paymentsnz®

Customer and Product Data Bill

Payments NZ Limited submission to Economic Development, Science and Innovation Committee

5 September 2024

Introduction

Payments NZ Limited (Payments NZ) welcomes the opportunity to make a submission to the Economic Development, Science and Innovation Committee on the Customer and Product Data Bill (the Bill). We would also like to make an oral submission to the Committee.

Payments NZ's API Centre has led open banking in Aotearoa New Zealand since its establishment in 2019, and continues to work closely with both the Ministry of Business, Innovation and Employment Hīkina Whakatutuki (MBIE) and the Commerce Commission New Zealand Te Komihana Tauhokohoko (Commerce Commission) on our shared goal to see open banking thriving.

We welcome the Bill's introduction into the House. We view the Bill's unanimous support on its first reading as a sign of widespread commitment to the goal of a fit-for-purpose thriving consumer data regime for Aotearoa.

We appreciate the opportunity to provide ongoing input into the Bill's development and into the policy underlying this legislation. However, as we intend to raise significant issues regarding the completeness of the CPD framework, we are concerned that consultation has started on CPD regulations affecting the banking and energy sectors before the primary legislation has been enacted and any design issues have been resolved through the Committee process.

We believe there is considerable value in officials continuing to work closely with us to embrace the experience and expertise we bring to the operationalisation of the open banking framework in Aotearoa. We can offer real-world, first-hand insight into what has and has not worked to date, allowing officials a unique opportunity to design a CDR framework that can be applied across multiple sectors with maximum efficiency and uptake, empower the data economy, and delivering on the Bill's outcomes for society.

A fundamental element for a thriving data ecosystem, and one that will underpin the digital economy for decades to come, is the ongoing availability of new technical and operational standards ("standards"). In this submission we outline suggested improvements which will help ensure that the Bill fosters and appropriately enables this ongoing pipeline of standards. At present, the Bill delegates this fundamental matter to secondary legislation.

Through our recommended recognition model, private companies like Payments NZ could play a foundational role, ensuring the availability and use of new and/or updated standards, as well as promoting wide uptake and effective management of available standards through their lifecycles. This will help ensure that the Bill's policy objectives are met and sustained for decades to come and at the lowest cost to government.

We also see a thriving data ecosystem in Aotearoa as one that enables the active participation and representation of Māori. Our recent consumer research 'Understanding how consumers in Aotearoa pay – now and in the future' showed Māori respondents were the most enthusiastic about open banking. Māori respondents rated many open banking use cases as more appealing and were also more comfortable with secure data sharing to enable open banking than others.

More specifically, we encourage the Committee and other sectors to incorporate Māori Data Sovereignty principles and Māori Data Governance frameworks into the development of the legislative framework. We have been working closely with Māori Data experts in the API Centre to align and embed these principles and frameworks into our standards, guidelines and policies. Payments NZ is committed to this work as those principles and frameworks serve to provide foundational best practice for open data ecosystems.

Overall, we have found the Bill to be materially improved from the Exposure Draft, particularly in its recognition that a thriving data ecosystem has a considerable degree of technical and operational matters, and that these matters are best handled via secondary legislation (whether as CPD regulations or as CPD standards). When compared to the Australian CDR regulatory regime, this is a good example of Aotearoa learning from the experience of other jurisdictions and utilising the experience of industry, as available in the case of open banking via the API Centre.

The Legislation Guidelines of the Legislation Design and Advisory Committee (paragraph 14.1) states:

"As a general rule, matters of significant policy and principle should be included in an Act. Secondary legislation should generally deal with minor or technical matters of implementation and operation of the Act."

We have organised our submission around the above stated guideline. This approach recognises that we believe the Bill could still strike a better balance by ensuring fundamental features and policy are recognised in the Bill, while adding flexibility by shifting operational and technical matters into secondary legislation.

We also note some specific opportunities to remove unnecessary complexity and operational matters from the Bill, particularly in relation to secondary users, joint customers, and the Register.

We have provided a summary of key takeaways for the Committee's convenience, along with additional recommendations to further improve the Bill in an Appendix.

Table of Contents

1. Key takeaways for the Select Committee

Payments NZ Limited is committed to continuing to play its critical role in leading the open banking industry within the CPD framework

Our Payments NZ API Centre has successfully led the delivery and implementation of open banking in Aotearoa, and we are committed to continuing to play this key role into the future.

The API Centre was borne from strong system foundations. Payments NZ's governance role and leadership of the payments industry has meant the API Centre is strongly tied back to, and built to contribute to, our core vision and payments modernisation strategy on behalf of industry. This tie-back to industry wide strategy and digital infrastructure has enabled us to secure commitment to drive tangible progress in open banking, while leveraging knowledge, technical and operational know-how, legal and governance arrangements and structures.

We firmly believe that desired outcomes are best set by government, but operationalised and delivered by each sector through non-competitive industry bodies (like Payments NZ and our API Centre). We believe that our extensive experience and world-class standards in both core payments and open data standards, along with well-designed CPD legislation and regulation, will set up the data and digital economy for decades of success.

We trust the Committee fully understands the breadth and depth of progress made through the API Centre in establishing open banking. Significant industry effort and investment has delivered the necessary components to safely and securely unlock open banking, and 2024 has proven to be a key year for bringing these components together and seeing a wider range of innovative solutions reach the consumer market.

There is, however, more work to do. In the fast-changing digital economy, this work will never be fully done. We believe a well-designed CPD framework is necessary, and that this framework should empower specialised sector bodies, such as Payments NZ, to continue to play a key role.

A complete framework for a multi-sector rollout within the Bill is essential to deliver its desired outcomes

Robust, trusted, and widely accepted technical and operational standards, allowing data to be shared with appropriate consent, are fundamental to the success of any consumer data regime.

In the context of the current Bill, success will hinge on a sustained pipeline of well-managed standards, both operational and technical (API), which can be made available to the MBIE Chief Executive for incorporation under the Act.

However, the Bill as drafted does not provide the necessary means to ensure that this will happen.

To close this critical design gap and complete the framework for CPD, the Bill should empower and incentivise organisations, whether public or private, to develop both operational and technical standards on an ongoing basis.

By empowering what we call the 'recognition' model for standards management in primary legislation, the Bill will set up open banking, open energy, open telco and more for decades of success. In section 3 of our submission, we provide specific recommendations to resolve this critical gap in the design of the CPD framework. Our key advice to the Committee on this matter is:

1. To ensure Aotearoa is not out of step with global best practice, the Bill needs to establish a framework for operationalising CPD;
2. For CPD to support the data economy on a sustainable basis, the Bill must incentivise sectors to develop and manage a pipeline of high-quality technical and operational standards;
3. To maintain open banking momentum the Bill should explicitly 'recognise' the vital role of specialised standards management bodies for developing and managing standards;
4. Specific changes to the Bill are required to bring clarity and to support the 'recognition' model for CPD (in this regard, we recommend six changes to the Bill);
5. The 'recognition' model will ensure efficient use of government funds, bring greater clarity to the role of regulators and minimise duplication.

We recommend unnecessary operational matters and complexity should be removed from the Bill

Our recommendations to de-risk the Bill, and also remove operational details, are:

6. For the benefit of customers and to avoid unnecessary complexity, the concepts of a 'secondary user' and a 'joint customer' should be removed entirely from the Bill;
7. To maintain operational flexibility (where required), most of the Bill's detailed requirements for the Register should be moved to secondary legislation.

Further matters that will strengthen the Bill are recommended, with detailed rationale set out in Appendix 1.

We have drawn from our expertise and experience to identify a range of additional opportunities to improve the Bill. These are summarised as follows:

8. To ensure the Bill does not create inconsistencies and unintended consequences, obligations to prevent customer harm should be consistent with existing sector practices – particularly in relation to payment actions;
9. To avoid operational uncertainty for data holders, there should be greater clarity regarding the grounds on which a data holder can or must refuse to provide data, and any grounds for refusing payments should be consistent with current payment practices;
10. For the protection of customers throughout the data ecosystem, the duty of preventing customer harm should apply to both accredited requestors and data holders;
11. To ensure the Bill does not introduce unnecessary complexity, cost, or stifle uptake, no changes should be made to the Bill regarding derived data;
12. To ensure data can flow between sectors, the Bill should require that consideration be given to cross-sector consistency and interoperability;
13. To avoid uncertainty and ensure appropriate levels of standardisation, there needs to be more clarity on what the mandatory accredited requestors and data holder policies are expected to do;
14. To ensure there is sufficient flexibility, the Bill should allow for a standard to be made on any CPD subject;

15. To ensure designations can be well-scoped, regulations defining a sector's designation should include 'coverage' (e.g. customer segment and digital channels);
16. Given the role of the CPD framework in the digital economy, the Bill should have regard to digital inclusion outcomes;
17. To ensure trust in accredited requestors systems, the potential for testing electronic systems should cover both data holders and accredited requestors;
18. To avoid unintended loopholes and potential misuse, additional conditions are required around any ability for data holders to refuse a request from an accredited requestor based on debt owed to the data holder.

2. The API Centre's industry leadership role in delivering open banking

Payments NZ launched the API Centre in May 2019. It works to foster a self-governing open banking ecosystem for Aotearoa, in essence functioning as a trust framework for the industry. The five foundations of the API Centre's service model are:

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

The open banking ecosystem led by the API Centre now comprises 25 registered Standards Users – six API Providers (i.e. banks) and 19 registered Third Parties – as well as over 370 Community Contributors with a wider interest in the API Centre's work. The API Centre offers:

- **Proven capability** in facilitating the development of the open banking ecosystem – including growing membership, defining standards and rules, providing a process for breach resolution, and identifying and addressing strategic risks;
- **Expert knowledge** of open banking and a track record of clearly understanding and articulating the voice of the industry as a whole – enabling it to consistently deliver common API Standards, vital digital tool sets and services, and a partnering framework;
- **Balanced and open governance** which incorporates and acknowledges voices from across the open banking ecosystem, with all decisions made explicitly in the interests of the industry as a whole;
- **Central and trusted coordination** for open banking – allowing standards users to innovate, compete and establish commercial relationships within a structured, safe and secure open banking ecosystem.

The API Centre has overseen years of ecosystem and standards co-design with our Standards Users, representing over 100,000 people hours and a significant financial investment both within the API Centre itself and within standards user organisations (banks and fintechs).

Standards Users have been meeting weekly, with API Centre coordination, in either a technical or business working group capacity, for over five years. This cadence of constant knowledge-sharing and development has enabled the API Centre to continuously build the organisational and industry capability required to foster a thriving open banking ecosystem.

The API Centre supports regulation that will enable open banking to be thriving over the coming years – building upon what the industry has already achieved and leveraging the skills and knowledge we have collectively established over the last five years to deliver an innovative, safe and secure open ecosystem for Aotearoa.

3. Add to the Bill empowering provisions to recognise the vital role that sector developed standards play

To ensure Aotearoa is not out of step with global best practice, the Bill needs to establish a framework for operationalising CPD

To be successful across multiple sectors, and for decades to come, the Bill must define a framework with clear roles and responsibilities so there is a pathway for the development (and management) of technical and operational standards.

Globally, each region has defined how its version of a consumer data right regime will operate in practice prior to its rollout. Countries such as Australia, Canada, US, and UK all have frameworks that provide for deep engagement with key stakeholders during the development of such standards, as does the API Centre through its weekly working groups.

We have the opportunity to learn from other regions in designing a CPD framework that positions Aotearoa as a world leader, potentially at a lower operating cost.

We acknowledge MBIE may incorporate some of the API Centre's standards under a future designation of the banking or payments sector, and that it intends to rely on our efforts and processes to continue to develop and manage those standards once the Bill is enacted.

We also acknowledge MBIE intends to work with industry and the API Centre to ensure a smooth transition to regulated open banking. This is reflected in the Bill's Explanatory Note, which says: "It is intended that the Bill should not prevent industry-led options from being progressed in parallel to regulatory intervention and where possible, should seek to leverage that work, for example by making use of existing industry standards, technologies, and expertise."

However, as drafted, the Bill is silent on what is required to make "use of existing industry standards, technologies, and expertise" into the future, seemingly intending to rely on secondary regulations[1].

As the governance body for industry-led open banking, the API Centre's role extends well beyond just technical standards – we also take leadership responsibility for a host of complex operational issues, risk management, non-functional considerations, implementation management, and customer usage and experience matters.

We note with some concern that the full scope of standards, both technical and operational, that are required for a thriving ecosystem has not been fully accounted for in recent discussion materials from MBIE in reference to the Bill. These materials also seek feedback on various subjects that have already been considered and resolved by the API Centre through our efforts working with industry experts.

A more joined-up approach between a sector and CPD would better support our common goals of maintaining momentum in open banking and establishing a successful open data model for extension to other industries. Our recommendations for a 'recognition' model would solve this problem, acknowledging that it would materially impact the consultation on secondary regulations (running in parallel). It is our view that the Committee and MBIE should prioritise completion of the CPD framework design.

---

[1] See clauses 126(1)(f) and 126(1)(g)

The model outlined below represents what we believe is the best approach to ensure that the Bill achieves its desired outcomes in all sectors where it is applied.

For CPD to support the data economy on a sustainable basis, the Bill must incentivise sectors to develop and manage a pipeline of high-quality technical and operational standards

Setting the scene

Below we summarise the key points we made in our previous submission on the Exposure Draft. We believe they still hold paramount importance and remain relevant to the Bill:

- Progress achieved to date would be accelerated if the Bill created the power to hold a sector accountable for delivering the outcomes of the Bill;
- In particular, if the Bill provided the power to accredit or recognise a sector body to appropriately develop and manage standards and day-to-day operations, then progress to date in the banking sector could be leveraged, accelerated and sustained. A competent and empowered sector body could achieve the same outcomes as regulator-developed standards more efficiently and effectively, and at lower cost. Those standards would be able to respond to market needs, with minimal regulatory overhead;
- A preferable approach is for a 'recognised' sector body to be responsible and accountable for standards development and management functions. These vitally important functions include: standards ideation, prioritisation (desirability, viability, and feasibility), standards development and design, consultation and feedback, problem resolution, delivery, implementation, versioning, lifecycle management and overall management efficiency;
- The Bill should explicitly acknowledge the importance of standards management and how this relates to ongoing and coordinated standards development. This is crucial for delivering value in the proposed ecosystem.

As drafted, the Bill is essentially silent on the above matters. As a result, it does not ensure that the CPD framework will have ongoing access to a pipeline of cohesive technical and operational standards, which we believe should be remedied as a critical matter to ensure the CPD regime is a success.

This lack of clarity is further compounded by the broad power the Chief Executive has to make a standard. The Bill does not require the Chief Executive to have regard to any matter when making a CPD standard. We also note that a decision by the Chief Executive not to consult will not affect the validity of the CPD standard[2]. Moreover, external standards, such as the API Centre's open banking API standards, could potentially only be recognised in part or with modification (via the Legislation Act 2019), adding to the uncertainty.

We believe that delegating the design of how the CPD framework will operate to subsidiary legislation[3] undermines the clarity and focus required of the Bill. In our view it also potentially falls short of the Legislation Guidelines in terms of the expectations about the certainty and predictability of the law and creates many practical consequences, including:

1. Uncertainty as to where CPD standards will come from, and how the prioritisation of the technical and operational CPD standards is determined;

[2] See clause 134(5)
[3] See clause 126(1)(f)

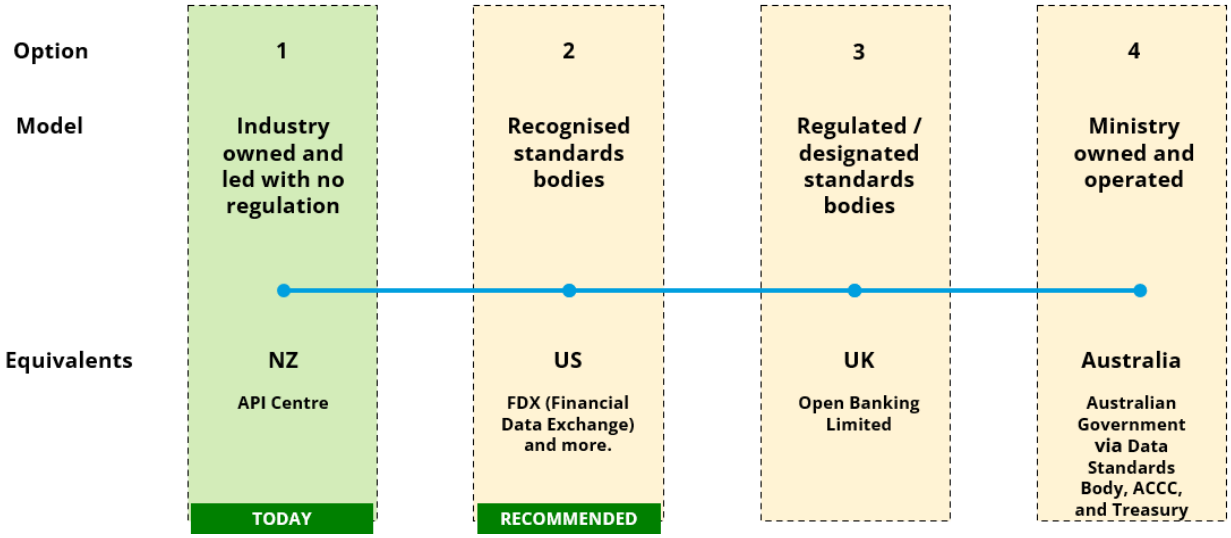
2. A likely direct and adverse impact on the API Centre and its ability to operate in a sustainable manner (MBIE's discussion paper on open banking regulations under the Bill released on 2 September 2024 provides that accredited requestors can access the standards via accreditation under the Bill, which removes the need for accredited requestors to join the API Centre. This would reduce the API Centre's ability to work with accredited parties to prioritise and co-design future standards);
3. Standards could be made by the Chief Executive with no consideration of the interests of customers, costs/benefits, security, privacy, confidentiality, or intellectual property rights (such as the Minister must consider when making designation regulations);
4. Weak incentives for sectors to invest in developing standards towards incorporation into the CPD framework, as the Bill creates no obligation on the Chief Executive to recognise or give consideration to a sector's standards development efforts and process – potentially resulting in duplication of industry development processes and efforts, significant costs and implementation delays (MBIE's discussion paper reopens and duplicates matters that have already been considered and resolved by the industry[4]);
5. The conduct of consultations by the Chief Executive could lead to changes to technical or operational standards, which could result in conflicting standards that cannot be implemented securely and safely;
6. Adoption of sector standards "in part", or "with modification"[5] (i.e. picking and choosing what parts of a sector standard is made into a CPD standard) would undermine the integrity, effectiveness and process of sector efforts to develop and implement that standard. (MBIE's discussion paper says on one hand it will adopt the API Centre's standards that align to its implementation plan[6], but on the other hand proposes variations to what is in the standards and the API Centre's implementation plan[7].)

Next, we outline a potential approach to resolving these issues within the context of the Bill and its objectives.

[4] For example, 148 of MBIE's paper covers what the payment initiation consents state when this is defined in the standard. Another example is 139 which considers whether customer data sharing consents expire after a certain time, when this is already defined in the Standards)
[5] Refer section 64(2) of the Legislation Act
[6] See 39 of MBIE's discussion paper
[7] See 56 e. of MBIE's discussion paper

To maintain open banking momentum the Bill should explicitly 'recognise' the vital role of specialised standards management bodies for developing and managing standards

Other countries operate with Recognised, Regulated or Government-owned models for standards development and management. The Bill does not provide any indication as to what model Aotearoa's open data economy is pursuing. We note MBIE's discussion paper indicates elements of both option 2 and option 3 but there is no authority in the Bill to recognise, or operationalise, either model. These models are illustrated on a spectrum below.



Each model has its own operating costs and delivery considerations. In Appendix 2 of this submission, we set out a description of each model and analyse their respective strengths and weaknesses.

Based on this analysis and our extensive experience in managing open banking standards, we consider that the 'recognition' model (as at #2 above) is clearly the best fit for Aotearoa. This will empower sectors to develop and manage technical and operational standards and ensure the efficient use of both public and private sector resources, thus enabling the CPD framework to play a key role in the future of Aotearoa's digital economy.

Specific changes to the Bill are required to bring clarity and to support the 'recognition' model for CPD

To realise the 'recognition model', we **recommend** the following six features are added into the CPD legislation:

1. **Recognise standards bodies:** That the Bill provides the Chief Executive with the authority to recognise public or private organisations who, as part of their business and expertise, intend to publish and manage technical and operational standards that can be considered for incorporation as CPD standards (for anything the Bill says may be a standard). We suggest that the Bill should enable the Chief Executive to:
    - manage a public register of such recognised bodies;

- determine the criteria for their recognition, clearly outlining expectations that standards bodies produce both the technical standards as well as the operational and customer standards that underpin the use of the technical (API) standards (for a cohesive, useable and trusted data ecosystem);
- define the operational process for applying and renewing the recognised status, with operational aspects perhaps being left to secondary legislation; and
- provide the process for both public and private organisations to apply to become recognised.

2. **Reinstate clause 89(3):** That clause 89(3) from the Exposure Draft is reinstated, ensuring that it is applicable to any standards and/or materials produced by recognised standards bodies;
3. **Whole adoption of standards:** That standards and/or materials published by a recognised body must be incorporated wholly, or not at all (avoiding the application of section 64(2)(a) of the Legislation Act 2019 that allows for standards to be incorporated in part or with modification);
4. **Chief Executive decision-making**: That the Chief Executive should have obligations set out in the Bill to have regard to important matters when a CPD standard is made. For example, similar to what the Minister must have regard to when making designation regulations (e.g. customer interests, costs, benefits, risks, security, privacy, confidentiality, sensitivity of data, intellectual property rights);
5. **Chief Executive standards**: That, in the absence of a recognised standards body for the sector (i.e. and in the absence of available standards), the Chief Executive would be able to make standards but only after establishing the necessary operational requirements, similar to that of a recognised standards body;
6. **Regulations and standards**: That the Bill is definitive between the use of regulations and the use of standards, in particular, in spelling out the types of matters where standards are appropriate (against matters that are better suited in regulations), giving greater certainty to the nature and scope of standards that a recognised standards body may deliver.

Recognising and being able to rely on the ongoing supply and management of technical standards and supporting materials produced by specialised standards bodies will bring clarity and efficiency to the ecosystem.

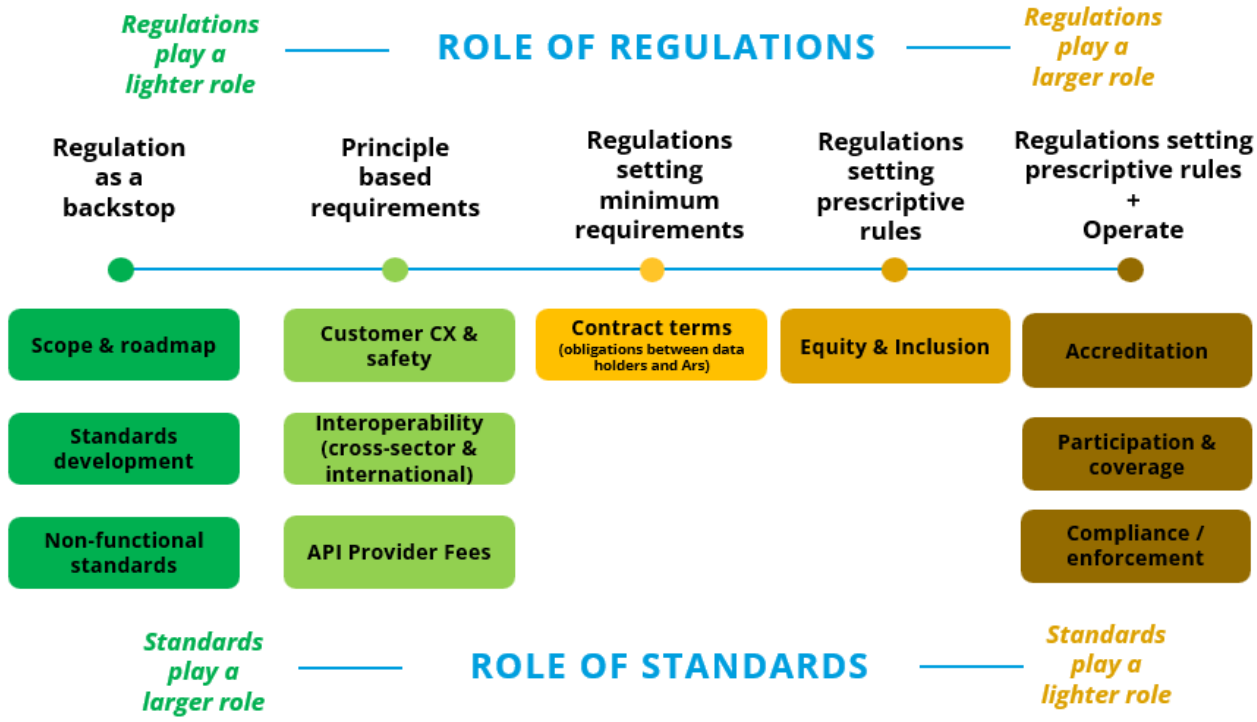
The reinstatement of clause 89(3) of the Exposure Draft would provide a legal foundation and starting point for the criteria to be established to recognise sector standards bodies. We do not see any rationale for removing this clause, which we considered well-designed (indeed reflecting international practice). Further, the outcome of its removal is uncertainty and a higher risk of unintended consequences.

In Appendix 2 we provide further rationale and analysis to support these recommendations.

The ‘recognition’ model will ensure efficient use of government funds, bring greater clarity to the role of regulators and minimise duplication

One major benefit of the recommendation above to accommodate a ‘recognition’ model in primary legislation is that it brings significantly improved clarity to the role that regulations need to play across the key areas of a CPD ecosystem. Some areas are better suited to standards and/or sector specialists playing a key role and, in these areas, a regulatory backstop approach could be in place to ensure essential public policy outcomes are delivered.

The diagram below illustrates a range of key areas within a CPD ecosystem, and the role that regulations and standards could play in supporting their effective delivery. In areas to the left of the diagram, we propose that the CPD framework allows for recognised standards bodies playing key roles, with clear responsibilities and expectations. The areas on the right-hand side represent areas where we believe appropriate regulation can be most effective in delivering the right outcomes.



4. Our recommendations to remove unnecessary complexity and operational matters from the Bill

For the benefit of customers and to avoid unnecessary complexity, the concepts of a 'secondary user' and a 'joint customer' should be removed entirely from the Bill

Secondary users

A secondary user in the Bill is a person who is not the customer but has the authority to act on the customer's behalf to view or maintain an account.

Practical examples of a secondary user can include a person with authority to act on behalf of a natural person (such as a parent/guardian, or someone holding power of attorney), or on behalf of a legal entity (such as the director of a company as an authorised signatory over the company's bank accounts).

Our experience of delivering open banking suggests it would be highly problematic if the Bill introduced this new and relatively abstract definition for persons or classes of persons who have authority to act or instruct under CPD. It would create the potential for different requirements, via regulations or standards, to apply to each category of person who may authorise data sharing.

Any new customer classes and rules for access and authority on accounts will create a risk of inconsistency with the operating authority that the data holder may have in place with its customer. They may also be contrary to the data holder's established terms and conditions.

We consider including a definition of secondary user to be an unnecessary complexity (not in the customer's best interests), and one which carries a significant risk of unintended consequences. As such we do not support the concept of a secondary user as defined and recommend that it be removed from the Bill.

Leveraging the experience of open banking to inform design of the Bill

Our industry work and our open banking standards hinge on the customer's ability to authorise data sharing or authorise a payment being consistent with the customer's account operating authority and with their bank's terms and conditions.

In open banking, API Centre standards do not have any distinction between different levels of a customer's authority or the types of customers who may authorise a new consent. This means that the 'one source of truth' with respect to the customer's authority remains with the bank (the data holder). This is an area where the API Centre and its standards users have invested significant effort to determine an approach that establishes clarity, provides the best customer experience and can be implemented efficiently (i.e. without unnecessary requirements or consequences).

It is essential that legislation and regulations align with any existing rights or obligations in relation to secondary users and joint accounts. The approach taken in the Bill runs contrary to the approach taken by the industry and the open banking standards, and as such it is our strong view that they should not be accommodated or referenced in CPD legislation in any way.

Recommended action

Amendments should be made to the Bill to preserve and not undermine the existing authority customers have with their data holders for account access, including for individuals, joint customers, and people with operating authorities for legal entities such as limited companies. Secondary users should be entirely removed from the Bill (and should not be left in the Bill 'just in case').

Particular attention in this regard should be paid to clause 100(3), which appears to expand on the definition of secondary users, but serves to underline the potential for confusion involved in creating this category of users. The removal of secondary users throughout, but particularly for this clause, would resolve this issue.

In place of secondary users, we recommend that an obligation is imposed on the data holder to ensure that any regulated data service request – such as data sharing or a payment action, in an open banking context – must be authorised by a customer with the appropriate authority to act.

Joint customers

The Bill recognises joint customers[8]. We describe joint customers as:

> *Two or more natural people, together, are the "customer". They may share account(s) for personal or business purposes.*

Following the same rationale for secondary users, we believe that joint customers should be removed from the Bill. By adopting the above-mentioned recommendation to preserve the authority customers have with the data holder for account access, there would be no need to single out joint customers in the Bill as needing special consideration.

Should it be necessary, we envisage that standards or regulations should be able to provide sufficient levels of guidance and certainty with respect to how authorisations are given for certain categories of customers.

Summary of our recommendations regarding joint accounts and secondary users:

- Remove all references and clauses in relation to secondary users;
- Remove all references and clauses in relation to joint customers;
- Include recognition that the data holder is responsible for managing the customer's authority to access and manage their accounts;
- Include obligations that the data holder will enable all authorised natural persons to authorise a request;
- Where necessary, use regulations or standards to provide guidance on how any data holders manage any specific group of customers' requirements for authorising a request.

[8] See clause 21

To maintain operational flexibility (where required), most of the Bill's detailed requirements for the Register should be moved to secondary legislation

In our view the Bill has appropriately deferred various operational and technical matters to be provided for in secondary legislation. However, Subpart 7 of the Bill (in contrast) sets out in substantial detail what the Register must contain and do operationally.

We consider the level of detail the Bill contains with respect to the Register could be significantly simplified, creating greater consistency of approach across the Bill.

The Register performs an operational role that is very likely to evolve and change over time. As such, defining its operation in detail within the Bill creates a risk that relatively low-level operational changes will require amendments to legislation.

In light of this, we recommend that Subpart 7 is simplified, establishing the Register's purpose and role, but leaving the specifics of what it must do and contain to be defined in secondary legislation.

5. Other recommended improvements to the Bill

In Appendix 1 to this submission, we set out additional recommendations that we think should be made to the Bill. These recommendations cover a range of important issues that will ensure a smooth transition to regulated open banking, and ensure our experience benefits a multi-sector customer and product data regime.

Conclusion

We thank the Economic Development, Science and Innovation Committee for the opportunity to respond on this consultation. We hope you find that our feedback and recommendations constructively contribute to the direction and development of the law. We look forward to the opportunity to discuss this further before the Committee.

Nāku noa, nā,

Steve Wiggins

Chief Executive

Payments NZ Limited

APPENDIX 1

Other important recommended improvements to the Bill

To ensure the Bill does not create inconsistencies and unintended consequences, obligations to prevent customer harm should be consistent with existing sector practices – particularly in relation to payment actions

The legal and common law basis for a banker's duty of care in relation to a customer instructing their bank to make a payment is well established. A contractual duty of care is implied into the banker customer relationship at common law, and reflects concerns to ensure that banks do not abuse the trust placed in them by their customers.

As drafted, the Bill risks being inconsistent with these practices, creating a dual practice where CPD has different and unnecessary obligations compared to other payment types.

In the context of processing payment instructions, banks have two contractual duties: (a) to act on a customer's instruction without delay; and (b) to exercise reasonable care in carrying out the customer's instructions. These duties can be modified or clearly articulated and defined in the bank's contract with its customer. These may, for example, also detail the bank's ability to refuse to act on a payment instruction if they have reasonable grounds to suspect that acting on a payment instruction might result in the misappropriation of funds through fraud.

Generally, the above described duties apply across the many different types of payments and the various channels that the customers interact with. Currently, the duty of care obligations on banks when processing an open banking payment are broadly consistent with other types of payments and digital channels. In other words, to date, open banking payments have leveraged and adopted existing payments practices regarding the duty of care owed to customers, and have not created separate bespoke sets of duties.

For the successful adoption of open banking payments under CPD, it is of paramount importance that CPD does not introduce additional and unnecessary complexity specific to open banking payments (compared to payments initiated via other payment instruments or digital channels). However, as drafted, the Bill's proposed duties to prevent customer harm applied to open banking payment actions will result in inconsistencies between how open banking payments are processed, compared to how other payments are processed.

We **recommend** that open banking payments should attempt to codify and align with current payments practices (and not create a separate set of duties). Otherwise the customer's rights will differ depending on whether the payment was initiated directly with a bank or via an accredited requestor. If this recommendation is not adopted, there is a risk that open banking payments will have higher levels of regulatory requirements compared to other payment types. This will put open banking payments at a comparative disadvantage compared to other payment types. It will add unnecessary costs to both data holders and accredited requestors, and will add unnecessary customer experience friction.

To avoid operational uncertainty for data holders, there should be greater clarity regarding the grounds on which a data holder can or must refuse to provide data, and any grounds for refusing payments should be consistent with current payment practices

As mentioned, the Bill sets out grounds[9] upon which a data holder '<u>may</u>' refuse to act. However, it is unclear whether there is any obligation on the data holder to be satisfied that these matters are not issues, or whether it applies only in situations where the data holder has express prior knowledge of these matters.

These provisions also specify situations in which a data holder '<u>must not</u>' act – where the data holder has reasonable grounds to believe that the request is made under the threat of physical or mental harm. As currently drafted in the Bill, it is not clear what, if any, positive enquiries a data holder must make, and whether these enquiries differ from existing practices.

It would also be helpful to understand how these obligations:

- will sit alongside existing banker / customer obligations; and
- how they might be impacted by obligations on certain data holders (banks) in relation to vulnerable customers, where it is expected that they have embedded the fair treatment of vulnerable customers in policies and processes throughout the whole customer journey.

This is especially relevant in the context of payment actions initiated under CPD. As mentioned above, it will be important that CPD does not introduce additional and unnecessary complexity specific to open banking payments, compared to payments initiated via other payment instruments or digital channels.

For the protection of customers throughout the data ecosystem, the duty of preventing customer harm should apply to <u>both</u> accredited requestors and data holders

The Bill puts a range of obligations on accredited requestors and data holders. Some of these obligations apply to both accredited requestors and data holders. Other obligations apply either to the data holder, or the accredited requestor.

The Bill currently sets out obligations on the data holder to ensure the protection of the customer. This includes scenarios where a data holder *may* reject a request for data sharing where they have reasonable grounds to believe harm may occur to the customer[10]. Similar protections apply for 'actions' (e.g. making a payment) where the data holder *may* or *must* refuse the action when the data holder reasonably believes that performing the action would be "likely to pose a serious threat to the life, health or safety of any individual"[11] or creates "...significant likelihood of serious financial

[9] See clauses 16 & 20

[10] See clauses 16 & 20

[10] For example, the data holder may reject a request for 'data' in 16 (a) "likely to pose a serious threat to the life, health, or safety of any individual..." and (b) re harassment etc

[11] See clause 20 (1) (a)

harm"[12], or arises as a consequence of *"deception*[13]. Further, the data holder *must* refuse an action requested (e.g. payment) if the holder has reasonable grounds to believe the request is "made under the threat of physical or mental harm"*[14]*.

Notwithstanding the above recommendation to ensure that obligations to prevent customer harm are consistent with current sector practices (especially in relation to payments), we believe that if the Bill does introduce any duties to protect the customer, these duties should fall equally to both the data holder and the accredited requestor throughout the Bill.

The lack of a duty of customer care on the accredited requestor is notable given the way that CPD regulated data services will operate. In all scenarios, the accredited requestor will be actively engaging with the customer. In many cases the accredited requestor may have access to more information than the data holder about the customer's situation and why the customer intends to use a regulated data service, and data holders may receive a request for data sharing or action via an accredited requestor without being made privy to any of the information driving the request.

In order to better foster trust and protect the safety and wellbeing of the customer, we recommend that any duty of customer care introduced (if any) should be a shared duty by both the accredited requestor and the data holder, with respect to the customer that they both have in common.

This recommendation also has a supplementary benefit. The Bill features strong enforceability and consequences for non-compliance, along with customer dispute resolution obligations. As a matter of principle, we believe any consequences and resolution of any customer harm that occurs should fall on the party who was most responsible for it and/or able to prevent that customer harm, irrespective of whether they were the accredited requestor or the data holder. As written in the Bill at present, the only party who could be held responsible for not preventing customer harm under the Bill is the data holder, and this is irrespective of the circumstances. Introducing a shared duty of customer care would help to align any consequences and customer recourse to the party who was best positioned to prevent the harm to the customer.

To ensure the Bill does not introduce unnecessary complexity, cost, or stifle uptake, no changes should be made to the Bill regarding derived data

Introduction

We cannot emphasise enough that the stakes are very high with respect to getting the approach right on derived data. The public policy stance on derived data will be a key determinant of how successful CPD will be. It will determine how data can flow through the ecosystem in accordance with the customer's instruction and authorisation. Poorly designed legislation or regulations risk severely constraining open banking's potential and adding significant cost and delays. In this context, we have provided an expansive analysis of derived data below.

Definition of derived data

[12] See clause 20 (1) (b)
[13] See clause 20 (1) (b)
[13] See clause 20 (1) (c)
[14] See clause 20 (2)

The term "derived data" has been defined in clause 33(3) to mean data that is "wholly or partly derived from— (a) designated customer data; or (b) other derived data", and only in the context of accredited requestors.

While the term "derived data" has a controversial history, most notably its role as a blocker to CDR uptake in Australia, the definition in the Bill is believed to be appropriate in our view and is consistent with the API Centre's Terms and Conditions.

As such, we recommend that no changes are made to the Bill regarding derived data. However, we note that this is an area where great care needs to be taken when forming regulations. In light of this, while we do not make any change recommendations, we believe it is valuable to set out some key considerations on this subject.

Examples of derived data include: credit score (for loan applications), transaction categories (for expense management, budgeting, or loan applications), disclosable income (credit worthiness or responsible lending assessment), net worth (for budgeting or loan applications) and more.

Issues arise when designated data and derived data are treated equally

Derived data sits at the heart of the Australian CDR legislation because derived data is "CDR Data", whether held by a data holder or a requestor. It is data that has been 'wholly or partly derived' from the data set out in the designation instrument, and *"includes information derived from information covered by paragraph (a), information derived from that derived information, and so on.*[15]*"*

Therefore, aside from some exclusions, all rules applicable to CDR data, within the Australian CDR legislation, will apply to both designated data and derived data, equally.

This, in our opinion and experience, is hugely problematic for Australia. Under Australian CDR rules, there are multiple issues that collide, and while derived data is only one component, the sum complexity means that the CDR rules do not provide a general authorisation for a data recipient to disclose CDR data (or derived data) with consumer consent outside of the CDR regulatory regime, although some limited exceptions apply (for example for certain "trusted advisers")[16]. The extent of regulation of derived data under the Australian CDR rules is seen as a key issue inhibiting transition of use cases from screen scraping[17].

Unlike Australian CDR, the Bill before the Committee does not conflate designated customer data and derived data. The draft Bill accurately associates derived data with accredited requestors who:

1. Must keep certain records[18]; and
2. Must adhere to secondary legislation regarding the use, modification, and disclosure[19]

There is consistency between the Bill and current industry practice as described in the API Centre Terms & Conditions (as applicable to open banking) which requires Third Parties to do the following in relation to derived data:

1. obtain consent for its access and use;
2. protect it from unauthorised access;

---

[15] Australia: Treasury Laws Amendment (Consumer Data Right) Act 2019, Subdivision 3, 56AI
[16] Jodi Ross – Chief Risk and Compliance officer (Tiimely), formerly Assistant Secretary, CDR Regulatory frameworks, Australian Treasury
[17] See: https://tiimely.com/news/response-to-screen-scraping-policy-and-regulatory-implications-discussion-paper; Towards safer alternatives – NAB welcomes Government direction in relation to the practice of screen scraping - NAB News
[18] See clause 46(b)(i)
[19] See clause 33(1)

1. delete, destroy or anonymise it (as/when requested by the customer).

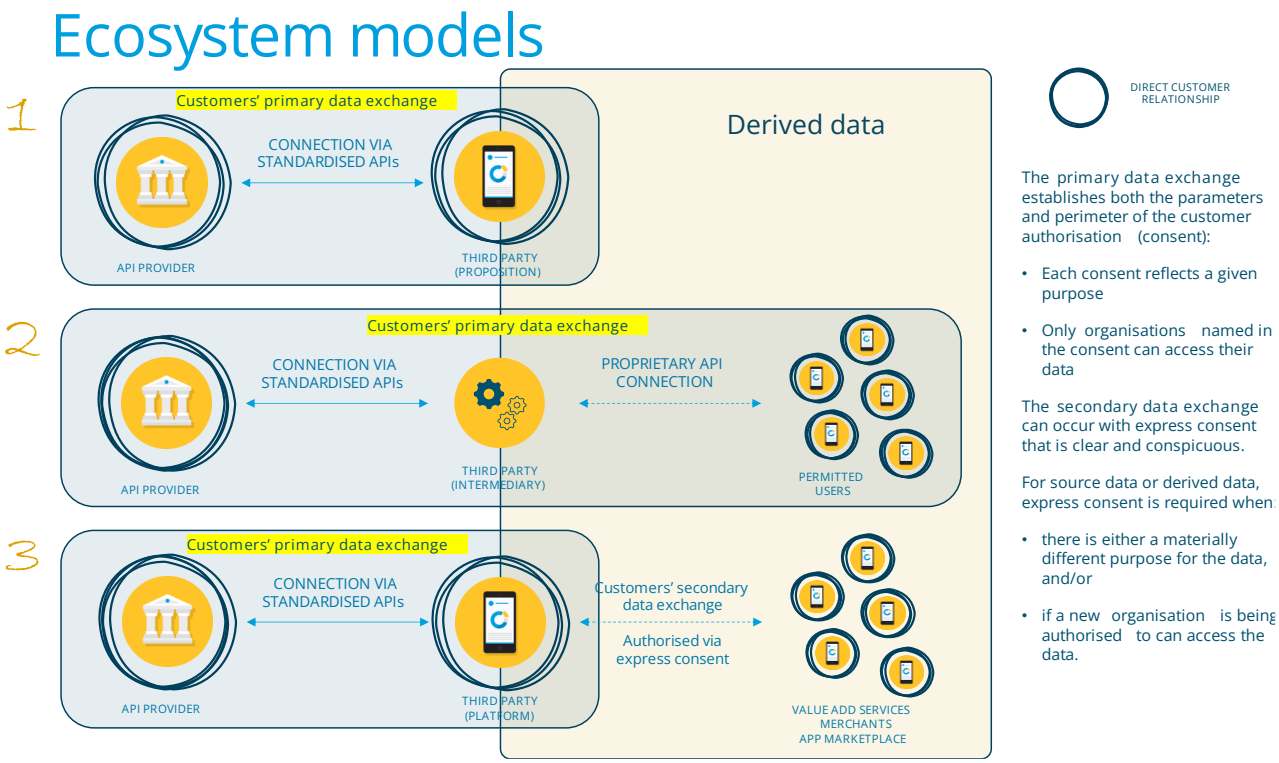
A pathway forward: no change to the Bill

Data, even in the open data ecosystem, is not the end goal. Data is an input in the supply chain and derived data is a natural by-product of a thriving data ecosystem. Put another way, deriving new value from source data is one clear signal that innovation is alive and well. That said, customers must have the right, and the mechanism, to control their data (both designated and derived). Organisations that come into contact with customers data should face strong deterrents from using data modification as way to avoid obligations under CPD.

Therefore, we recommend that secondary legislation takes care to preserve the customer's rights over their data and not unnecessarily inhibit the supply chain of data. However, as mentioned above, great care will need to be applied when establishing these regulations in order to avoid the pitfalls experienced by Australia's CDR. In principle, we must collectively ensure that:

1. Customers can expressly consent to the accredited data requestor sharing their data to other parties (customer has control);
2. Accredited requestors are responsible for accessing and using customers' data solely for the purposes that the customer has authorised (customer trust);
3. Customers data is secure (accredited requests meet security obligations as a condition of their accreditation) (data security);
4. Customers have a mechanism to exercise their right to be forgotten (customer control).

The models below demonstrate ways that data can flow through the ecosystem, according to the customers instruction and authorisation. The Bill does, and should continue to, enable these models including model #3 below where the customer may instruct data to leave the CPD ecosystem to a fourth or fifth party.



Scenario #3 and other on-sharing scenarios have risks

Customers instructing an accredited data requestor to share their data with a non-accredited party has risks. To protect customers, the following mechanisms must be in place:

1. Strong accreditation criteria and suitable penalties to help to protect customers from accredited requestors who may share or use their data in unauthorised ways;
2. A crystal clear definition of "express consent" (authorisation) and the requirement for it to be obtained before sharing or using the customer's data. For example, express consent should mean that the customer is offered a clear, conspicuous, and readily available mechanism to exercise choice (i.e. not hidden in Ts & Cs, a Privacy Notice, or via an "opt out" mechanism which customers may miss if they are not paying attention).

To ensure data can flow between sectors, the Bill should require consideration be given to cross-sector consistency and interoperability

The Bill's preamble discusses the certainty, predictability and interoperability benefits of consistently applying the CPD's framework across multiple sectors. We support this intent.

Over the long term, there will be significant efficiencies if there are consistent approaches across sectors in key areas such as accreditation criteria, customer authorisation practices and key technical practices (e.g. common technical features in API standards). A consistent cross-sector approach supports the interoperability of data and actions between sectors, which in turn will support new innovations.

While we endorse the intent described in the preamble, we note that the Bill itself does not reference the goal of achieving a level of consistency across sectors where that is considered beneficial and practical. We suggest that this stated outcome of consistency between sectors should be included in the Bill.

We acknowledge that this outcome could be achieved through cross-sector coordination of regulations and standards over time. However, we believe that CPD will be better future-proofed if consistency is recorded in the legislation as something that needs to be considered. We consider that a level of consistency between sectors in key areas is achievable while retaining the necessary flexibility for sector-specific regulations and standards to be established.

To avoid uncertainty and ensure appropriate levels of standardisation, there needs to be more clarity on what the mandatory accredited requestors and data holder policies are expected to do

The Bill requires data holders and accredited requestors to have and publish policies on their CPD regulated services in relation to data, products and actions[20]. As drafted it is not clear as to what the purpose of these policies are and what they would need to cover.

Generally, we advocate for standardisation, and individually prepared policies would open the door to non-standardised customer experiences. It is our view that no data holder or accredited requestor

[20] See clause 47

should create policies that may inhibit the efficient access to standardised customer data in accordance with the Bill.

We recommend that organisational policies should only be required on subjects specified in regulations or standards. By way of example, in an open banking payments action context, regulation may require action performance policies that define the following:

a. Payment limits per transaction;

b. Payment limits per day;

c. Customer safety requirements for ecommerce purchases.

We recommend that policies can only be required on matters in relation to CPD if specifically prescribed in CPD regulations or standards.

To ensure there is sufficient flexibility, the Bill should allow for a standard to be made on any CPD subject

The Bill establishes three layers to designate a sector and define its features and requirements, as follows:

1. Legislation sets out the overarching framework, powers, obligations and the scope of what regulations and standards might do;
2. Regulations can be established, for example, with respect to a specific sector. Regulations can be made by the Governor General on the recommendation of the Minister;
3. Following consultation, standards can be approved by the Chief Executive. Should there be any conflict, the regulations prevail over the standards.

The Bill states that the Chief Executive may make standards in order to provide "*... for anything that this Act says must or may be provided for by the standards*[21]*"*. A literal interpretation of these words is that a standard can only be made if the Bill specifies that a standard might be required with regard to the subject of a specified clause.

As such, if a standard is not referenced in the Bill for a given clause or subject, then it may not be possible to make a standard on that subject.

The potential need for both a regulation and a standard is referenced in many instances throughout the Bill, across a wide range of subjects. However, there are also a significantly larger number of references to regulations alone, without any specified reference to a standard being potentially required. Some illustrative examples include:

- Information prescribed in data holder and accredited requestor's annual reports may include statistical information, which we believe is better defined in technical standards[22];
- The operation of the Register may necessitate standards that define how to technically interact with it[23];

[21] See clause 132(1)
[22] See clause 112(2)(b)(ii) and 113(2)(b)(iii)
[23] See 118(2)(b)

- Standards may be required (i.e. not just regulations) for how data holders and accredited requestors deal with joint customers and secondary users (if retained in the legislation)[24].

Our extensive experience in establishing an open banking framework has highlighted the importance of having the flexibility to establish industry standards across a very wide range of subjects. Open banking sector standards will in fact be needed in places where only regulations have been specified.

We recommend that more flexibility is introduced into the Bill for where standards might be created, with the outcome being that the Chief Executive (or recognised standards body as proposed in section 3 of this submission) can make a standard on any subject contemplated within the whole CPD framework. This would avoid limiting standards to just the confines of where the Act specifically says a standard may or must be made.

To ensure designations can be well-scoped, regulations defining a sector's designation should include 'coverage'

The Bill sets out a list[25] of areas that regulations may set out in relation to a sector's designation, as applicable to data, action and product scenarios.

The Bill is relatively non-specific as to what is in the scope of a designation. Generally, we support this approach as it provides flexibility.

However, we consider it important that the 'coverage' of a designation encompasses a critical mass of customers, products and digital channels, so that CPD enabled services can have viable reach and scale. The following outcomes of any designation must be achieved:

- Designation of data, actions, or product should apply to all types and/or categories of customer, unless otherwise specified in a standard;
- Data holders may not seek to unreasonably prohibit access to segments of their customer base through their implementation of regulated data or actions.

As such, we recommend that the Bill is amended to include a provision for the making of regulations setting out the coverage of a sector's designation.

Given the role of the CPD framework in the digital economy, the Bill should have regard to digital inclusion outcomes

The Bill should recognise that the Minister and Chief Executive should have regard to ensuring digital equity and inclusion when proposing regulations or making standards, respectively.

In the right conditions, the market(s) will drive much of the content of the Bill by reacting to market forces. However, should inequities arise the CPD regime should be empowered to prioritise remedies, as needed.

Consulting with Māori is a good start but does not fulfil or exhaust the requirements of digital inclusion, and is not enough. Digital inclusion, the collective rights of Māori, and financial equity are all possible areas for recognition.

---

[24] See clauses 21(2) and (3) for joint customers, and 24(1) and (2) for secondary users
[25] See clause 100(1)

To ensure trust in accredited requestors' systems, the potential for testing electronic systems should cover both data holders and accredited requestors

The Bill includes the ability for the Chief Executive to require a data holder to test their electronic system to verify that it complies with CPD requirements[26].

There are some situations where it could be appropriate for an accredited requestor to also have their systems tested. One example would be testing to verify that the accredited requestor handles or stores CPD data in line with security requirements.

We recommend that the Bill is amended to ensure the Chief Executive may require both data holders and accredited requestors to test their electronic systems.

To avoid unintended loopholes and potential misuse, additional conditions are required around any ability for data holders to refuse a request from an accredited requestor based on debt owed to the data holder

The Bill refers to scenarios where the data holder could refuse a request from an accredited requestor if the accredited requestor owes a debt to the data holder in relation to a CPD regulated data service[27].

We presume that this refers to a scenario where service fees (for access to the regulated services) are charged by the API Provider to the accredited requestor. If this were the case, there would need to be some form of commercial contract in place.

We argue that owing a debt may represent a very low threshold for a data holder to refuse requests made on behalf of customers, especially given the Bill's overarching intent to empower consumers in relation to their data. It raises the possibility of debt offering a legitimate and legal means for data holders to refuse requests for customer data even in cases where debts may be disproportionately small or are not actually overdue.

We recommend that the Bill should be revised to add qualifying context to the nature of a debt that meets the threshold for a data holder to refuse a request from an accredited requestor. It should also be clear that the debt in question must relate solely to fees charged in relation to an accredited requestor's access to the regulated services.

[26] See clause 29

[27] See clauses 16(1)(e) and 20(1)(f)

APPENDIX 2

Definition and analysis of the alternative models for standards development (of open data ecosystems)

Models for Standards development	**1** **Industry ownership**	**2** **Recognition model (Recommended)**	**3** **Regulated model**	**4** **Ministry ownership**
Description	Status quo. Sector and participant led delivery, with no formal regulation.	CPD regime allows for recognised consensus standards to be incorporated under the appropriate conditions, in accordance with the criteria that it sets.	CPD legislation empowers and establishes an entity to develop standards and manage policies & implementation according to a regulatory compliance agenda. e.g. Open Banking Limited, UK	MBIE can prescribe sector standards, policies and technical and operational practices. e.g. Australian Data Standards Body
Strengths	• Direct alignment of standards functionality to market demand • Specialist expertise and knowledge • Very low cost to Government • Balancing governance and decision-making processes with data holder and data requestor incentives Industry consensus	• Effective use of Government and private sector money • Sustainable, for decades to come • Flexible to apply across all sectors • More likely to maintain existing industry momentum (open banking) • Easy to move to a regulated model, if needed • Works closely with sector experts to design standards with in-demand features, resulting in more innovative and viable products • Ministry sets backstop regulations while retaining power to intervene as needed	• Establishes clear authority and mandate to manage standards and delivery • Ensures technical and operational specialist skills are in-house and able to align to delivery milestones	• Centralisation of regulation, standards and setting delivery milestones all in one body

(Table continues overleaf)

Models for Standards development	**1** **Industry ownership**	**2** **Recognition model (Recommended)**	**3** **Regulated model**	**4** **Ministry ownership**
Weaknesses	• Compliance & enforcement tools	• Risk of standards being 'cherry picked' or not wholly adopted as a regulated standard, undermining whole sector standards proposition	• Little ability to do innovative things beyond minimum compliance (key UK finding) • High cost to Government and private sectors	• Hard to wind back or move to other models • Hard to maintain pace with industry and technology change • Ministry must remain 'hands on' in detailed design, technical and industry operations • High operational costs for Government • High industry costs for solutions that may not align to market demand or not easily compatible with market practices • Dependency on scarce subject-matter expertise across a number of sectors • Risk of withdrawing expertise away from the sector