacy, confidentiality, or other sensitivity of customer data and product data

82. We consider that the designation will have a number of benefits for the security, privacy and confidentiality of customer data in banking:

    a. A customer's banking data will only be provided to accredited requestors with the customer's express and informed consent. Customers will only provide their account credentials to their bank.

    b. Security standards ensure that accredited persons are identified and strong encryption is used.

    c. As open banking is adopted, some data sharing activities that are currently undertaken through insecure methods, such as screen scraping, will instead be undertaken through secure APIs. This should reduce instances of customers providing their bank account credentials to third parties.

83. There are also risks in relation to security, privacy and confidentiality. In particular, open banking is likely to result in a larger number of persons holding customer's banking data than under the status quo. This creates a greater risk of data breaches and misuse of data. These risks are mitigated to some extent by:

    a. the consent and security measures discussed above. Section 0 below discusses further requirements to ensure that customers are informed about who their customer data will be disclosed to and for what purpose

    b. accreditation of primary recipients (see section 0 below), which helps to ensure that those persons are trustworthy and have robust systems in place

    c. obligations under the Privacy Act around use, disclosure and security of customer data.

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

Benefits and risks in relation to intellectual property rights that may exist in relation to customer data or product data

84. We do not consider that the proposed open banking designation poses risks in relation to intellectual property rights. This is because designated customer and product data is intended to be confined to data that customers already have access to, through internet banking, bank websites and bank statements.

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

6 Accreditation criteria – what specific criteria should businesses need to meet before they can become accredited to make requests on behalf of customers?

85. MBIE will be responsible for accrediting requestors under the Bill. An accreditation regime improves the security and privacy of customer data and removes the need for third parties to have multiple bilateral agreements with separate data holders. This will greatly improve the efficiency of the regime. An open banking regime will require trust in both the industry and requestors, particularly considering the sensitive nature of the data and how it may affect consumers' personal finances.

86. Clauses 105(2)(c) and (d) of the Bill provide for regulations to set criteria that persons must meet to be accredited to access customer data. Below we set out proposals and options for accreditation criteria, including:

    a. that the directors and senior managers of the applicant are fit and proper persons for their positions

    b. insurance requirements

    c. information security requirements

    d. a general criterion that the applicant can demonstrate how it will comply with its policies around customer data, product data and action initiation, and with the Act, and that there is no reason to believe that the applicant will not comply

87. We have considered these proposals and options against the following criteria:

    a. promoting a high level of trust and confidence that accredited requestors will meet their obligations under the Bill

    b. maintaining adequate security measures to protect customer data and to protect against unauthorised payments (or other designated actions)

    c. enabling participation by a range of businesses, including emergent and smaller start-ups

    d. the level of cost associated with becoming accredited and maintaining compliance with accreditation criteria.

88. A higher accreditation threshold will provide more security for customers to ensure their data is being utilised appropriately. However, if the threshold is set too high, it risks blocking new and emergent participants who may not have the capital or infrastructure to meet the requirements.

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?

Fit and proper person test

89. A common feature of licensing regimes for regulated services is a check that the directors and senior managers of the applicant are fit and proper persons. That is, that they are of good repute and they possess appropriate knowledge and experience to perform their roles. Both the Australian consumer data right and the United Kingdom's open banking systems have a test of this nature for requestors.

90. Accordingly, we propose that directors and senior managers of the accredited person must be fit and proper persons to hold their positions. The test would take into account insolvency, criminal offences or other similar court determinations, the nature and size of the requestor seeking accreditation, any professional body memberships or requisite certification, particularly around the safe usage of data, as well as any other relevant experience in banking and data.

91. We would welcome feedback on whether requestors whose directors and senior managers have already met the 'fit and proper' licensing test by the Reserve Bank, Financial Markets Authority or Commerce Commission should be deemed to meet this requirement without further assessment.

92. The advantage of the fit and proper person test is that it is a common term used in existing legislation which many industry participants are familiar with. However, it is a potentially subjective and interpretation-based exercise which may lead to ambiguity.

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?
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?

Insurance requirements

93. There is a risk that if an accredited requestor is lightly capitalised, then it may be unable to fully compensate banks or customers in the event that it breaches its obligations in the Bill. A number of overseas jurisdictions mandate cyber insurance or professional indemnity insurance. Cyber insurance protects and insures businesses against cyber attacks that can either damage or gain access to internal systems, processes or data. The insurance is business-focussed as it compensates the insured for the loss of income that comes with

cyber attacks. Professional indemnity insurance covers claims for breach of professional duty or negligence resulting in financial loss.

94. In Australia requestors are required to have adequate insurance, or a comparable guarantee. This responds to the risk of CDR consumers not being compensated for any loss that might reasonably be expected to arise from a breach of obligations under' the CDR obligations. The Australian CDR rules do not further define 'adequate' insurance. Australian Competition and Consumer Commission (ACCC) guidance suggests that professional indemnity or cyber insurance could be used to meet the requirement for 'adequate' insurance, dependent on the scope of cover and policy terms, in line with the requestors needs and capabilities.

95. The UK open banking regime leverages authorisation under the *Payment Services Regulations 2017* (UK). This requires that applicants who seek authorisation must hold either professional indemnity insurance or a comparable guarantee, this should cover the potential liability for any relevant breaches of the regulations resulting from unauthorised or fraudulent payment transactions or access to account information.[23]

96. We propose a similar principles-based requirement for adequate insurance and guarantees as in Australia and the UK. The regulator would have discretion as to what insurance or guarantees are adequate. This would require consideration of the degree of risk associated with the applicant's proposed activities, and their existing financial resources.

97. The advantage of this approach is its flexibility. This is because insurance or guarantees would only be required to the extent that there is a risk that the accredited requestor would be unable to satisfy any potential liabilities.

98. On the other hand, it may create uncertainty for prospective applicants about the level of insurance or guarantees required. This may deter requestors from applying to become accredited, if they consider the costs are excessive.

99. However, we note that insurance requirements did not appear to be raised as a significant issue in the Australian statutory review of the consumer data right.[24]

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

[23] Payment Services Regulations 2017, Regulation 6(7)(e) and (f)

[24] ***Statutory Review of the Consumer Data Right - Report (treasury.gov.au)***

Dispute resolution

100. Clause 49 of the Bill requires that accredited requestors (and data holders) must have an internal complaints process.

101. Clause 50 provides that regulations can require accredited requestors to be a member of an external dispute resolution service.

102. Banks and other financial service providers are currently required to be members of an external disputes resolution scheme. Some accredited requestors who provide financial services covered by the *Financial Services (Registration and Disputes Resolution) Act 2008* will already be members of a disputes resolution scheme.

103. We propose that all accredited requestors be required to be a member of a financial services dispute resolution scheme. These schemes are: the Banking Ombudsman (BOS), Insurance and Financial Services Ombudsman (IFSO), Financial Services Complaints Limited (FSCL), Financial Dispute Resolution Service (FDR). In the absence of such a requirement, customers whose complaints were not resolved by the internal complaints process would need to rely on the Disputes Tribunal, or the courts. The Disputes Tribunal is subject to a claims threshold of $30,000, whereas external disputes schemes handle claims up to $500,000. External schemes are also free to customers, whereas customers must pay a filing fee to the Disputes Tribunal.

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

Information security

104. An important element of trust and confidence in accredited requestors is that customers' data is protected from unauthorised access, and customers' accounts are protected from unauthorised payments. We want to ensure that accredited requestors have the requisite information security whilst also keeping the regime accessible.

105. The open banking standards specify 'security profiles' for the transfer of information. However they do not directly address wider information security practices, including third parties secure customer information that they hold. We therefore consider options from overseas regimes and levels of prescriptiveness for consideration.

Status quo – New Zealand Privacy Act framework

106. Without any further regulation, accredited requestors and other businesses that hold customer data that is also personal information will be required to meet the information privacy principle 5 under the *Privacy Act 2020*. This requires an agency that holds personal information to ensure—

    a. that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against—

i. loss

ii. access, use, modification, or disclosure that is not authorised by the agency

iii. other misuse.

b. that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

107. The Privacy Commissioner has issued *Poupou Matatapu*, guidance on the information privacy principles which is aimed at enabling organisations to 'Do privacy well'. This guidance covers information privacy principle 5 (**IPP5),** relating to storage and security of personal information.[25] The 'security and internal access controls' provide that organisations should implement a combination of physical, technical, and organizational controls to secure personal information and information technology infrastructure. This includes:

a. physical security for documents and devices

b. technical safeguards like encryption and role-based access controls

c. organizational policies for staff training and behavior monitoring

108. The guidance suggests that organisations should tailor these controls based on the sensitivity of the data they handle and the potential consequences of a security breach. Regular audits and updates to security measures are important, as is the engagement of external experts when necessary. Moreover, organisations should have robust policies for email communication, device security, information storage and disposal of sensitive data. Regular training and awareness programs are required to maintain compliance and minimise risks associated with employee misuse of information.

Australia

109. Schedule 2 of the Australian CDR rules contain a detailed set of information security requirements that are necessary in order to attain and maintain accreditation.[26] These include measures relating to:

a. *Governance:* Accredited data recipients must establish a formal security governance framework to manage information security risks related to CDR data. This framework

[25] ***https://www.privacy.org.nz/responsibilities/poupou-matatapu-doing-privacy-well/security-and-internal-access-controls/***.

[26] ***https://www.legislation.gov.au/F2020L00094/2023-07-22/2023-07-22/text/original/epub/OEBPS/document_1/document_1.html#_Toc143251580***

must outline the policies, processes, roles, and responsibilities necessary to ensure effective oversight and management of information security.

b. *Documentation of the CDR data environment*: Recipients need to define and document the boundaries of their CDR data environment, which includes the IT systems and processes managing CDR data.

c. *Maintaining an adequate information security capacity*: Recipients need to ensure that their information security capacity is appropriate for the CDR data that it holds, and the threats to that data and potential losses to CDR consumers.

d. *Information security controls***:** The CDR Rules mandate specific minimum security controls that must be implemented. These include multi-factor authentication for all access to CDR data, restricting administrative privileges to necessary personnel and reviewing these privileges regularly, and ensuring critical events are logged and monitored for irregularities. Access security measures must include timely revocation of access for users who no longer require it and quarterly reviews of user access privileges. Physical access to facilities storing or accessing CDR data must be restricted to authorized individuals. Additionally, role-based access controls should be implemented to limit access rights based on the principle of least privilege.

e. *Incident management and reporting*: Accredited data recipients must have procedures in place to detect, record, and respond to information security incidents promptly. They must develop and maintain incident response plans that cover all stages from detection to post-incident review. These plans must include notifying the Information Commissioner and CDR consumers of data breaches as required, as well as reporting security incidents to the Australian Cyber Security Centre within 30 days of awareness.

f. *Regular review:* The governance framework, CDR data environment, information security capacity and incident reporting must be reviewed and updated annually or in response to new threats in the landscape or the organisation's operational environment.

110. The Australian Competition and Consumer Commission **(ACCC)** provides further guidance on the information security aspects of the CDR Rules.[27] This guidance specifies the types of evidence that applicants for accreditation must provide to show that they meet the above information security requirements. For an unrestricted accreditation (which enables full participation in the CDR system), ACCC states that applicants must have one of the following:

a. an assurance report prepared to ASAE/ISAE/SOC 1 or 2 standard, from a suitably experienced, qualified and independent auditor

[27] ***CDR - Supplementary accreditation guidelines - information security***

b. ISO 27001 certification, together with a reduced scope assurance report that covers certain controls that are not covered by the ISO 27001 certification

c. level 1 PCI DSS compliance, together with a reduced scope assurance report that covers certain controls that are not covered by the PCI DSS certification

d. a top tier ATO Digital Service Provider Operational Security Framework compliance letter of confirmation, together with a reduced scope assurance report that covers the controls that are not covered by the ATO Digital Service Provider Operational Framework.

111. All of these evidence requirements involve the applicant commissioning an external auditor or reviewer to certify that it meets various standards, and applicants are often required to provide other detailed evidence.

United Kingdom

112. Under the *Payment Services Regulations 2017*, payment service providers must establish a framework to manage the operational and security risks to the payment services it provides, including effective incident management procedures[28]. The UK Financial Conduct Authority (**FCA)** Handbook provides further guidance, and directs that payment service providers must meet the European Banking Authority's (**EBA)** guidelines.[29]

113. Unlike the Australia guidance, the EBA guidelines[30] do not mandate compliance with specific standards such as ISO 27001. Instead, they present nine principles, including: having an operational and security risk management framework, undertaking regular risk assessments and asset monitoring, implementing both physical and data system preventative security measures, a continuous monitoring and detection policy, a business continuity plan, adequate testing of security measures, situational awareness and continuous learning, and payment service user relationship management measures.

Options

114. There are three options for information security criteria, with varying levels of prescriptiveness:

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

---

[28] ***The Payment Services Regulations 2017 (legislation.gov.uk)*** Regulation 98

[29] ***SUP 16.13 Reporting under the Payment Services Regulations - FCA Handbook*** at SUP 16.13.12

[30] ***https://www.eba.europa.eu/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf***

- 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).

115. We would welcome feedback on which of these approaches would best suit open banking in New Zealand. More prescriptive approaches may provide greater assurance that customer data is being treated safely and securely by organisations, but could make accreditation more costly and less accessible.

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

General criteria that the applicant demonstrates compliance with policies around customer data, product data and action initiation and with the Act

116. Finally, we propose that the regulator satisfy themselves that:

a. the person can demonstrate how they will comply with their policies relating to customer data, product data, and performance of actions under this Act

b. the person can demonstrate how they will comply with their obligations under the Act as an accredited requestor.

c. there is no reason to believe that the applicant will not comply with the above.

117. We envision these criteria will facilitate the imposition of compliance reporting conditions and will allow for suspension of accreditations where there is serious or repeated non-compliance.

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

7 Fees – what restrictions should there be on fees for providing customer data or initiating payments?

118. A key issue for open banking is what fees can be charged by banks to accredited requestors.[31] Fees create incentives for banks to invest in systems so that performance exceeds regulatory minimums. On the other hand, they create disincentives for customers and accredited requestors to use open banking.

119. The Bill contains provision for charges in connection with regulated data services. Under the Bill, accredited requestors have a statutory right to make requests for data and actions. This means that it is not necessary for there to be a contract between the accredited requestor and a data holder before these requests are made, although there may be other reasons to enter into such contracts. Instead, under clause 32(1)(a) of the Bill, regulations can prescribe requirements about charging amounts payable in connection with regulated data services.

120. In Australia (for customer data) and the UK, basic open banking API requests are free. Fees can be charged for access to voluntary 'premium' APIs. Similarly, in the EU, the Payment Systems Directive effectively prohibits fees by providing that API requests are not made on the basis of contract. Unauthorised screen scraping, the main alternative to open banking in an online context, is also inherently fee-free.

121. In 2023, the UK's HM Treasury commissioned a *Future of Payments Review*, which made recommendations relevant to pricing. The report recommended that the pricing model should be changed so that firms can recover some part of their costs on a sustainable commercial basis to fund consumer protection (e.g. purchase protection and merchant disputes for open banking payments) and incentivise innovation and growth. However, it also suggested that fees might only be charged for a volume of requests at a threshold above today's consumption levels to protect existing fintech business models. [32]

122. We understand that in New Zealand banks tend to charge fees for accessing APIs, with two charging models in use:

    a. tiered fees, based on numbers of API calls per month

    b. a flat subscription model, with a single monthly fee.

123. Open banking payments exist in an environment where there are both low cost but insecure alternatives (e.g. screen scraping services operating by businesses like POLi) and

[31] We have not considered fees charged by accredited requestors to customers, as these are assumed to be more competitively set.

[32] Joe Garner (2023) *Future of Payments Review*, pp. 71–75, ***https://assets.publishing.service.gov.uk/media/6557a1eb046ed400148b9b50/Future_of_Payments_Review_report.pdf***.

higher cost alternatives (card schemes, such as Visa, Mastercard or buy now pay later schemes).

124. We would welcome further feedback on what fees should be permitted to be charged in respect of both account information and payments.

125. Requests under the Bill could be:

    a. free (as in the UK)

    b. subject to pricing limits and tiers set by regulations, such as:

        i. free up to a maximum number of monthly requests per accredited requestor, with accredited requestors able to contract with banks to increase that limit

        ii. free for certain types of requests (e.g. basic, one-off payments), but with fees able to be charged for other request types (e.g. enduring payments)

        iii. capped at particular levels.

    c. subject to pricing principles set by regulations, for example requiring them to be fair and transparent, and in line with efficient long-run costs.

    d. left to commercial negotiation

    e. for payment fees, left to regulation by the Commerce Commission under the *Retail Payment System Act 2022*.

126. Under the options in subparagraph b above, specific levels or caps would need to be set. These could be adjusted over time once their impact is assessed.

127. Leaving price regulation for payments to the Commerce Commission could be an option if the interbank payment network were designated the under the *Retail Payment System Act 2022*. The Minister of Commerce and Consumer Affairs is currently considering a Commission recommendation for designation. If the Minister agrees to the designation, the Commission would have broad discretion as to how it intervenes.

128. The issue of fees and charges has only been covered to a limited extent in previous submissions on the Bill. The submissions we have received tended to favour designated data being provided either free of charge, or with caps on fees.

129. Advantages of a free or low capped approach are that:

    a. it maximises use of regulated open banking services by accredited requestors

    b. it reduces incentives to use screen scraping as an alternative to open banking.

130. Disadvantages are that:

    a. because banks cannot directly recover the costs of regulated open banking through charges, they may recover them indirectly through charges on other services provided

to customers – we are not aware of any direct evidence of this occurring overseas, although concerns about cross subsidies have been expressed in the UK[33]

b. the lack of any charges may result in an inefficiently large number of requests being made to banks by individual accredited requestors – this could limit incentive for banks to invest in increased system capacity

c. banks may be unwilling to invest in other enhancements and contribute to standards development.

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

[33] Joe Garner (2023) *Future of Payments Review*, p. 71, ***https://assets.publishing.service.gov.uk/media/6557a1eb046ed400148b9b50/Future_of_Payments_Review_report.pdf***.

8 The detailed rules for open banking

131. While many of the basic obligations on banks and accredited requestors are set out in the Bill, the Bill allows more detailed matters to be prescribed in regulations and standards. Regulations are made by the Governor-General by Order in Council on the recommendation of the Minister of Commerce and Consumer Affairs. They must be approved by Cabinet and are subject to regulatory impact analysis requirements. Standards are made by MBIE through a more streamlined process that make them more suitable for frequently updated or technical matters. Both regulations and standards can incorporate other documents by reference.

132. Key issues in banking include how express and informed consent should be obtained from customers, how consent can be withdrawn and how joint accounts and secondary users are dealt with. Some of these issues were consulted on as part of MBIE's June 2023 discussion paper, *Unlocking value from our customer data*.[34]

133. Many of these issues are currently addressed by the Payments NZ API Centre through a combination of contractual agreements between Payments NZ and participants (which are confidential) and guidelines. These requirements would not automatically apply to all accredited requestors (unless this were a condition of accreditation), and are not currently in a form where they could be incorporated as standards under the Bill.

134. In this paper we consult on our expectations for what any regulations or standards should deliver. Where standards have been developed through an industry process and meet expectations, our preferred approach would be to adopt those standards under the Bill. Where there are gaps, either because standards have not been developed, or where it would not be appropriate to develop such standards, we are likely to recommend regulations (at least in the interim).

Express and informed consent

135. Strong consent protections are central to the Bill. They are the key to respecting the authority of all customers – including businesses or other entities – over the data held about them by businesses. Clause 36 of the Bill provides that designated customer data and actions can only be requested if that customer has provided express and informed consent.

136. The June 2023 discussion paper consulted on the approach to consent to be taken under the regulations. Submitters had a range of suggestions for how to ensure that consent is sufficiently informed, and for giving customers more fine-grained control over consent. Submitters were divided on whether there should be a maximum duration for consent.

[34] ***https://www.mbie.govt.nz/assets/unlocking-value-from-our-customer-data-bill-discussion-document.pdf***

Most consumers who answered our consumer questionnaire indicated they would prefer to receive regular reminders about the consent, rather than for consent to automatically expire at a set point in time.

Express and informed consent to sharing of customer data with accredited requestors generally

137. On the basis of submissions, we propose that accredited requestors seeking authorisation to request customer data must state, immediately alongside the request:

    a. the specific data or action that will be requested

    b. the goods and services that the data will be used to provide to the customer

    c. any intended use of the data that is not necessary to provide the service

    d. a link to the accredited requestor's customer data policy.

138. We propose that customers should be required to opt in to specific uses that are not necessary to provide the service. This helps to ensure that customers are freely consenting to their data being used in other ways, without simply accepting a bundled all-or-nothing consent. However, this proposal has some disadvantages that we would welcome further feedback on:

    a. It may make it more expensive or uneconomic to provide the service, if customers do not opt in to other uses of their data that benefit the accredited requestor.

    b. It would make handling of customer data more complex, as accredited requestors would need to exclude the data belonging to some customers (who did not opt in) when processing it for certain purposes.

139. We propose that ongoing authorisations will not automatically expire, but accredited requestors will be required to notify customers at least every 12 months of:

    a. the scope and purpose of the authorisation

    b. that consent can be withdrawn at any time, and a link to where the customer can withdraw consent.

140. We would like feedback on other options to ensure that consents given to accredited requestors are express and informed. For example, whether customers should have the ability to set an expiry on ongoing consents.

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?
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?

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?

Additional requirements for express and informed consent to intermediaries

141. Particular issues arise for accredited requestors who are making requests for customer data primarily as intermediaries for other businesses, rather than to provide the customer with goods or services themselves. These intermediaries obtain accreditation to provide unaccredited businesses with customer data. Some intermediaries are 'data aggregators', which combine data from multiple sources, carry out further processing of that data, and repackage it as value-added services for other businesses. An example of this is services that combine bank transaction records from multiple banks to provide information on loan serviceability to third-party lenders.

142. This creates a risk that the initial consent is drafted in a way that is too broad. If so, the intermediary may be able to re-use data provided for one unaccredited business to provide to another unaccredited business, without the customer having expressly consented to the other unaccredited business receiving their data.

143. To address this risk, we propose that if the accredited requestor is an intermediary, authorisations must disclose:

    a. the specific persons who the accredited requestor will disclose the customer data, or other customer data that the accredited requestor derives from it, to

    b. the purpose for which each of those persons will hold and use that data.

144. Subsequent disclosure by the accredited intermediary to a different unaccredited person would require subsequent consent.

145. These disclosures should also cover customer data that is derived from designated customer data because this is still information about the customer and so should be treated as the same as the customer data originally requested. For example, the accredited requestor may request the customer's transactions, but instead of disclosing that customer data to the unaccredited person, for a certain application they may use that data to calculate and disclose the customer's total income and expenses to the unaccredited person. The customer's total income and expenses are also customer data, and so the consent should expressly cover the persons to whom this information is intended to be disclosed.

146. We do not propose that unaccredited persons receiving customer data (whether designated customer data or data derived from designated customer data) be required to become accredited. We also do not propose they be subject to any restrictions on their use and disclosure of that data other than (for personal information) complying with the *Privacy Act 2020*. We also do not propose that accredited or unaccredited persons receiving customer data be treated as data holders.

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?

Express and informed consent to payments

147. Payment initiation consents pose different issues to data consents, but some of the same basic principles apply. Many payments for goods and services will be made through an accredited payment services provider who contracts with merchants. If so, the customer will interact with the merchant in the first instance. Under the Bill as introduced, the merchant could either refer the customer to the accredited requestor to authorise the payment, or the merchant could collect the authorisation on behalf of the accredited requestor. For enduring authorisations, the merchant may subsequently instruct the accredited requestor to make payment requests in accordance with the authorisation. The accredited requestor retains primary liability for any breach of obligations under the Bill.

148. The content of the consent depends on the specific types of payments that are supported by standards, for example a one-off online payment or recurring payments. Based on existing open banking payment standards, we propose that payment initiation consents state:

    a. the details of the payment being authorised (e.g. particular, code, reference)

    b. who can act on the authorisation

    c. the account that funds will be paid to.

149. API standards will further define aspects of the authorisation, such as the amount (or for enduring consents, the maximum amount) and payment frequency.

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?

Customer dashboards

150. Clause 39 of the Bill requires data holders and accredited requestors to provide customers and secondary users with systems to enable them to view and withdraw existing authorisations. This is a key aspect to ensure customers maintain control over who has access to their customer data.

151. We propose that, for this purpose, banks provide a ‘dashboard’ that:

a. must be available to the customer through a website and mobile application at all reasonable times

b. must provide information about each active authorisation, including the accredited requestor, and the customer data or actions that the authorisation covers.

152. We propose that the dashboard provided by accredited requestors must:

a. be available to the customer through a website or mobile application at all reasonable times

b. provide information about each active authorisation, including the scope of the authorisation and its purpose

c. if the accredited requestor is an intermediary:

i. disclose the specific persons to whom customer data may be disclosed and how those persons intend to use the customer data

ii. enable the customer or secondary user to immediately withdraw authorisation to disclose to each of those persons

iii. ensure that all unaccredited parties receiving the customer data also provide an equivalent mechanism for revoking consent.

153. If a customer withdraws authorisation from the bank dashboard, this will mean that data is no longer provided by the bank to the accredited requestor, and the bank will no longer action requests from the accredited requestor. However, an accredited requestor may continue to use or disclose customer information that it has already received, in accordance with the consent.

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

Joint customers

154. Clause 21 of the Bill requires that data holders and accredited requestors must deal with the joint customers in the manner prescribed by the regulations.

155. We propose that the regulations generally follow the 'equivalency principle' for dealing with joint customers set out in the API Centre's *Equivalency Principle Policy.*[35] That is, a customer will be able to access information about joint accounts and authorise payments

35 ***https://paymentsnz.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/pages/1578467379/Equivalency+Principle+Policy***

under the same conditions as they can under existing account operating authorities and bank terms and conditions, outside of open banking.

156. By default, the Bill allows any joint customer to authorise requests for account information relating to that customer. Clause 16 provides exceptions for circumstances such as risks to safety or potential for harassment. These generally align with the circumstances in which a bank could refuse an access request from a joint customer under IPP 6 of the *Privacy Act 2020*. Given the focus of the Bill on specific designated information, the Bill does not include an equivalent to section 53(b) of the Privacy Act, that 'disclosure of the information would involve the unwarranted disclosure of the affairs of (i) another individual; or (ii) a deceased person'.

157. We are interested in feedback on whether account operating authorities for joint customers currently have any limits on a joint customers accessing account information, other than in the circumstances set out in clause 16. If there are such limits, we are interested in understanding whether this information can be requested separately under IPP 6?

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?

158. For payments, clause 19 providers that data holder is only required to perform an action if 'would ordinarily perform actions to which the request relates in the course of the data holder's business'. We take this as meaning that a bank would need to make a payment authorised by one customer if the customer's normal account operating authority allowed them to authorise payments alone. However, the bank would not be required to make such a payment if the account mandate required, for example, all joint customers to authorise payments.

159. We would welcome feedback on whether this is likely to present any difficulties in practice. In addition, we are interested in understanding whether, and how, open banking under the Bill should cater for situations where payments must be authorised by more than one joint customer.

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?

Secondary users

160. The Bill provides for 'secondary users' who operate accounts on behalf of customers. Secondary users can consent to accredited requestors making requests for customer data and actions, and secondary users also have access to the customer 'dashboard' for viewing and withdrawing authorisations. A secondary user could be, for example, an employee or contractor of a company, or an external advisor.

161. By default, the Bill does not require that data holders support secondary user functionality. Secondary users must be defined through the designation process, and regulations can set out how data holders must deal with secondary users.

162. We propose that, for open banking, authorised signatories on a customer's account be designated as secondary users. This means that there is equivalency between what authorised signatories can do under the Bill to what they can do outside the Bill.

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?

Payment limits

163. For payments, one key issue is what monetary limits there should be on payments initiated through open banking. At present open banking payment limits are at the discretion of the bank and may be the same as, or differ from, the limits imposed on internet or mobile banking. For example, a bank may have an upper limit of $10,000 per transaction, or per day. Different security measures may be taken for smaller payments compared to larger payments.

164. By default, the Bill does not limit the size of payments that may be made.

165. Payment limits are important to limit potential loss from payments made in error or due to fraud. However, if payment limits are set too low, this will limit some of the use cases for open banking.

166. Options include:

    a. providing for payment limits to be set at the discretion of banks

    b. providing for payment limits to be set at the discretion of banks, but setting a minimum limit that banks cannot go below (this minimum could differ between business customers and consumers)

    c. linking payment limits to the limits imposed on transactions the customer can initiate through internet or mobile banking (noting that these limits may be different between different types of payments, bill payees vs one-off payments, etc)

    d. imposing a standard payment limit.

38	How should payment limits be set?

Remediation of unauthorised payment

167. In certain circumstances payments may be requested that are unauthorised, resulting in consumers incurring a loss. These may be due to, for example:

a. merchant errors when initiating payments through an enduring consent

b. accredited person errors in seeking authorisation

c. customers credentials being disclosed due to a scam or fraud

d. cybersecurity incidents involving merchants or accredited persons.

168. Under the *Code of Banking Practice*, banks are liable to customers for unauthorised payments, unless the customer was dishonest or negligent, failed to comply with terms and conditions or failed to take reasonable steps to protect themselves.[36]

169. However, where an accredited requestor has requested the unauthorised payment (which would breach the provisions of the Bill), we consider liability should sit with the requestor. This is because in most cases the accredited requestor is better able to manage this risk than the bank.

170. To achieve this, we propose that an accredited requestor who requests a payment from a customer's account that has not been authorised by the customer or a secondary user must:

a. notify the bank about the unauthorised payment as soon as practicable

b. if the bank reimburses the customer, reimburse the bank for that amount.

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?

Content of the register and on-boarding of accredited requestors

171. The Bill provides for a register that holds details of data holders and accredited requestors, and support connections between them.

172. Currently the API Centre operates a register of participants that is maintained by a third party. Consideration will be given to whether this register is suitable for operation under the Bill and, if so, what organisational arrangements would need to be in place.

173. The Bill requires that the register contain certain minimum information, and provides for regulations to prescribe additional information. For data holders the minimum information comprises their name, New Zealand Business Number, physical address, details of the designations they are subject to and complaints processes. For accredited requestors this

[36] New Zealand Banking Association, *Code of Banking Practice*, ***https://www.nzba.org.nz/banking-information/code-banking-practice/code-of-banking-practice/will-respect-privacy-confidentiality-keep-banking-systems-secure/***

comprises their name and New Zealand Business Number, the classes of accreditation held and complaints processes.

174. Additional information to be included on the open banking register will depend on the functionality it is intended to support. The API Centre register helps to maintain trust between participants, providing metadata such as API endpoints, and links to digital certificates. Digital certificates are issued by internet certificate authorities, rather than by the register. The current register does not support dynamic client registration, which would allow accredited requestors to automatically register their software applications with data holders.

175. Where information is held on the register, it can either be publicly available, or restricted to participants. Information may be restricted to participants if it is desirable to do so for security purposes.

176. To minimise additional costs, we propose that, at least to begin with, the register will contain minimal additional information beyond that currently available through the existing API Centre register, and that this information be private to participants. This could be implemented by the existing register being used as the register under the Bill (see section 10).

177. This means that data holders will be expected to manually on-board accredited requestors' software applications. We consider that on-boarding is required by clause 27(a), which requires that the data holder's system enables the data holder to receive requests for regulated data services. However, we would appreciate feedback on whether regulations should provide more explicit obligations. For example, this could require banks who receive an on-boarding request from an accredited requestor to expeditiously enable access to the accredited requestor's software applications.

40	What functionality should the register have? Is certain functionality critical on commencement of the designation, or could functionality be added later?
41	What additional information needs to be held by the register to support this functionality? Should this information be publicly available, or only available to participants?
42	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?

Content of policies relating to customer data and action initiation

178. Clause 47 of the Bill requires a data holder or an accredited requestor to maintain policies relating to customer data, product data, and action performance.

179. Submissions on the draft Bill indicated a strong interest in accredited requestors' customer data policies, and proposed a range of matters that should be covered.

180. On the basis of submissions, we propose that for accredited requestors, the customer data policy be required to cover:

a. how the accredited requestor minimises data collection to what is necessary

b. geographic location where data is stored

c. all purposes for which customer data is used, and who benefits from each purpose

d. all purposes for which de-identified customer data is used, and who benefits from each purpose

e. how data is de-identified.

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?

9 Standards for open banking

API specifications for customer data and payments

182. Consistent with the expected direction of the *Minimum Open Banking Implementation Plan*, we propose that designated banks initially be required to implement APIs that meet the following technical standards from the Payments NZ API Centre:

    a. one of the Account Information API Specifications from version 2.3 to 3.0

    b. one of the Payment Initiation API Specifications from version 2.3 to 3.0.

183. Designated banks would be required to comply with the customer authorisation and authentication and security standards set out in the API Centre NZ Banking Data Security Profile from version 2.3 to 2.3.2 or the API Centre Security Profile version 3.0.

184. Beyond version 2.3, the standard setting process under the Bill would likely replace future iterations of the *Minimum Open Banking Implementation Plan*.

185. Accordingly, as part of this consultation, we are seeking feedback on when version 3.0 of the standards should become mandatory. Version 3.0 updates the security profile to improve overall safety, and adds a system for banks to notify requestors of changes to consents.[37]

186. We anticipate that the API Centre (or any successor organisation – see section 10) will continue to develop future standards (e.g. version 4.0) that, subject to consultation, MBIE will require banks to implement on specific timeframes under the Bill.

44	Do you agree with the proposed standards? Should any additional standards be prescribed?
45	When should version 3.0 of the API Centre standards become mandatory?

API specifications for product data

187. API standards have not yet been developed in New Zealand for product data. Standards for product data have been developed overseas:

    a. In Australia, requests can be made for a list of products that are currently openly offered to the market. Detailed information about specific products can be requested, including product features, eligibility criteria, fees and interest rates.[38]

[37] ***https://www.apicentre.paymentsnz.co.nz/news/articles/version-30-api-standards-released/***
[38] ***https://consumerdatastandardsaustralia.github.io/standards/#cdr-banking-api_get-products*** and ***https://consumerdatastandardsaustralia.github.io/standards/#cdr-banking-api_get-product-detail***

b. In the UK, the Open Data API Specification comprises several API specifications for ATM locations, branch locations, personal current accounts, business current accounts, SME commercial credit cards and SME loans.[39] This data is publicly available through API endpoints published on the Open Data API Dashboard.[40]

188. We would welcome feedback on what standards should be developed or adopted for product data, if this were included in the designation.

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

Performance

189. Performance standards are minimum requirements for system availability, timeliness of responses, and the number of requests that can be responded to over time (throughput).

190. Payments NZ has indicated that it is currently working on a performance standard that will set clear obligations on parties, along with metrics and minimum thresholds, for performance and availability. The requirements take into account the analysis of operational requirements in the UK Open Banking regime and New Zealand requirements based on the advice of the business and technical working groups.[41]

191. Our preference is to require compliance with this standard under the Bill, if it is finalised and meets market and customer expectations. Alternatively, if such a standard is not finalised, MBIE would look to set performance standards through regulation. In the following section, we seek feedback on expectations for performance levels.

Availability and timeliness

192. At present, the Payments NZ API Centre sets non-binding guidelines for availability and timeliness of responses. In the terminology of the Bill, these are as follows:

a. Availability – the data holder must ensure that requests are able to be received at least 99.5% of the time, each month.

b. Timeliness – while the data holder's electronic system is available, the data holder must ensure that:

i. 95% of valid payment requests are responded to within 300 ms

ii. 95% of valid customer data requests are responded to within 2 seconds.

193. We expect that banks would meet these availability and timeliness targets as a minimum.

---

[39] ***https://openbankinguk.github.io/opendata-api-docs-pub/***
[40] ***https://openbanking.atlassian.net/wiki/spaces/DZ/pages/1165263140/Open+Data+API+Dashboard/***
[41] Payments NZ, Letter to the Commerce Commission, 27 June 2024.

Throughput

194. In Australia, there are overall throughput requirements that apply across all requests. Data holders do not need to respond to requests that would result in specific thresholds being exceeded. E.g. for banks with 0 to 10,000 active authorisations, this is 150 transactions per second; for banks with 10,001 to 20,000 active authorisations, 200 transactions per second. A 'transaction' refers to responding to an API call for the purpose of the Bill.

195. The Australian standards set additional traffic thresholds for individual customers or accredited requestors during low traffic times (12am-6am) or for requests in which the customer is present.

196. Whether throughput requirements should apply to open banking under the Bill depend on what restrictions regulations provide on pricing. If pricing is left to negotiation between banks and accredited requestors, then service level commitments such as throughput may be negotiated alongside pricing. On the other hand, if regulations were to require a free tier, there may be global or individual limits on the number of transactions that were required to be provided under that free tier.

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

Performance monitoring

197. In Australia, data holders report information to the ACCC regarding performance and availability. This is achieved by data holders implementing an API that can be used by the ACCC to periodically collect this information. We would welcome feedback on whether a similar system should be adopted in New Zealand.

48	How can MBIE most effectively monitor performance?

10 Implementation, monitoring and review

198. We expect the Bill to be passed in early 2025. Regulations and standards would be made soon after to designate banking and (as discussed above) these would start to come into force in December 2025. As discussed in section 3, we consider this timeframe is realistic for banks given progress to date.

199. MBIE will be the regulator under the Bill, which means that it will be responsible for making standards (which incorporate API Centre standards by reference), setting up an accreditation function and enforcement of most obligations under the regime. These systems will need to be in place by December 2025. The Office of the Privacy Commissioner will investigate complaints that persons have breached the Privacy Act.

200. While the Minister of Commerce and Consumer Affairs and MBIE have an oversight role of the implementation of the Bill and will carry out certain functions, the API Centre will, absent further change, continue to be responsible for implementation of a wide range of functions in respect of open banking. These include:

    a. hosting of standards

    b. standards development

    c. providing best practice guidelines

    d. providing a sandbox for current and prospective accredited requestors to test software

    e. general promotion of open banking

    f. open banking delivery outside the Bill, including accreditation and partnering frameworks for any premium APIs.

201. The API Centre may also deliver the register of data holders and accredited requestors, based on its existing register of participants.

202. While existing API Centre standards and work underway provides a strong starting point for New Zealand's open banking system, it is vital that standards in the banking sector continue to evolve to meet existing or new use cases with high societal value, and to keep up with technological developments. This raises questions about whether existing governance, organisational structures and funding arrangements for open banking are fit for purpose, or whether change is required to maximise benefits from open banking.

Potential issues with current institutional arrangements

203. Currently the API Centre is a business unit of Payments NZ, and is funded by fees paid by banks and third party standards users. The Payments NZ board is responsible for approval of the API's Centre's annual business plan and fees, approval of the *Minimum Open*

Banking Implementation Plan and appointments to the API Council. The Payments NZ board delegates most other governance responsibilities for the API Centre to the API Council, which comprises up to six API Provider Standards Users (i.e. banks), six third parties (i.e. businesses that use bank data and payments), three independent members (including the chair), and a non-voting regulatory observer (currently from MBIE).[42]

204. This means that banks, who provide the majority of funding and own Payments NZ, ultimately have significant control over what standards are developed and what functionality is required to be implemented. This has a number of advantages, in helping to ensure that standards are practical and cost effective for banks to implement, and that standards take due account of developments in the banking industry. Ownership by Payments NZ ensures that API standards are aligned with wider payment system developments. However, it means that implementation is somewhat subject to banks' priorities and commercial ambitions.

205. We note that the Commerce Commission has published expectations of Payments NZ and the API Centre, including that the API Centre provide public transparency on decisions (including recommendations not adopted by Payments NZ) and its plans for the next five years of standards development.[43] Payments NZ has indicated that it will implement some of these expectations, but has expressed reservations about others.

Alternative options for institutional arrangements

206. We would welcome feedback on what arrangements are desirable, both over the short term, and the longer term, to deliver the outcomes discussed in this paper. A further consideration is what arrangements might be needed to support implementation of the Bill in other sectors that may be designated in future, such as electricity, telecommunications, etc.

207. Options include:

    a. altering the governance of the API Centre to give it greater independence from Payments NZ, or to widen representation on the API Council, e.g. from customers

    b. replacing fee funding for the API Centre with funding via levies under the Bill, to provide more funding independence

    c. creating a new body to drive implementation and standards development across multiple sectors.

---

[42] ***https://www.apicentre.paymentsnz.co.nz/about/api-council/***

[43] Commerce Commission, *Retail payment system: update on our payments between bank accounts work*, Annex B: Expectations for Industry, p. 15, ***https://comcom.govt.nz/__data/assets/pdf_file/0017/344132/Retail-Payment-System-Update-on-our-Payments-Between-Bank-Accounts-work-22-February-2024.pdf***

208. While these options could address perceived issues with current arrangements, they would have some drawbacks:

    a. Separation or greater independence of the API Centre from Payments NZ may reduce alignment of API standards with wider payment system developments. Payments NZ is currently working on a framework for 'next generation payments', which could result in a broader range of payment functionality such as verifying payees, payment to proxy identifiers (instead of requiring account numbers), real-time payments, and adoption of new standards for rich data. Much of this functionality will have links to open banking payment APIs.

    b. Any change in the short term is likely to significantly disrupt and delay current API Centre work, including improvements to standards.

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?

Review

209. The Bill does not currently include a requirement for a review. However, given the Bill is a new regime in an area of technological change, we anticipate that there will be a need to consider relatively early whether the regime is performing as expected and New Zealand is on track to meet the outcomes discussed in section 3.

210. As a short-term benchmark, if we maintain our timeframes, we will expect to see several businesses offering fully open banking-enabled services across the four largest banks by June 2026, and across the five largest banks by early 2027.

211. Over the following 2-3 years, we anticipate a review to consider:

    a. whether there has been a substantial amount of accredited requestor and customer uptake

    b. whether there has been continued development and adoption of new standards supporting new use cases

    c. whether there should be broadening of the designation to encompass additional banks and deposit-takers, and a wider range of customer data and actions.

11 Recap of questions

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?
2	Do you have any comments on the problem definition? How significant are the risks of suboptimal development and uptake under the status quo?
3	What specific objectives should the government be trying to achieve through a banking designation? What needs to happen to achieve these objectives?
4	Do you have any comments on the criteria that should be used to assess designation options?
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?
6	Do you have any views on the costs and benefits of designating a wider range of deposit takers, beyond the five largest banks?
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?
8	Do you have any comments on the customer data to be designated?
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?
10	Do you have any comments on designating payments under the Bill? Should other actions be designated? If so, when?
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?
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.

13	Do you agree that the designation will promote the implementation of secure, standardised, and efficient regulated data services?
14	Do you have any comments on the benefits and risks to security, privacy, confidentiality, or other sensitivity of customer data and product data?
15	Are there any risks from the designation to intellectual property rights in relation to customer data or product data?
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?
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?
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?
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?
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?
21	Do you agree that a principles-based approach similar to the Australian CDR rules is an appropriate insurance measure?
22	Do you agree that accredited requestors in open banking should be required to be a member of a financial services disputes resolution scheme?
23	Do you consider that information security requirements should form part of accreditation?
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?
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?
26	Do you consider any additional accreditation criteria are necessary?

27	What would be the impact of requests under the Bill being free, for banking?
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?
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?
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?
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?
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?
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?
34	Do you agree with the proposals in this paper for customer dashboards for viewing or withdrawing consent?
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?
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?
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?
38	How should payment limits be set?
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?
40	What functionality should the register have? Is certain functionality critical on commencement of the designation, or could functionality be added later?

41	What additional information needs to be held by the register to support this functionality? Should this information be publicly available, or only available to participants?
42	Is it necessary for regulations to include express obligations relating to on-boarding of accredited requestors? If so, what should these obligations be?
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?
44	Do you agree with the proposed standards? Should any additional standards be prescribed?
45	When should version 3.0 of the API Centre standards become mandatory?
46	If product data were included in the designation, what standards should be adopted or developed for product data?
47	Do you have any comments on performance standards that should apply?
48	How can MBIE most effectively monitor performance?
49	Are existing institutional arrangements with the API Centre fit for purpose, to achieve desired outcomes? If not, what changes should be considered? How should the approach change over time as other sectors are designated?