paymentsnz®

Consultation on exposure draft of open banking regulations under the Customer and Product Data Act

Payments NZ Limited submission

29 August 2025

Introduction

Payments NZ Limited (Payments NZ) welcomes the opportunity to make a submission to the Ministry of Business, Innovation and Employment Hīkina Whakatutuki (MBIE) on the Consultation on the exposure draft of open banking regulations under the Customer and Product Data Act, released on 15 August 2025.

Payments NZ's API Centre has led open banking in Aotearoa New Zealand, in conjunction with industry stakeholders, since its establishment in 2019. We have always shared with regulators the goal of seeing open banking thriving. Given the considerable progress achieved by the API Centre, together with the introduction of the Customer and Product Data Act 2025 ("the Act") and the forthcoming designation of the banking sector, we believe Aotearoa is well placed to see strong growth in the open banking ecosystem and to deliver real benefits for New Zealanders. We remain committed to playing our leadership role in open banking in Aotearoa and driving these positive outcomes.

The regulations that designate the banking sector are a critical component of the future open banking ecosystem. We support the regulations drawing extensively from our existing open banking standards. We consider it paramount that the regulations align with existing standards and market practices – particularly given designated Data Holders and Accredited Requestors will be required to comply with the regulations, once finalised, in only three months. In this context, the Payments NZ and API Centre team have put considerable effort into compiling this submission since this consultation was released two weeks ago.

We support, in principle, the API Centre's Standards being incorporated by reference under the Act and we look forward to continuing our engagement with MBIE on the arrangements for facilitating this. Our submission assumes the API Centre's Standards will be incorporated by reference, and focuses particularly on the relationship between the regulations and the standards. In this submission, we refer to "**API Centre Standards**" (which have been incorporated by reference as a standard under the Act) as a "**regulatory standard**".

Our submission contains the following main sections:

- Part A: key messages
- Part B: regulations and the API standards
- Part C: accreditation
- Part D: liability.

PART A: KEY MESSAGES

The following summarises our key messages:

1. The API Centre is dedicated to maintaining industry and regulatory momentum during the implementation of the Act. We advocate for public and private sector collaboration to achieve regulatory certainty swiftly.
2. For data holders to be compliant on 1 December 2025, regulations must align with v2.3 API Centre Standards. This can be achieved through amendment to the draft regulations.
3. Designated 'relevant accounts' include account product types that are not required by v2.3 of the API Centre Standards. To avoid material compliance issues on 1 December 2025, the regulations should be amended to align with the API Centre Standards.
4. There are instances of divergence between the regulations and the API Centre Standards. For a seamless commencement of the regulations on 1 December 2025, the regulations need to be aligned to the API Centre Standards.
5. The introduction of the giving of written notice to customers about long lived authorisations requires detailed industry consideration of customer safety and consistency of outcomes before it is introduced as a regulation.
6. The regulations covering the accreditation of requestors have materially significant gaps that need to be addressed.
7. The regulations should describe what security safeguards are required as an accreditation requirement.
8. The regulation on dispute resolution is appropriate for now, but in time, all open banking customers should be able to access independent dispute resolution services.
9. The regulations on intermediaries are unnecessarily ambiguous and amendments are required to ensure more certain outcomes.
10. We believe the proposed five-day onboarding timeframe could be achieved, in time. However, expecting to meet this timeframe by 1 December 2025 is unrealistic. Transitionary accommodations are necessary to establish the required supporting processes and capabilities.
11. The lack of information and certainty with respect to how liability will be managed needs to be resolved for open banking to succeed under the Act.

PART B: REGULATIONS AND THE API STANDARDS

1. Regulatory certainty to maintain momentum

The API Centre is dedicated to maintaining industry and regulatory momentum during the implementation of the Act. We advocate for public and private sector collaboration to achieve regulatory certainty swiftly.

We acknowledge that the regulatory regime under the Act is being introduced at pace. These regulations, once finalised, will provide another important pillar of regulated open banking. We welcome this momentum. We also acknowledge that the regulatory regime under the Act will not be fully formed on 1 December 2025 and there will be further regulatory matters to implement and work through into 2026.

Concurrently, industry has also maintained significant momentum. The API Centre has recently:

- published five new operational standards.[1]
- published our Ngā Tohu Ārahi data handling guidelines.[2]
- updated our customer experience guidelines[3].

We are working towards the release of our performance standard this year.

The v2.3 Payments Initiation API Centre Standard was implemented by the four major API Providers in May 2025, adding significant functionality for open banking fintechs and paytechs to the earlier v2.1 Standard implemented last year. The v2.3 Account Initiation API Centre Standard is also on track for implementation by 30 November 2025.

Despite the progress of both industry and regulation, we need greater regulatory certainty to ensure that momentum is maintained. For example, it is unclear when the following will be available:

- Accreditation requirements for Accredited Requestors.
- Onboarding process and requirements for Accredited Requestors and Data Holders.
- Incorporation of API Centre Standards under the Act, and the process for making regulatory standards (i.e. specifying APIs standards, customer authorisation and disclosures, reporting and more).
- Details in relation to fees and levies.
- Operational details for the criteria and application processes for exemptions.

Recommendation

We recognise these matters are likely to be transitionary and short-lived challenges. To ease the burden of uncertainty in the short term, we recommend that MBIE makes a transition plan publicly available, with phased target dates showing when each of the gaps in the regime (above), as well as the additional scope items proposed in the exposure draft, will be resolved.

[1] See Operational Standards - Payments NZ API standards - Confluence
[2] See Ngā Tohu Ārahi - API Centre data handling guidelines - Payments NZ API standards - Confluence
[3] See Customer Experience Guidelines v3.0 - Payments NZ API standards - Confluence

2. Alignment of regulations and API Centre Standards

For Data Holders to be compliant on 1 December 2025, regulations must align with v2.3 API Centre Standards. This can be achieved through amendment to the draft regulations.

Once an API Centre Standard is incorporated by reference into a standard under the Act, the resulting regulatory standard will provide the means for Data Holders and Accredited Requestors to comply with relevant parts of the Act and the regulations. However, we note that if there is inconsistency between the regulatory standard and the regulations, the regulations will prevail[4].

As such, Data Holders and Accredited Requestors have a legal obligation to meet the requirements prescribed in the regulations, irrespective of the regulatory standards. Some of our API Providers (who will become designated Data Holders) have built their platforms to comply with v2.3 API Centre Standards. In this context, any variation between the regulations and v2.3 API Centre Standards which have been (or are soon to be) implemented by Data Holders and Accredited Requestors creates a material risk of the regulations not being complied with on 1 December 2025.

Currently, there are material variations between the draft regulations and the existing v2.3 API Centre Standards. Sections 3 – 5 of this submission explains these variations.

Recommendation

Given the tight timeline and the intention of the regulations to utilise industry work to date, our view is that there should not be any variation between the regulations and the v2.3 API Centre Standards. Accordingly, we recommend that all variations are resolved by making amendments to the draft regulations, as set out in sections 3 - 5 of this submission.

3. Account and Product Types

Designated 'relevant accounts' include account product types that are not required by v2.3 of the API Centre Standards. To avoid material compliance issues on 1 December 2025, the regulations should be amended to align with the API Centre Standards.

The account product types that are proposed to be designated as 'relevant accounts' in the draft regulations[5] go beyond the scope of the API Centre Standards. We recommend that the regulations be aligned with the account types specified in the API Standards, noting that these account types were implemented in 2024 by the API Providers who will become designated Data Holders.

If these amendments to the regulations are not made, the following adverse impacts could occur:

- designated Data Holders may be unable to comply with all requirements in the regulations by 1 December 2025, as they will have insufficient time and certainty to operationalise new functionality; and

[4] Clause 138 (2) of the Act states "*If the standards are inconsistent with the regulations, the regulations prevail to the extent of the inconsistency*".

[5] See clause 7(3) of the Banking and Deposit Taking draft regulations

- because additional account types have not been through the industry co-design process to properly consider whether the data structures are needed to support that product or account type, Data Holders may implement in non-standard ways.

If the API Centre were to begin work to amend a future API Centre Standard (e.g. v3.x) to accommodate additional account product types, this work will not be completed before 1 December 2025. Further, if this work were undertaken, it may carry an opportunity cost as it would displace other potentially higher priority upgrades to the API Centre Standards.

Account Information API Centre Standards (for designated data)

Some financial products covered by the draft regulations are not covered by the current Account Information API Centre Standards and implementations, including: notice accounts[6], fixed term deposits[7], call and term PIE accounts[8] and bank perpetual preference shares[9].

The inclusion of an account relating to a credit contract as defined under section 7 of the Credit Contracts and Consumer Finance Act 2003 ("CCCFA") in the definition of a relevant account for designated data is broader than the API Centre Standards[10]. The API Centre Standards prescribe that in scope lending accounts are either Bulk Electronic Clearing System ("BECS") identifiable[11], or are a credit card account. Given the broad definition of a credit contract under the CCCFA, we expect there will be credit contracts which do not relate to credit cards and which are not associated with BECS identifiable accounts (i.e. outside the scope of the standards), but which are in the scope of the regulation.

We have not commented on the relevant accounts under regulation 7 relating to credit unions and building societies, since no credit unions or building societies are in the scope of the designation.

Recommendation (designated data)

We recommend the scope of relevant account types for designated data regulations[12] is limited to:

1. section 44 (1A) (c) (a call debt security) of Schedule 8 of the Financial Markets Conduct Regulations 2014; and
2. accounts relating to a credit contract as defined under section 7 of the CCCFA that are Credit Cards or BECS identifiable.

[6] Financial Markets Conduct Regulations 2014, sch 8, clause 44(1A)(a)
[7] Financial Markets Conduct Regulations 2014, sch 8, clause 44(1A)(d)
[8] Financial Markets Conduct Regulations 2014, sch 8, clause 44(1A)(f)-(g)
[9] Financial Markets Conduct Regulations 2014, sch 8, clause 44(1A)(h)
[10] See clause 7 (3) (a) (iv) of the Banking and Deposit Taking draft regulations
[11] BECS identifiable accounts are account numbers following the bank-branch-account-suffix format, e.g. 12-1234-1234567-12
[12] See clause 7 (3) (a) (i) of the Banking and Deposit Taking draft regulations

4. Relationship between regulations and API Centre Standards

There are cases of divergence between the regulations and the API Centre Standards. For a seamless commencement of the regulations on 1 December 2025, the regulations need to be aligned to the API Centre Standards.

Optionality within the API Centre Standards, particularly regarding data points and response fields, is a crucial aspect that makes these standards efficient and workable. This is a best practice approach for API Standards design to enable the conditionality and flexibility necessary to accommodate a wide range of customer scenarios and the diverse range of data that is available across different account types. Many of the optional data fields cannot or should not be made mandatory for this reason.

This means in practice that:

- if the data in relation to an optional response field does not exist, it will not be populated; and
- if the data in relation to an optional response field does exist, our guidance encourages API Providers to return the data in a manner reflecting data available in its online/mobile banking channels.

Recommendation (handling data optionality)

We recommend that the regulations reinforce API Centre guidance on this issue, and specifically that the regulations ensure that:

- if the data in relation to an optional response field does not exist, it will not be populated;
- if the data in relation to an optional response field does exist, Data Holders should respond in a manner reflecting data available in its online/mobile banking channels; and
- transitionary arrangements are considered to facilitate the above.

Further recommendations to ensure alignment with v2.3 API Centre Standards

- The regulations[13] should not require data that describes how balances are calculated because:
    - the definition of balance types is documented in the API Centre Standards; and
    - balance types are consistent for all customers and accounts, i.e. they are not defined and described on a per-account or per-customer basis.
- The minimum time period for returning historical transaction particulars should be removed from regulations for 1 December 2025 so that further research can be undertaken to determine what is reasonable and feasible. This research should include understanding the impacts on system capacity, e.g. for some business customers, two years of data may be a significant volume of data that will consume capacity of the system, and Data Holder data retrieval capabilities. As noted earlier in our submission, consideration could be given to a transition period where some proposed requirements are delivered at a later date.
- We recommend the regulations should designate classes of data in line with the API Centre Standards resources, i.e. Accounts, Balance, Transactions, Statements and Party to remove ambiguity, and that detailed matters are better managed via the incorporation of standards. Note:
    - We believe the regulations for designated customer data are too detailed. This level of detail is unnecessary and creates unintended consequences.

[13] Refer 7 (1) (c) (iii) of the Banking and Deposit Taking draft regulations

- Further, the level of detail is internally inconsistent across the various data topics. For example, there is significantly more detail in relation to statements[14] than other designated data topics.
- The draft regulation on statements is selective as it lists some, but not all, data points contained in the API Centre Standards[15].

- The introduction of regulations[16] in relation to open banking payment limits is a potential implementation risk, as the regulations may not align with how Data Holders currently manage payment limits in relation to their digital channels, account types and customers. As noted earlier in our submission, consideration should be given to a transition period where some proposed requirements are delivered at a later date.

A note on exemptions

The proposed regulation scope creates a risk that Data Holders will be unable to comply with requirements on 1 December 2025. The exemptions regime under the Act could be used to exempt Data Holders from compliance with regulatory requirements which diverge from existing API Centre Standards, although we note any such exemption must be granted prior to 1 December 2025 to avoid regulatory compliance breaches and it could be challenging to meet this timeline.

5. Customer notifications

The introduction of the giving of written notice to customers about long lived authorisations requires detailed industry consideration of customer safety and consistency of outcomes before it is introduced as a regulation.

The regulations introduce a new requirement for an Accredited Requestor to notify customers in relation to any active enduring authorisations[17]. While we acknowledge the intent of the regulation is to ensure customers are periodically prompted to review their consents, we have the following material concerns that will likely erode any benefits of the regulation:

- Customer notifications will introduce a new fraud vector that will put customers at risk. This requires careful thought to set out how an Accredited Requestor must implement effective and safe customer notifications.
- If this level of detail (i.e. the 'how') is not set from 'day 1', it will cause re-work for Accredited Requestors.
- The pool of Accredited Requestors will continue to grow over time, increasing the likelihood of variable customer experiences and low customer muscle memory.

Recommendation

If MBIE wishes to pursue this feature, we believe that it will be necessary to work with industry (through the API Centre working groups) to develop a safe, impactful and consistent customer

[14] Refer 7 (1) (e) of the Banking and Deposit Taking draft regulations
[15] For example, 7 (2) directly copies the 13 of the 22 Codes in the Statement Amount Type standard, but, for unknown reasons, omits the remaining codes.
[16] Refer 8 (3) of the Banking and Deposit Taking draft regulations
[17] See clause 10 of the General Requirements draft regulations

experience. We recommend that this work is set out in the 'transition plan' recommended in section 1 of this submission.

We also suggest that this work should consider who is best placed to provide these notices (i.e. Data Holders and/or Accredited Requestors) to ensure the best outcomes for customers and keep them safe.

Given the proposed work with the industry will likely change the content of any regulation, we recommend that regulation 10 of the General Requirements draft regulations should be removed from the initial regulations and be considered for implementation after 1 December 2025.

PART C: ACCREDITATION

6. Accreditation requirements

The regulations covering the accreditation of requestors have materially significant gaps that need to be addressed.

The regulations set out the criteria that need to be satisfied in order for the Chief Executive to accredit requestors. The API Centre has been conducting the Accreditation and Partnering project through a working group comprised of 16 Third Party Standards User organisations (potential future Accredited Requestors) and five API Providers (all future designated Data Holders) ("the working group"). Based on this work, we believe the accreditation criteria in the draft regulations has materially important gaps.

We address the absence of any security safeguards in the regulations separately in the section immediately below.

We **recommend** that any applicant is screened to confirm it:

- is not a designated entity under the Terrorism Suppression Act 2002 or Russia Sanctions Act 2022;
- is not subject to UN sanctions; and
- has no history of financial crime.

We **recommend** that accreditation should consider scenarios where the applicant is not supervised under a New Zealand regulatory regime and is a payment service provider whose business model includes acting as a funds handling agent (where they temporarily hold the money on behalf of other customers). While the working group preferred that creditworthiness should generally not be a factor for accreditation, the scenario where the customer is exposed to settlement risk needs considering in the accreditation process.

We **recommend** that an 'absence of negatives' test is applied to ensure that there is no reason to suspect that the applicant will materially undermine the integrity or reputation of the open banking ecosystem, the Act, or any other Data Holder or Accredited Requestor. The applicant should provide supporting information to inform this test, including:

- type of organisation (e.g. New Zealand incorporated company),
- ownership structure (including the interests of any overseas entities),
- type of business (e.g. the sector and a description of key services provided), and

- a description of the applicant's governance structures, particularly in relation to the provision of open banking services.

7. Security accreditation requirements

The regulations should describe what security safeguards are required as an accreditation requirement.

We note that while the Act[18] includes a general requirement for an applicant to have adequate security safeguards in relation to data, there are no draft regulations that support the Act in relation to what the applicant's security safeguards are.

The high-level requirements in the Act, on their own, do not provide the necessary clarity for applicants on how a customer's data must be safeguarded. We believe the lack of accreditation requirements in relation to security safeguards falls short of the Act where the Minister must give regard to the likely benefits and risks associated with any proposed designation regulations in relation to the security of customer data[19]. The lack of security safeguards accreditation regulations also appears to be internally inconsistent compared to other accreditation subjects (for example, compared to accreditation regulations in relation to good character, dispute resolutions or intermediaries).

We support the draft regulations[20] requiring an applicant who wishes to act as an intermediary to provide reasonable assurance that those who they provide an intermediary service to, such as a merchant or a fourth party, have adequate security safeguards in relation to data and/or transactions. We believe that the regulations need to also specify what the adequate safeguards are for the applicant as well, and that the same security safeguards need to be applied to both data and payment scenarios.

Recommendation

We recommend that regulations should underpin the Act by setting out general accreditation requirements applicable to all applicants. The API Centre's Standards Users, via the working group, have invested a significant amount of time and resource to develop proposed security accreditation requirements for open banking. We recommend that MBIE adopt the working group's recommended accreditation security requirements and reflect these in the regulations.

8. Customer dispute resolution

The regulation on dispute resolution is appropriate for now, but in time, all open banking customers should be able to access independent dispute resolution services.

We believe the regulation[21] regarding customer dispute resolution is broadly appropriate given current dispute resolution schemes and financial service provider regulations in Aotearoa.

[18] Refer section 112(2)(c) of the Act
[19] See section 105 (1) (d) of the Act
[20] See clauses 14 (b) (i) and (ii) of the General Requirements draft regulations
[21] See clause 12 of the General Requirements draft regulations

However, while this may be appropriate for now, we do not consider this to be an ideal situation in the longer term. We **recommend**, in line with the findings of the working group, that actions should be taken over time to ensure that **every** open banking customer has access to a recognised independent dispute resolution scheme or equivalent, and that there is consistency with respect to how all open banking disputes are resolved. We recommend this on the basis that:

- not all open banking customers will have access to independent dispute resolution services;
- open banking disputes will be managed in several different places, with no guarantee of consistent dispute resolution outcomes across these different places; and
- it may not always be clear, particularly to the customer, whether an open banking dispute is best managed via Data Holder or Accredited Requestor dispute resolution mechanisms, or indeed how to best resolve a customer dispute that includes both a Data Holder and an Accredited Requestors.

9. Intermediary class of accreditation

The regulations on intermediaries are unnecessarily ambiguous, and amendments are required to ensure more certain outcomes.

In line with the findings of the working group, we support establishing an intermediary class of accreditation.

We believe that the regulations currently introduce unnecessary ambiguity and that amendments are required to ensure a more certain outcome.

In practice, a customer may authorise an Accredited Requestor to access their bank account information data or initiate payments on their behalf. Subsequently, and in relation to data only, the customer may grant a separate authorisation to subsequently share their data held by the Accredited Requestor. These two events are authorised separately by the customer where:

- the first event is authorised by the customer and is facilitated in accordance with the API Centre Standards.
- the subsequent event (commonly referred to as "on-sharing") is outside the scope of regulated open banking[22].

Recommendation

We are unclear why "mainly"[23] has been included in the draft regulations and recommend that this be deleted because it creates ambiguity about how requests are limited to the customer's authorisation.

We also note that the example set out in 9(3) of the regulations may be misinterpreted and we recommend the emphasis that **subsequent** services to Party B is conducted under a **subsequent** customer consent.

[22] Refer section 11 below for further information on this

[23] See clause 9 (3) (a) of the Banking and Deposit Taking draft regulations

10. Accredited Requestor onboarding

We believe the proposed five-day onboarding timeframe could be achieved, in time. However, expecting to meet this timeframe by 1 December 2025 is unrealistic. Transitionary accommodations are necessary to establish the required supporting processes and capabilities.

We strongly support achieving an efficient and timely process for an Accredited Requestor to be onboarded with every Data Holder. Ensuring process and timeline certainty is crucial for encouraging potential Accredited Requestors to commit, which will in turn help the open banking ecosystem to thrive.

For onboarding to a Data Holder, there are three distinct phases:

- Completion of Accreditation (pre-requisite)
- Onboarding to the Data Holder business (including business contacts etc)
- Onboarding to the Data Holder platforms and specific API testing and production access (Technical)

To our knowledge, achieving business and technical onboarding in this timeframe for access to the Data Holder's system would give Aotearoa the fastest open banking onboarding process in the world and far exceed the integration timeframes for connecting new API services into the Data Holder's own internal channels. However, while this may be an appropriate goal for the sector, we believe achieving this ambitious timeframe from 1 December 2025 is unrealistic and imposes risk.

Globally, it is best API onboarding practice for API requestors to satisfy requirements before they can be granted access to an organisation's production systems. In the case of regulated open banking in Aotearoa, these requirements may include being onboarded onto the trust platform, providing their certificates and other credentials, accessing the sandbox, completing pre-prod testing, and then production verification. Subject to the integration maturity of the Accredited Requestor and quality of Data Holder supporting documentation and support resource availability, it can involve numerous active interactions between the Accredited Requestor and Data Holder. We consider it unrealistic to achieve this within the proposed five-day timeframe from 1 December 2025. We believe that consistently achieving a five-day onboarding timeframe will require:

- all test disciplines, operational standards (i.e. procedures for interactions), and supporting technical automation tools to have been developed and put in place; and
- these to have been optimised to address any initial lessons learned.

We also anticipate higher capacity demands from the (expected) larger batch of Accredited Requestors undergoing onboarding processes from December 2025, and this will occur at a time where the supporting onboarding processes are less mature and scalable.

Recommendation

We recommend that the regulations provide transitionary accommodations to allow for the necessary supporting processes to be put in place.

The regulations will play an important role in creating the preconditions for achieving an optimal onboarding timeframe. We **recommend** the following improvements to the draft regulations:

- Provide clarity in relation to the Accredited Requestor giving the notice to each respective Data Holder[24] to commence the timeframe.
- Recognise that the Data Holder will need to be actively involved in the testing and production migration process beyond just providing "information", as described in the current draft regulations[25].
- Provide certainty as to what happens to the timeframes if Accredited Requestor requirements are not satisfied (i.e. is the timeline paused?).

PART D: LIABILITY

11. Liability

The lack of information and certainty with respect to how liability will be managed needs to be resolved for open banking to succeed under the Act.

Currently, liability matters are managed via bilateral contract arrangements between an API Provider and a Third Party. MBIE has communicated that the regime under the Act will "remove the need for bilateral contracts between banks and data requestors[26]".

We note that section 58 of the Act contemplates that where a Data holder or Accredited Requestor contravenes the Act, they will be required to take steps, prescribed by the regulations, to avoid, mitigate, or remedy loss or damage caused by the contravention. We note that the regulations appear to be silent on these steps. We also note that the right of a person who has suffered loss or damage to recover the amount as debt due (in section 59) will not apply as no regulations have been made for the purposes of section 58.

The draft regulations are silent on the allocation of liability (although we note the defences set out at sections 89 – 91 of the Act).

In the absence of any other information, we assume that this is because the intention is to rely on liability regimes set out in other legislation (e.g. the Privacy Act) and the terms of customer contracts in the event of any issues. However, the operation of these other liability regimes, in combination with the defences set out in the Act, may lead to:

- poor customer outcomes in the event of a customer loss caused by an open banking related issue,
- uncertainty in relation to who is liable for any customer losses,
- uncertainty regarding the liabilities intermediaries may have, if any, for the actions of the parties to whom they provide services, and
- unintended consequences arising from not clearly addressing liability within the framework of the Act.

We also believe that the regulations should provide absolute certainty in relation to the perimeter of regulated open banking. This should make it clear that any subsequent data on-sharing arrangement

[24] See clause 6 (2) of the General Requirements draft regulations
[25] See clause 6 (2) (b) of the General Requirements draft regulations
[26] Refer page 2 Fact Sheet - Open banking regulations.pdf

or payment made following the initial customer-consented open banking action using API Centre Standards is beyond the open banking and regulatory perimeter. Having this certainty would provide the basis that liability arising from subsequent actions cannot then flow back, or be attributed, to Data Holders in the regulated open banking ecosystem.

Providing certainty to the market on liability matters will be critical to the success of open banking under the Act. Given there is very little information on how the regime under the Act will manage and allocate liability in open banking, we believe it would be beneficial if MBIE communicated how liability will be managed, including what role (if any) regulations will play. If liability management and allocation is to be left to the market to manage, then this should be made clear by MBIE.

Ngā mihi,

Steve Wiggins
Chief Executive
Payments NZ