paymentsnz®

Exposure Draft – Customer and Product Data Bill

Submission by Payments NZ Limited

July 2023

1.0 Introduction

1. This submission is made by Payments NZ Limited (Payments NZ). Our Payments NZ API Centre (the Centre) is leading Aotearoa New Zealand's open banking future through its industry trust framework for open banking standards and services.

2. We welcome the publication of the exposure draft of the Customer and Product Data Bill (the Bill) and its associated discussion document, 'Unlocking value from our customer data'.

3. The consultation opened on 22 June and closed on 24 July.

4. Both the discussion document and the draft Bill are lengthy. The discussion document seeks responses to 35 detailed questions relating to the Bill. The consultation allowed for 22 working days to undertake analysis, consult with a broad range of stakeholders across both Payments NZ and the Centre, and then formulate an informed response.

5. We have addressed all questions, and these are contained in an appendix to this submission. Given the tight timeframes involved, we have elected to emphasise certain answers where our experience in building an open banking trust framework provides subject matter expertise and additional insight. Had further time been allowed we would have been able to consider the Bill and the discussion document in more detail and been able to work more closely with the cross-section of open banking stakeholders involved in the Centre.

6. The Bill and the discussion document refer to accredited requestors and data holders. Our equivalent terminology for the Centre is Third Party (usually fintechs) and API Provider (banks) respectively (collectively, these registered organisations are known as Standards Users). The context for the issues canvassed by our submission has determined which terminology we use.

7. We welcome the opportunity to provide ongoing input as the policy and legislative development process unfolds. We believe there is a need for officials to work closely with the Centre to fully embrace the value and expertise we have brought to open banking in Aotearoa to date. This is essential if officials want to achieve the policy outcomes sought by the Bill and to avoid unintended consequences in designated sectors.

2.0 Background and context

8. In this section we summarise the work of Payments NZ and the development of open banking in Aotearoa to date. This material provides important context for the points raised in the balance of our submission and outlines the experience and expertise we have in developing and managing an open banking trust framework.

9. Payments NZ is the governance organisation at the heart of Aotearoa's payments system. We govern the country's core payment clearing systems and interoperable frameworks, which process over $6 trillion of payments annually, and we work with the industry to lead the future direction of payments in Aotearoa.

10. Payments NZ's vision is for world-class payments in Aotearoa. We are committed to driving a world-class payments network to ensure financial wellbeing and equity, to build a more productive economy and to encourage greater innovation and competition in payments. As an industry leader we bring together stakeholders from across the ecosystem to develop and

deliver critical national infrastructure and payments solutions and innovations for Aotearoa[1].

11. Payments NZ has recently set a foundational Te Ao Māori Strategy, Tō Mātou Haerenga – our journey. This strategy sets out our commitment to te ao Māori and upholding Te Tiriti o Waitangi by ensuring representation and the rangatiratanga of Māori in the payments network. We believe payments that enable equity for Māori will enable equity for all. Our role as a kaitiaki of the payments system is to help enable the financial wellbeing and equity of Māori whānau, hapū and iwi.

12. The systems Payments NZ governs, including those associated with the Centre, enable the transfer of data, including Māori data. Payments NZ is currently working with data experts in Māori Data Governance to understand how those concepts might be incorporated into our rules, standards, practice and into our API Centre standards.

13. Payments NZ leads the strategic direction for the payments industry through our Payments Direction programme. This looks at the evolving future of payments and sets out plans, roadmaps, and ecosystem characteristics for that future. Since its inception, Payments Direction has set two long term strategic plans – one in 2015 with our 'Payments 2025' paper, and then in 2020 with the Payments Modernisation Plan (PMP). Next year the programme will be publishing an updated PMP, reflecting developments across the ecosystem with a focus on a next generation payments system. The Centre's trust framework has, and continues to be, an integral component of payments modernisation and the future next generation payments system.

14. Through the Payments Direction programme, industry interest in open data ecosystems and open banking began to accelerate following the publication of Payments 2025. That document laid out a view of the payments ecosystem and while it did not specifically call out open banking, it:
    - Spoke to the characteristics of the ecosystem of the future (simple payments, fast payments, informative transactions, dynamic networks etc.).
    - Set out an expectation that competitive markets would be instrumental in realising these characteristics and enabling innovation.

15. At that time there was no industry-wide standardisation of payment-related APIs in Aotearoa. This lack of consistency made it difficult for businesses to draw upon ready-to-use technical specifications and implementation models to help accelerate and scale the development of new products and services.

16. In 2017, Payments NZ started work on standardised APIs on the basis that they are an essential element of payments modernisation. Importantly, those APIs are a strategic asset for delivering greater openness in banking and payments. They enable greater competition and new forms of partnerships between financial institutions, fintechs, government and the wider financial services ecosystem.

17. In early 2018, Payments NZ launched an industry pilot of two API standards (Account Information and Payment Initiation), as key building blocks in allowing safe and efficient third party access to data from financial institutions. These standards were adapted from the Open Banking Implementation Entity (OBIE) in the United Kingdom (UK) and were modified to fit local ecosystem conditions.

18. The API Centre was established and launched in May 2019. The Centre is best thought of as a trust framework for ecosystem orchestration of open banking in Aotearoa. The five foundations

[1] A recent example of that critical infrastructure can be found here: Payments every day arrives in Aotearoa New Zealand | Payments NZ

of the Centre's service model are:

- Taking an innovation first approach
- Being market driven
- Industry led
- Inclusive and open
- Allowing for distributed delivery.

19. The Centre:
    - Has primary responsibility for facilitating the development of the open banking ecosystem, growing membership, defining standards and rules, and providing a process for breach resolution.
    - Combines central coordination of a pipeline of common API standards, the use of digital tool sets and services, and a partnering framework, with balanced and open governance so a wide range of voices from across the ecosystem can be heard.
    - Aspires to be a central coordination point, allowing networks of commercial and business relationships to grow within a structured, safe, and secure ecosystem.

20. The open banking ecosystem led by the Centre now comprises 25 registered Standards Users, made up of 8 API Providers and 17 Third Parties and over 230 Community Contributors[2].

21. The Centre has overseen years of ecosystem and standards co-design with our Standards Users. This represents over 100,000 people hours, and significant investment both within the Centre itself and within Standards User organisations. Our Standards Users have been meeting weekly, in either a technical working group or business working group capacity for over four years now. This cadence of collaboration and development has enabled the Centre to continuously build and adapt our trust framework (see the diagram in appendix 2 which sets out the Centre's open banking ecosystem including its trust framework).

22. The Centre is governed by The API Council (the Council) which represents both registered API Providers and Third Parties, in equal proportions by voting power. It also includes three independent members, one of whom is the Chair. The Council makes decisions on the day-to-day governance of the Centre and uses majority (not consensus) decision making to ensure no one party can hold veto power.

23. Over the past two years the Centre has been working with our Standards Users to strengthen the trust framework with more powers and compliance mechanisms. We have recently used those to set a minimum open banking implementation plan for our five largest API Providers.[3] Once these five API Providers are live with the same version of our standards, it will represent coverage of more than 90% of all consumer bank accounts in Aotearoa.

24. We have also been focused on supporting use case development in the ecosystem. We have developed and implemented a proof-of-concept framework for API Providers and potential Third Parties to live prove and test their customer propositions.

25. Partnerships between API Providers and Third Parties are based on bilateral commercial arrangements. The Centre supports this with its template bilateral agreement and due diligence service. Several bilateral partnerships have been formed between API Providers and Third Parties which means our API standards are being used to underpin a range of customer propositions in the market.

[2] Community contributors are interested parties, who are not yet able to become a Third Party.

[3] Minimum Open Banking Implementation Plan | API Centre (paymentsnz.co.nz)

26. While partnering based on a bilateral model will be preferred for some commercial arrangements, to truly scale an open banking ecosystem a risk-based accreditation framework is necessary. The constraints of the Commerce Act 1986 have meant the Centre has not developed an accreditation regime to date. However, we continue to look for opportunities to deliver a more comprehensive and effective partnering framework within the constraints of that legislation.

27. The new open banking ecosystem led by the Centre is not yet fully functioning and is yet to scale. However, over the next 12-18 months we expect to see significant progress across several areas including:

- The development of customer trust through further enhancement of our secure API standards and the incorporation of Māori Data Governance concepts into their design.

- A focus on quality implementation, ensuring a high level of availability and performance by monitoring and conformance testing.

- More streamlined access to our standards and services for innovators.

28. The Centre’s medium-term focus is on fostering customer trust, ensuring quality implementations, and offering clear guidance to support market led innovation and a speed to market pathway for our Standards Users.

3.0 General commentary

29. The Bill and the accompanying discussion document are aspirational statements of intent to empower consumers, unleash innovation in Aotearoa, and increase competition across the economy. The core principles of the Bill – respect, care and trust – are worthy, and as a high-level framework of intent, we are supportive of the Bill.

30. We believe enabling legislation can help the open banking ecosystem established by the Centre to realise its full potential. At a practical level, however, there is much left to be decided. Many trust framework and operational details are to be the subject of later regulations and standards.

31. While the Bill is lean, innovative, and broadly provides for a long-term framework, aspects of the Bill as currently drafted are unlikely to be fully workable in practice. If the banking sector is the first to be designated, and we agree this is a good starting point, then it is imperative there be a clear bridge between the current industry-led open banking ecosystem and the new statutory ecosystem. The enabling legislation should embrace the strategic value already created by the Centre and the industry with a view to growing and further developing scalable and sustainable products and services for customers. Without that, we have concerns meaningful progress will not be possible in that first sector and achievement of the policy intent of the Bill will be delayed.

32. In our view, a best practice customer and product data framework in Aotearoa would have the following critical attributes:

Framework and governance

- Combine sector-led delivery with regulatory oversight. This would ensure speed to market and sustainable and viable business models, while ensuring risk and safety are appropriately managed.
- Have open and inclusive representation and include representation and the rangatiratanga of Māori in the framework.
- Prioritise ecosystem needs in a way that is fair and equitable to both current and potential

future ecosystem participants.
- Provide a mechanism to set an adequate funding base to grow the ecosystem while also meeting current participant needs.

Customer-focused
- Ensure customer outcomes and consent are at the core.
- Prioritise ecosystem needs to maximise consumer and customer benefits.
- Have a robust customer redress and dispute resolution framework.

Access
- Distinguish the accreditation of an entity from conformance testing and certification of solutions/services developed by that entity.
- Provide legal certainty and clarity of relationships (regulatory permissions and requirements, civil and criminal liability).
- Provide risk-appropriate monitoring and enforcement.

Standards
- Have an industry-led mechanism for developing standards and updates.
- Have processes to introduce and update standards at the pace technology and use-cases allows for/requires.
- Provide a monitoring and assurance capability to ensure minimum ecosystem service levels are maintained.
- Apply a robust mechanism to determine roll-out timetables for new standards and major updates.
- Implement conformance requirements to match the level of access and permissions provided to participating firms.

33. With further refinement, the Bill has the potential to give effect to a best practice framework, as outlined above. However, we have identified four primary areas of concern with the Bill (and/or the supporting discussion document) that would need to be addressed to achieve its desired outcomes:
    1. The Bill does not provide a mechanism to drive innovation and uptake in open banking at an early stage.
    2. The Bill does not adequately reflect the importance of standards management (as opposed to standards development).
    3. The Bill does not adequately reflect the complexity of accreditation and conformance.
    4. Without addressing gaps in the current insurance market in Aotearoa, Third Parties may have difficulty participating in the eventual regime.

3.1 Driving innovation and uptake at an early stage

34. The Centre has already developed its trust framework and open banking ecosystem aligned with the concept of consumer data rights. That trust framework is based on best-in-class security standards, informed customer consent, leading functional (technical) standards, operational rules, guidelines, and balanced ecosystem governance.

35. Progress achieved to date could be accelerated if the Bill created the power to hold a sector accountable for delivering to the designations, and the outcomes of the Bill.

36. If the Bill provided the power to approve/accredit a sector body to develop and manage standards and day-to-day operations, then progress to date in the banking sector could be leveraged and accelerated and sustained. In short, a competent and empowered sector body could achieve the same outcomes as Ministry-enacted standards, at lower cost, and more

efficiently and effectively. Those standards would be able to respond to market needs, with minimal legislative overhead.

37. The Centre is well placed to fulfil such a role for the banking sector because it:
    - Has demonstrated appropriate knowledge and expertise in managing customer, operational and technical standards.
    - Has a proven governance model that reflects the industry voice (e.g., majority vote, not consensus so as not to allow veto powers for any one party).
    - Is “open” and includes broad consultations on standards.
    - Has proven standards management policies and procedures in place. Those policies and procedures include making and iterating upon standards that demonstrate a priority on customer value, takes account of international and cross sector interoperability, and increasingly will reflect the principles of Māori Data Governance.
    - Has the means to operate.
    - Has established and operational trust services (industry “registry”)
    - Is operationally ready to receive and assess proposed standards from any party.

3.2 Importance of standards management

38. In a related point, we are concerned that the importance of standards management is not fully reflected in the Bill. In clauses 87 – 89 the Bill contains extensive provisions for making or enacting new standards. However, in practice standards are iterative, and the larger task of standards management should be acknowledged in the primary legislation.

39. While making or enacting standards is a natural starting point, delivering value for the customer and product data ecosystem requires those standards to evolve in a sustainable, coordinated, and iterative way and in a customer-centric manner. This means those standards need to be managed over a lifecycle. The standards may be technical, operational (including security standards and non-functional/performance standards) or customer standards. The issues that might arise over the standards lifecycle may vary from sector to sector.

40. As a function, standards management needs to provide ideation, prioritisation (desirability, viability, and feasibility), design, consultation and feedback, problem resolution, delivery, and ongoing mandates for implementation and versioning. It needs to be accompanied by the right-sized governance according to the iteration at hand. For example, certain security or functional iterations of a standard require urgency/speed.

41. Given the nature of standards management, certain clauses in the Bill are impractical, such as requiring the Chief Executive sign-off for each version. A preferable approach is for a designated sector body to be made responsible for the management process outlined. This body would be held fully accountable for implementing policies concerning versioning, lifecycle management, standards governance, and overall management efficiency.

3.2 Accreditation and conformance

42. The discussion document proposes introducing two classes of accreditation in regulations for action initiation and read-only access. While we appreciate the rationale behind two different tiers, our assessment is any accreditation framework must define clearly who the actors in the ecosystem are, articulate the common data-enabled business models and reflect the risk of those models. Setting out a risk-based accreditation framework that reflects party and business model risk, removes ambiguity, and creates trust.

43. Irrespective of who is responsible for the accreditation function, there is an opportunity to

leverage assets already created by the Centre. Accreditation is not a 'one and done' exercise. It is necessary to implement a conformance regime to ensure trust and ongoing compliance with the accreditation granted. Through the Centre's register, reviews to monitor any changes, such as alterations in directorships or modifications to the company name, could be conducted and access can be enabled, or blocked, as/when needed.

44. Accreditation should be thought of separately from conformance. We assume accreditation will result in an initial entry into the register, but access rights will only be granted once the commensurate conformance requirements for the accreditation have been met.

45. Confirmation of conformance is needed to ensure adherence to the rules and standards. Any entity is only granted rights to engage in that ecosystem commensurate with its proven abilities (and those of its product/service). Conformance might extend to matters of security, consent, or functionality. It is an essential means by which trust can be communicated across the ecosystem.

46. From our reading of the discussion document and the Bill, it is not clear how the consistent terms of service will be established, or a conformance function would be discharged. In our view, in respect to banking, there is a strong case for conformance testing compliance to be organised by the Centre as a designated sector body for reasons of practicality (avoiding inefficient duplication and hand-offs) and deep subject matter expertise with the technical standards.

3.3 Insurance

47. The discussion document notes the requirements for becoming accredited may extend to having appropriate insurance. What constitutes appropriate would be assessed on a case-by-case basis by the accrediting agency when it assesses the application.

48. In most jurisdictions with a consumer data right or open banking, there is a requirement to hold "adequate insurance, or a comparable guarantee". This is due to the risk of customers and other parties not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations.

49. The type of insurance required is normally Professional Indemnity Insurance and Cyber Insurance.

50. Insurance plays a crucial role within the ecosystem by ensuring fairness for data holders, data users, and customers. In cases of data loss or fraudulent activity, it is imperative the entity responsible for that loss or activity takes full accountability for the necessary remedies.

51. Other jurisdictions have noted the amount of insurance required is best calculated on a case-by-case basis. However, in broad terms, the coverage should be related to the size and nature of the accredited requestor, its risk profile, the type of activities it undertakes and the quantity and/or value of the activity it undertakes.

52. We have received advice that suggests the nature and type of insurance a technology business requires to operate in an open banking ecosystem is not currently available directly in the domestic market. Insurance is available from overseas using specialist brokers with links into those offshore markets.

53. While being accredited might help Third Parties obtain the required insurance cover, our experience to date is Third Parties routinely face difficulties obtaining the level of insurance required by API Providers. Even if a Third Party was willing to pay a higher premium for the coverage, the insurer is not obliged to underwrite the risk if they do not wish to assume it, or they see little prospect in that market segment being profitable in the long term.

54. In our view there is a gap in the domestic insurance market that requires serious attention by officials. It is on the critical path for the successful deployment of a customer and product data ecosystem. At present, the lack of access to affordable insurance would appear to be a significant barrier to entry for some Third Parties partnering with API Providers, especially smaller entities that have the greater potential to benefit from Te Rautaki Matihiko mō Aotearoa (The Digital Strategy for Aotearoa).

4.0 Conclusion

55. The Bill and its accompanying discussion document show a commendable aspiration to empower consumers, to foster innovation, and to increase competition in Aotearoa. While the core principles are worthy, our experience to date suggests certain aspects of the Bill are impractical as currently drafted.

56. To ensure meaningful progress, it is imperative a clear bridge is established between the existing industry-led open banking ecosystem and the proposed statutory ecosystem.

57. In our view, the Bill should:
    - Grant power to sector bodies to develop and manage standards. This would promote flexibility and responsiveness to market needs and draw on sector leadership, knowledge and deep subject matter expertise while minimising some of the overhead that is evident in the Bill.
    - Explicitly acknowledge the importance of standards management and how that relates to iterative and coordinated standards development. This is crucial for delivering value in the proposed ecosystem.
    - Distinguish between accreditation, standard terms of service, and conformance processes.
    - Address the gap in the domestic insurance market. This is essential to the success of the customer and product data ecosystem.

58. By refining the Bill to address these key concerns, it can pave the way for further industry collaboration to define the architecture of the customer and product data ecosystem. This would deliver on the goals of empowering consumers, driving innovation, and promoting healthy competition across the economy.

59. The appendix that follows contains our responses to the feedback questions. Some of our responses are limited due to the time made available to us to reply to the consultation.

We would welcome the opportunity to continue dialog with MBIE and further share our industry experience.

Ngā mihi,

Steve Wiggins

Chief Executive

Payments NZ Limited

Appendix 1: Consultation Question Responses

How will the draft law interact with protections under the Privacy Act?

Q1. Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?

60. We are supportive of the balance with respect to personal customers and personal information, with some caveats.

61. We suggest more definition in primary legislation should be provided as follows:
    - Privacy principles IPP5 (security and storage) and IPP11(disclosure) should extend to all designated customer data, including non-personal entities.
    - When a customer has consented to data sharing, all designated customer data must be treated as if it were Personal Information. The data should be treated the same as under IPP5 and IPP11.
    - Data derived from the execution of consented actions should also be protected by IPP5 and IPP11.

Consent settings: Respecting and protecting customers’ authority over their data

Q2. Should there be a maximum duration for customer consent? What conditions should apply?

62. Our assessment is there should be no maximum duration on a customer’s consent. This should not be set in primary legislation or regulations issued under that primary legislation. This level of detail should form part of the standards only.

63. A customer-centric approach would enable expiry rules to exist in the context of the designated data or action. In short, customer risks are best managed through the design of the standards. This is the best way to balance ease of use for customers with maximising participation and managing implementation costs for businesses.

64. Accordingly, our recommendation is that:
    - The duration of consent should remain an optional data parameter in the relevant APIs and the customer should be able to decide the duration of a consent (subject to minimum operational needs).
    - Both the accredited requestor and the data holder should clearly playback the duration of the consent to the customer through the customer journey and, if no duration is specified, they can use words like “until you tell us to stop”.
    - The duration becomes a “limit” in the consent that both parties adhere to. \

65. Cancellation of a service should immediately revoke any consents required for the running of a service. However, consents should remain in place if there are legal grounds for the accredited requestor to maintain access to the relevant data services for the customer.

Q3. What settings for managing ongoing consent best align with data governance tikanga?

66. Payments NZ is at the beginning of our journey to understand how to enable and embed data governance tikanga into our system governance and rules and standards development. With our early work we can see a pathway to align Māori Data Governance tikanga and principles into our Centre standards and have engaged Māori data experts to assist us with this. While we have started work in this space, we are being led by subject matter experts in this area and strongly encourage officials to engage extensively and be guided by Māori Data Sovereignty and Māori Data Governance experts on this Bill and this question.

Q4. Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?

67. We do not support any regulation that specifies expiry conditions that would apply to all consent types. Evidence from other jurisdictions suggests all attempts to create a rule for maximum durations and/or renewals have been problematic for customers and create an unintended consequence whereby customers blindly renew.

68. We do support customer-defined consent durations and the ability to set event-based expiration behavior in technical standards. Consent expiry should be contextual.

Q5. How well do the proposed requirements in the draft law and regulations align with data governance tikanga relating to control, consent and accountability?

69. Please refer to question 3 above and the material in section 3 of our submission for more information.

Q6. What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?

70. The Bill states that data holders and accredited requestors must have systems in place to allow customers to view or end the authorisation. From a customer perspective, there needs to be the ability to view, amend (within the limitations of the regulations or standards), or end the authorization.

71. Adding "amend" is important as it reflects an important customer and system need. A system may respond to a request for amendment by ending the original authorisation and creating a new one according to the customer instructions.

72. Customers who consent to direct access should have to accept greater responsibilities for the safety and security of systems, managing their own access safely, authorising individuals to act on behalf of entities and staying compliant with bank account authority rules.

73. Where an outsourced provider is named in a consent, the outsourced provider should become liable for their own acts or omissions. Currently clause 24(3) effectively makes the regulated entity responsible for the outsourced provider.

Other comments

74. Existing Know Your Customer (KYC) and Customer Due Diligence (CDD) regulations create complexity for the Bill that requires careful consideration. There may be other specific financial service regulations that should be considered but these have not been identified in our analysis given the truncated consultation period.

Care during exchange: Standards

Q7. Do you think the procedural requirements for making standards are appropriate? What else should be considered?

75. The standards are described as technical standards and is implied they will include customer consent requirements. In practice, there are multiple categories of standards that need to be delivered, including:
    - Technical standards – covering security and functional API specifications, including event notifications between regulated entities.
    - Customer standards – covering obligations on regulated entities to provide for express authorisation, customer control, and disclosures. This may include customer experience, and reference consistent customer terminology.
    - Operational standards – covering obligations on regulated entities, including clause 26(2), reporting, defect management, disputes between regulated entities, obligations on behalf of secondary users and outsourced providers.

76. Over the past four years, we have well-developed and proven mechanisms for developing and maintaining robust standards, guidelines, and operational rules within each of the categories mentioned above.

77. Further to section 3 of our submission, where more information is available, we reiterate the importance of standards management as a function allied with standards development.

Q8. Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?

78. The draft law is not sufficiently clear. We would like to see more clarification and definition of known uses of data and/or ethical uses of data.

79. There are scenarios where data can be held after a service and consent is revoked. The Bill and regulations should consider whether a customer has consented to storage and data use for purposes beyond the original service. The Bill needs to address:
    - Is there a lawful reason to retain the data beyond consent?
    - What disclosures are required and how transparent are they to a customer.
    - When must data be de-personalised and when must it be deleted?

80. The Privacy Act does not cover data beyond personal data. We believe these same protections should be extended to business / non-personal customers.

Q9. From the perspective of other data holding sectors: which elements of the Payments NZ API Centre Standards are suitable for use in other sectors, and which could require significant modification?

81. The following aspects of our standards would be suitable for use in other sectors:
    - Consent-based model (with updates).
    - Within our Account Information API, there is an endpoint for:
        - Party, which allows the accredited requestor to fetch the customer details associated with the account.
        - Balance, which is generic enough to use for energy or other ‘account balances’ scenarios.

    - Offers, covering any offer the customer received from the data holder (for example, discounted rates or premium benefits).
    - Statements (of account or service usage).
    - Beneficiaries - those who benefit from the product or service.
- Security profile (standard).
    - Encourages a high degree of security within any designated sector.
    - Network security using mutually authenticated TLS.
    - Client identification/authentication using JWT OAuth 2.0 client assertions.
    - User identity with signed ID Tokens issued by the data holder.
    - OAuth 2.0 TLS-bound access tokens to prevent token hijacking.
    - Strong security profile in OpenID FAPI (high security restrictions).
- Event notification (to be published in v3), which is designed for flexibility and can be used for a wide range of events.

82. Our standards are not suitable for direct customer access in any sector. To deliver direct customer access in any sector, including banking, there are significant issues to be resolved and, judging by the Australian experience, resolving these will not be easy.

83. Additionally, the following aspects of our standards would not be suitable for use in other sectors:
    - Payment Initiation, because it is specific to banking (although this “open banking” functionality can be leveraged by many sectors wishing to provide innovative payment services).
    - Accounts, because it assumes a bank account is the underlying account mechanism with a currency, scheme etc.
    - Transactions, because these are simple debit/credit records that assume a bank account mechanism.
    - Direct debits.
    - Standing orders.

Q10. What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API’s create barriers to entry?

84. Our assessment is the banking sector is the best place to start since the industry has an existing framework, standards, guidelines, and operational rules and over four years of experience in delivering an open banking ecosystem orchestrated by the Centre. Please refer to the material in section 3 of our submission for more information.

85. High security standards should be seen as non-negotiable for any data valuable enough to be designated.

86. Differentiating security standards by sector would create unnecessary complexity and inefficiencies.

Trust: accreditation of requestors

Q11. Should there be a class of accreditation for intermediaries? If so, what conditions should apply?

87. We believe there should be a class of accreditation for intermediaries, and a risk-based approach should be applied to accreditation based on the specific business model. Please refer to the material in section 3 of our submission for more information.

Q12. Should accredited requestors have to hold insurance? If so, what kind of insurance should an accredited requestor have to hold?

88. Even though insurance is difficult to obtain, we consider it an essential requirement. The functioning of the insurance market must be addressed. Please refer to the material in section 3 of our submission for more information.

Q13. What accreditation criteria are most important to support the participation of Māori in the regime?

89. We encourage direct representation and rangatiratanga of Māori be reflected in the Bill and observance with Māori Data Governance concepts and principles be included in the accreditation criteria for data holders and accredited requestors.

Q14. Do you have any other feedback on accreditation or other requirements on accredited requestors?

90. We have devoted substantial effort to accreditation-related work. The truncated time available for consultation means we cannot capture those insights in this response. We are available to work with officials outside of this consultation to share deeper technical and business insights and findings in this area.

91. We would however like to document the inherent risks of direct access.

92. The scope of the Bill includes customers directly accessing their own data, rather than via an accredited requestor. There is considerable benefit in allowing customers to connect directly to APIs. Allowing business to directly access account information and to make payments programmatically, without any reliance on third-party services, could reduce costs and bring efficiency benefits. To a lesser extent, it also benefits very early-stage innovators/entrepreneurs who, with technical skills, will be able to test product ideas using their own data or actions on their own accounts.

93. However, while other jurisdictions have this concept in their legislation, none have achieved the outcome of regulated direct access yet.

94. There are fraud and security risks associated with direct access that need to be considered more fully. There are no upstream security standards (for example OAuth, FAPI) which would apply to this scenario.

95. Direct customer access has the potential for unintended consequence of accredited requestors choosing to access 'customer APIs' as these may these have lesser security controls. These may appear 'easier' to access as there is effectively no consent step in accessing your own data. Please

refer to the material in section 3 of our submission for more information about risk-based accreditation.

Unlocking value for all

Q15. Please provide feedback on: The potential relationships between the Bill safeguards and tikanga, and Te Tiriti/the Treaty; The types of use-cases for customer data or action initiation which are of particular interest to iwi/Māori; Any specific aspirations for use and handling of customer and product data within iwi/hapū/Māori organisations, Te Whata etc, which could benefit from the draft law.

96. As mentioned previously, we are beginning our journey to understand how to enable and embed Māori Data Governance tikanga into our Centre practice. We expect, however, that in future our new standards, iterations of standards and operational framework will reflect Māori Data Governance, tikanga practice and Te Tiriti o Waitangi. We strongly encourage officials to engage extensively and to be guided by Māori on this Bill and this question.

Q16. What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?

97. We believe it is too early in the evolution of a regulated market to ask this question.

98. It is more important, at this stage, to focus on delivering sustainable governance that can respond to market needs as required.

Q17. What settings in the draft law or regulations should be included to support accessibility and inclusion?

99. Accessibility and inclusion are important aspects of the customer experience. This is best delivered as part of the detailed standards and within implementation guides, such as customer experience guidelines.

Q18. In what ways could regulated entities and other data-driven product and service providers be supported to be accessible and inclusive?

100. We support the use of resource libraries.

101. We have found that various types of "implementation guides" have become extremely valuable. For example, sandbox, registry, customer experience guidelines, joint account guide, and an implementation guide to accompany each standard.

Ethical use of data and action initiation

Q19. What are your views on the proposed options for ethical requirements for accreditation? Do you agree about requirements to get express consent for de-identification of designated customer data?

102. We support ethical requirements as a condition of accreditation.

103. We agree with express consent for de-personalisation of designated customer data.

104. In a scenario where the accredited requestor is transmitting data or holding it as an intermediary and the consent provided to a 4th party has subsequently been revoked, or expired, then the accredited requestor must delete or de-personalise immediately.

Q20. Are there other ways that ethical use of data and action initiation could be guided or required?

105. Where data is valuable enough to be designated then it should be subject to express consent. All uses of the data must be declared and form part of the consent and must stop when consent is revoked or expires.

106. Safeguards must be made clear in any regulations.

107. The proposed model in the Bill allows an accredited requestor that does not directly acquire customers (i.e., an "intermediary"), to store, enrich, and on-share designated customer data and/or provide a means to access designated actions.

108. Consideration should be given to consent obligations on accredited requestors whereby they must:
    - Ensure the customer has access to the right information as part of the consent journey, including the accredited requestor's name, purpose for receiving the customer data, and a link to the terms and privacy notice.
    - Hold express consent for the specified customer purpose only.
    - Capture a separate and additional consent directly from the customer where a 4th party is using an accredited requestor as an intermediary and the accredited requestor proposition is different from that of the 4th party.
    - Ensure the customer can revoke consent in the 4th party application.

109. To comply with ethical use of data, accredited requestors must not provide for other data use or storage purposes through privacy notices and terms and conditions. They must always achieve express consent.

Preliminary provisions

Q21. What is your feedback on the purpose statement?

110. We support the purpose of the Bill. We believe it will be important to balance the need to improve access with the need to ensure safeguards.

Q22. Do you agree with the territorial application? If not, what would you change and why?

111. The territorial application appears to cover all possible entities that may operate in Aotearoa.

Regulated data services

Q23. Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?

112. We do not agree with the position that the data holder is not allowed to decline a valid request.

113. In principle the data holder should always respond to a valid request. However, there should always be a safety net where a data holder can decline a customer request or an authorised action, where processing the request may:
    - Contravene other legislation.
    - Put the customer at risk.
    - Put the system at risk.

114. It is important to differentiate between declining a request and declining a consent for a request that may occur separately (immediate, future, or enduring). Even when a request is accepted, there may still be reasons for stopping the future processing under a consent provided.

115. There should be a mechanism to block access (possibly via the registry) where fraud or other security concerns surface, such that customer requests cannot be acted on.

116. There should be a mechanism to stop an action after it was received as a valid request, where additional details not available at the time of the request suggest there is a valid reason to stop the action.

117. There should be an avenue for regulated parties to lodge complaints about another regulated party.

118. Data holders must also comply with other regulations that may mean they have valid reasons to decline a request.

Q24. How do automated data services currently address considerations for refusing access to data, such as on grounds in sections 49 and 57(b) of the Privacy Act?

119. Given the truncated time available for the consultation, we are unable to provide a response to this question.

Protections

Q25. Are the proposed record keeping requirements in the draft law well targeted to enabling monitoring and enforcement? Are there more efficient or effective record keeping requirements to this end?

120. The proposed record keeping requirements appear fit for purpose.

Q26. What are your views on the potential data policy requirements? Is there anything you would add or remove?

121. We support the requirement for regulated entities to publish a customer-facing data policy.

122. We recommend high level requirements such as:
    - Regulated entities disclosing any secondary uses for the data, even if the data is de-personalised.
    - Regulated entities clearly explaining how a customer can revoke access or authorisation, and what happens to their data after revocation.

123. We recommend a common format is established for key information. The common format will allow customers to compare key facts between regulated parties with relative ease.

Regulatory and enforcement matters

Q27. Are there any additional information gathering powers that MBIE will require to investigate and prosecute a breach?

124. We note that to establish an ecosystem with trust, MBIE may need the capability and powers to investigate disputes between regulated entities.

125. Ensuring behaviors between regulated entities are not detrimental to the customer will be key to delivering trust and a well-functioning ecosystem.

Administrative matters

Q28. Are the matters listed in clause 60 of the draft law the right balance of matters for the Minister to consider before recommending designation?

126. The powers for designating sectors, data holders, customer data and actions are the critical powers that MBIE requires to bring about the benefits of innovation for Aotearoa and we support these powers.
127. We note the Bill is ambiguous as to whether it relates to the designation of data holders (as subpart 1 heading and clause 59 (1) states) or whether clause 60 onwards relates to all designations.

Q29. What is your feedback on the proposed approach to meeting Te Tiriti o Waitangi/Treaty of Waitangi obligations in relation to decision-making by Ministers and officials?

128. We encourage direct representation and rangatiratanga of Māori be reflected in the Bill and for Māori to be represented in the eventual regulatory oversight regime and in each designated sectors' governance, design, development and ongoing operation.

Q30. What should the closed register for data holders and accredited requestors contain to be of most use to participants?

129. The register has three functions:
    - To provide basic information and reporting on regulated entities within the system suitable for public consumption. This may include some limited contact information.
    - To provide detailed information that can be shared between users of the system and is held privately. This will likely hold detailed metadata that may enable system access.
    - To automate processes that ensure ongoing registration / accreditation compliance as is the case in the UK.

130. Both Australian (CDR) and UK (OBIE) use this concept for their registers.

131. Information held in a registry about registered data holders may include:
    - Contact information
    - Data holder status
    - API and security endpoints
    - Versioning information
    - Brand/business names
    - Brand/business information
    - Presentation information
    - Designated sector or industry
    - Supported authorisation
    - Authorisation server metadata (OpenID/OAuth)
    - information about accredited data requestors including:
        - Contact information.
        - Data requestor status.
        - Accreditation information and level.
        - Brand/business information.
        - Software product information.
        - Any relevant API or security endpoints.

    - Presentation information (e.g., logos).

132. The register should not include implementation dates.

Q31. Which additional information in the closed register should be machine-readable?

133. Protections for users and the ability to halt participation from a party in an urgent scenario should be machine readable.

134. We recommend there should be a power or protection that allows the licensing agency to stop access under certain scenarios, without asking. These would be scenarios of threat to the system.

135. Information the register may hold would include:
    - Public certificates, including any issuing certificate authorities, certificate revocation lists etc.
    - Public keys (such as JWKS) are used to sign software statement assertions that are used in dynamic client registration.
    - Register endpoints used to access information.
    - Register endpoints are used to perform actions.
    - Software statement assertion retrieval.
    - Registered software product statuses.

Q32. Is a yearly reporting date of 31 October for the period ending 30 June suitable? What alternative annual reporting period could be more practical?

136. We see no problems with the proposed timing of annual reporting.

Q33. Should there be a requirement for data holders to provide real-time reporting on the performance of their CDR APIs? Why or why not?

137. Having monitoring and reporting requirements showing the live status and performance of the APIs is key to ensuring a functional, trusted ecosystem.

138. We have existing performance requirements for API standards and expect to introduce monitoring of performance soon.

Q34. What is your feedback on the proposal to cap customer redress which could be made available under the regulations, in case of breach?

139. In principle, the customer should be entitled to be "put right" at the earliest possibility, where they have suffered loss through no fault of their own.

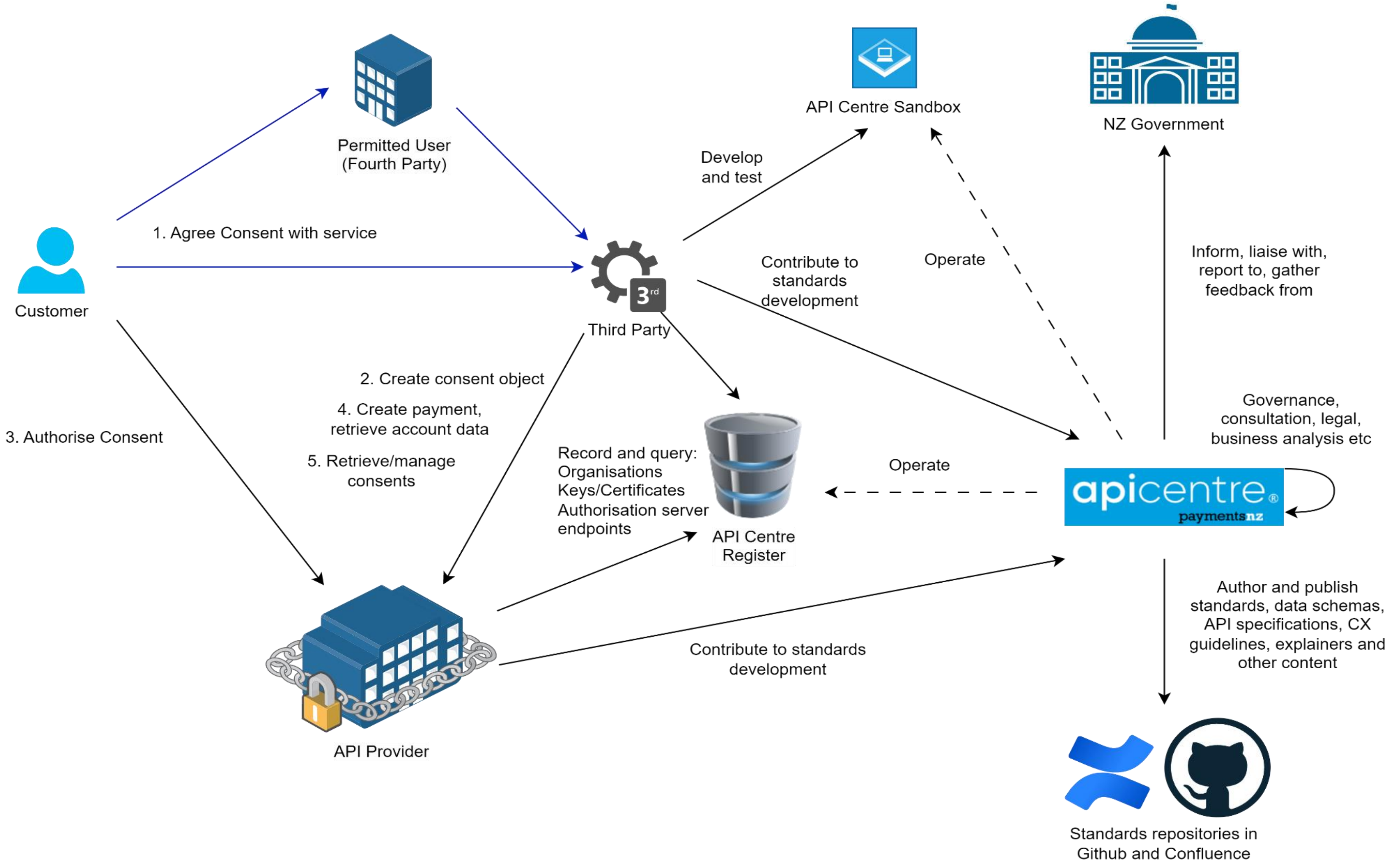
Complaints and disputes

Q35. In cases where a data holder or requestor is not already required to be member of a dispute resolution scheme, do you agree that disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes, with the Disputes Tribunal as a backstop? Why or why not?

140. We agree disputes between customers and data holders and/or accredited requestors should be dealt with through existing industry dispute resolution schemes.

141. In the UK, the OBIE spent significant sums on creating a bespoke dispute resolution scheme that was never used and has since been scrapped.

Appendix 2: API Centre Trust Framework


Permitted User
(Fourth Party)
API Centre Sandbox
NZ Government
Develop
and test
Customer
1. Agree Consent with service
Third Party
Contribute to
standards
development
Operate
Inform, liaise with,
report to, gather
feedback from
2. Create consent object
4. Create payment,
retrieve account data
5. Retrieve/manage
consents
3. Authorise Consent
Record and query:
Organisations
Keys/Certificates
Authorisation server
endpoints
Governance,
consultation, legal,
business analysis etc
Operate
apicentre
paymentsnz
API Centre
Register
Author and publish
standards, data schemas,
API specifications, CX
guidelines, explainers and
other content
Contribute to standards
development
API Provider
Standards repositories in
Github and Confluence