
Consultation on proposal to recommend designation of the interbank payment network

Payments NZ Limited submission

May 2024

1. Introduction

This submission is made in response to the Commerce Commission Te Komihana Tauhokohoko (the Commission) consultation on its proposal to recommend designation of the interbank payment network (published on 27 March 2024). This designation is proposed under the Retail Payment System Act 2022 (RPS Act).

In our submission, it is our preference to provide a general response instead of specifically addressing the consultation questions on pages 50 to 54 of the consultation document. Given the overlapping nature of the various issues with other Commission consultations and communications, this submission also responds to the Commission on:

- its draft market study report on personal banking services (published on 21 March 2024) in relation to open banking and the role of Payments NZ and the API Centre; and
- its open letter to participants of New Zealand's retail payment system (published on 22 February 2024).

Payments NZ is pleased to see the recognition of its role as the governing body leading the development and management of network rules for open banking. We are encouraged to see that the considerable industry work on open banking is recognised and would form the basis of any potential future regulation. The Commission has the expectation that industry will continue to lead the development of the API ecosystem and we also support that view.

Payments NZ supports the outcomes that the Commission is setting out to achieve. Those outcomes broadly align with the objectives of our API Centre framework and strategy. However, we do not support the designation of the full interbank payments network for the reasons set out in this submission and in our previous submission to the Commission in September 2023. Should the Commission seek a designation, Payments NZ has reservations about the current approach and its proposed scope. However, we do believe that our reservations can be easily addressed and resolved. Further, should a designation eventuate, it is our view that any resulting exercise of powers should be judiciously used only as a regulatory backstop to reinforce industry momentum and to provide a temporary bridge until the Customer and Product Data (CPD) legislation is fully effective.

In our submission we have put forward key messages, made specific recommendations to improve a potential designation, and have provided supporting rationale. For ease of reference, the key messages and recommendations are summarised in sections 2 and 3 respectively, with the supporting rationale set out in section 4. In section 5, we respond generally to the Commission's views and expectations regarding Payments NZ and the API Centre.

Should the Commission determine that a designation is appropriate, we propose that the Commission carefully consider our recommendations to ensure that the scope of that designation is well-designed and better aligned to the outcomes the Commission wants to achieve.

2. Our key messages

Payments NZ's key messages:

Key messages from our submission are summarised below:

1. The Commission has a unique opportunity to support industry and market efforts to improve consumer choice.
2. The proposed designation scope is too expansive with the inclusion of BECS and account information, but it is not comprehensive enough due to the omission of impersonated access.
3. Any designation should focus on retail payments only and not on the full interbank payments network.
4. Designating all BECS payment instruments goes well beyond what is needed to address the Commission's concerns.
5. The scope of any designation should be limited to the relevant functions and payments standards of the API Centre.
6. Impersonated access methods should be included in any designation.
7. Any exercise of powers should include the phasing out of impersonated access methods and a transition to secure and compliant standardised API access methods.
8. Other overlapping payments regulation should prevail over the Commission's designation of retail payments.
9. Any regulatory backstop should reinforce industry momentum and provide a temporary bridge to CPD legislation.
10. The Commission considers adopting our approach for drafting the designation scope statement, which could assist the practical application of any designation.
11. Payments NZ and our API Centre are committed to working towards the Commission's expectations in relation to increasing transparency and meeting the future needs of payments and open banking.

3. Summary of Payments NZ's recommendations:

Payments NZ's recommendations to the Commission are as follows:

1. That the Commission gives particular weight and attention to Payments NZ's submission and its recommendations.
2. That the proposed designation scope makes significant adjustments to ensure that it aligns it with the Commission's policy objectives and the Commission's powers.
3. That any designation focuses on retail payments, and that the full interbank payments network should not be designated.
4. That the Commission only designates specific Bulk Electronic Clearing System (BECS) payment instruments in relation to their usage in retail payment use cases.
5. That only the Direct Credit payment instrument be designated and only for when it is used in retail payment use cases.
6. That any designation of standardised APIs should relate solely to payments.
7. That the draft designation delineates more clearly between the designation of the API Centre's role and the role of BECS.
8. That the Commission changes its terminology and uses "impersonated access" instead of "sub-optimal methods".
9. That, as an initial step, impersonated access methods are designated.
10. That the Commission considers exercising its potential powers to phase out impersonated access methods and require a transition to standardised API access methods.
11. That any designation should explicitly state that it yields to any overlapping regimes such as the Financial Market Infrastructures Act 2021 (FMI Act) or the CPD legislation.
12. That any designation and resulting exercise of powers should act as a bridge to CPD only, and then step back.
13. That the duration of the Commission's designation should only be 5 years, to better align with CDP.
14. That the Commission only exercise its powers (if designation proceeds) to act as a regulatory backstop to reinforce industry momentum and bridge to CPD.
15. That the Commission gives serious consideration to adopting our proposed approach for drafting the designation scope statement (if designation proceeds).

4. Payments NZ's Submission

The Commission has a unique opportunity to support industry and market efforts to improve consumer choice

1. We recommend that the Commission gives particular weight and attention to Payments NZ's submission and its recommendations.

Payments NZ sets the rules and standards for the payment system and, through its work in establishing and operating the API Centre, has considerable expertise and experience in open banking. We are well placed to inform and contribute to what is needed in the future. We very much share the same goal in relation to a thriving API enabled payment ecosystem.

In this context, we ask the Commission to give particular consideration to Payments NZ's submission. Our submission draws from our expertise and experience, and the lessons we have learned covering a wide range of issues in payments and open banking. Our submission is put forward constructively to ensure that, if designation proceeds, it is well designed. Further, as the scope of the draft designation includes Payments NZ as an operator, these proposals are particularly relevant to the work we do.

As stated in the introduction, while we support the outcomes that the Commission is striving for, we do not support the designation of the whole interbank payments network. Our reasons for not supporting designation are set out in our September 2023 submission to the Commission.

However, if designation does proceed, then we think an outcome-focused regulatory backstop could have some utility if it is well designed and in line with its empowering legislation. This regulatory backstop could reinforce industry momentum and play an important role contributing to a flourishing open banking environment in Aotearoa New Zealand.

We share the Commission's aspiration to get open banking up and running, and to encourage this to happen as quickly as possible. We do, however, have concerns over the shape and form of the proposed designation. We consider that these can be easily overcome and have set out our views on how this can be achieved, together with a series of recommendations in the following sections.

The proposed designation scope is too expansive with the inclusion of BECS and account information, while it is not comprehensive enough due to the omission of impersonated access.

2. We recommend that the proposed designation scope makes significant adjustments to ensure that it aligns it with the Commission's policy objectives and the Commission's powers.

Payments NZ considers the exact nature and scope of what the Commission proposes to designate is of paramount importance even if, as noted in the consultation document, the Commission decides not to exercise any of its powers. In this submission, we put a major focus on the content of the proposed designation and recommend important improvements to ensure that its scope can be considered 'well-designed and clear'.

If there is to be a designation, it needs to be better focused and more aligned to resolving the issues raised by the Commission. It is our view that, currently, there is a significant disconnect between:

- the issues and concerns raised by the Commission with respect to achieving a "thriving API enabled payment ecosystem";
- the scope of the Commission's proposed designation; and
- the Commission's powers under the RPS Act.

We are of the view that the proposed scope of designation is simultaneously too broad and not broad enough. The proposed scope encompasses large areas of the payments system that are not relevant to retail payments, open banking, the issues highlighted by the Commission, or the Commission's powers under the RPS Act. On the other hand, the proposed scope could go further to state that (customer) impersonation access methods are included in the proposed designation.

Any designation should focus on retail payments only and not on the interbank payments network

- | |
|--|
| <p>3. We recommend that any designation focuses on retail payments, and that the full interbank payments network should not be designated.</p> |
|--|

The Commission is proposing to designate the "interbank payment network". This term is not used in the RPS Act, the FMI Act or internationally (for example the Principles for Financial Market Infrastructures issued by the Committee on Payments and Market Infrastructures and IOSCO). Payments NZ drew attention to this in our earlier submission dated 25 September 2023.

The term "retail payment" is used in the RPS Act and retail payment is defined as a payment by a consumer to a merchant for the supply of goods or services. The Commission will therefore be limited to payments of this nature when acting under the legislation. Accordingly, we do not believe the Commission has a mandate over the entire interbank payments network.

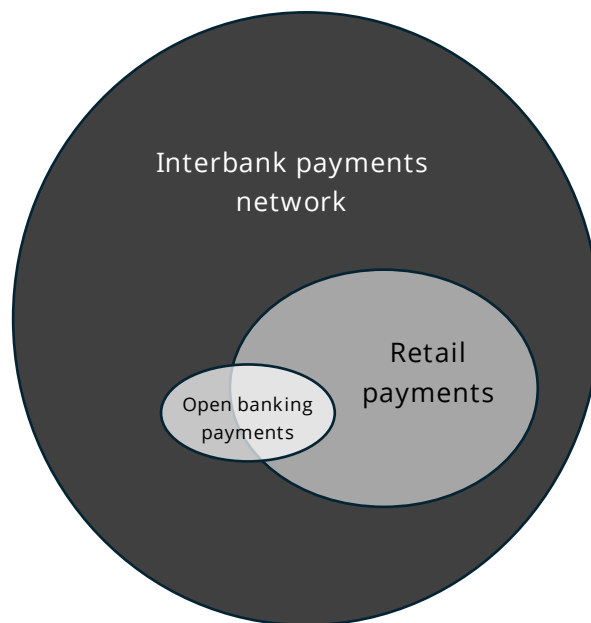
The scope of the proposed designation is set out at page 45 of the consultation paper. As we understand it, the Commission's fundamental interest is in seeing a thriving API enabled payment ecosystem and having this fully operational as early as possible. We consider the proposed designation goes well beyond what is needed to achieve this.

As presently framed, the designation would embrace our entire Payments NZ BECS rule set, both as applying to payment instruments and to participation (membership). Our BECS rules cover a wide range of payment instruments such as social welfare payments, direct debits, ATM settlements, point of sale inter-bank settlements, bill payments, direct credits and automatic payments. Some of these have no relation to retail payments at all. We expand on this further in

the next section below. We also note that our “membership rules” (as described in the proposed designation) include rules relating to how the status of a Participant (i.e. member) and their payments is treated during an event such as insolvency or failure to settle.

While some payment instruments do have application to retail payment scenarios, they are also used far more broadly beyond just retail payments. Similarly, it should be understood that open banking is used extensively for non-retail payment purposes. Examples of non-retail open banking payments include salaries/wages, person-to-person payments, customer funds transfers between their own accounts at another bank, investment contributions (like KiwiSaver), tax payments, charitable payments, etc.

The diagram below illustrates the scope of what the Commission proposes to designate (the “interbank payments network”) versus retail payments and open banking payments.



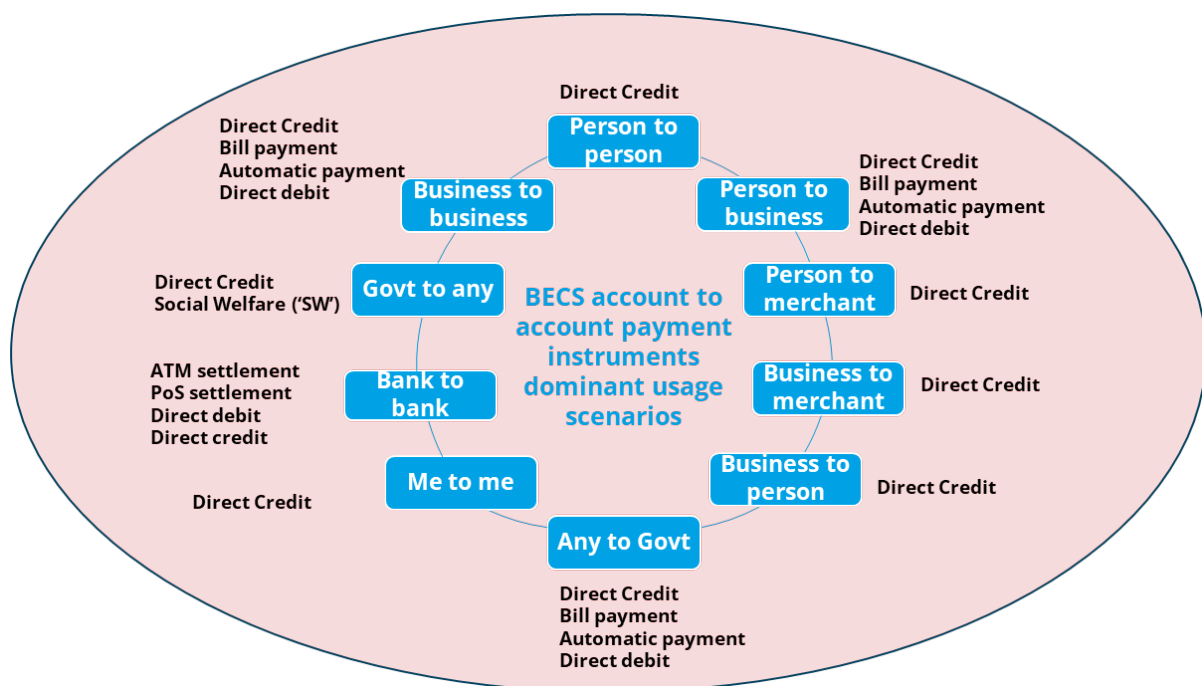
In these circumstances, we consider that the scope of a designation needs to have a far narrower focus and we do not support designation of the full “interbank payment network” as currently proposed. It is too expansive and goes well beyond retail payments. The Commission does not need to designate the entire interbank payments network to address the issues canvassed in the Commission’s consultation paper. We note that the paper provides in-depth rationale supporting the designation of open banking (API Centre), but it does not provide any substantive rationale for designating BECS and all of its payment instruments.

Designation should focus on “retail payment” account to account payments only, and only in the context of open banking, which is the focus of the consultation paper.

Designating all BECS payment instruments goes well beyond what is needed to address the Commission’s concerns

4. We recommend the Commission only designates specific BECS payment instruments in relation to their usage in retail payment use cases.
5. We recommend that only the Direct Credit instrument be designated and only for when it is used in retail payment use cases.

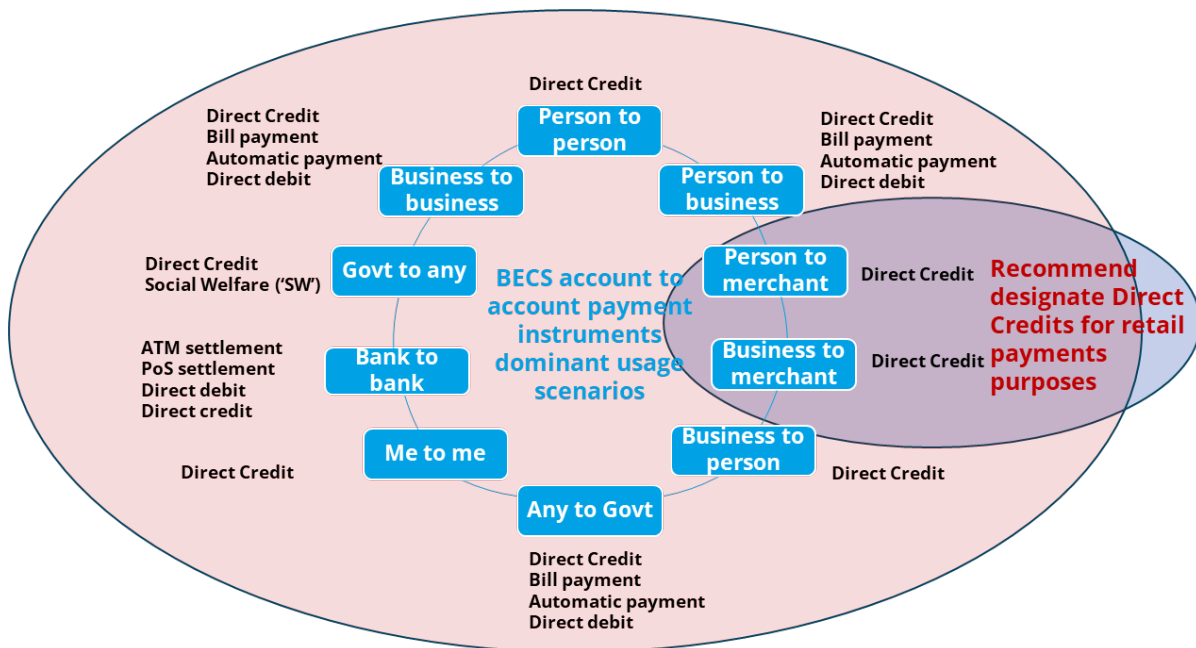
As noted above, BECS has a wide range of payment instruments that can be used across a number of different payment scenarios. The diagram below illustrates this by showing the dominant payment instrument per usage scenario.



The API Centre Payment Initiation standard enables Third Parties to safely facilitate the payments process on behalf of the customer. This standard only utilises Direct Credits.

It is our view that only BECS payment instruments used in open banking retail payments should be designated (i.e. Direct Credits, which are used as the foundational open banking payment instrument). If the Commission proposes to designate any other BECS payment instrument, we would like to understand the rationale for this, why the Commission considers it necessary and how this would support a thriving API enabled ecosystem.

Additionally, any designation should focus on “retail payment” account to account payments only, and only in the context of open banking (which is the focus of the consultation paper). The diagram below illustrates the recommended designation in relation to other non-retail payment usage scenarios and BECS payment instruments.



The scope of any designation should be limited to the relevant API Centre's functions and payments standards

6. We recommend that any designation of standardised APIs should relate solely to payments.
7. We recommend that the draft designation delineates more clearly between the designation of the API Centre's role and that of the Bulk Electronic Clearing System.

Although Account Information API standards are a crucial aspect of open banking and a flourishing API-enabled ecosystem, they do not constitute retail payments. The status of Account Information needs to be clarified. Currently, the draft designation encompasses all standardised APIs of the API Centre which would include Account Information. Accordingly, we recommend that the Commission explicitly states that its designation relates only to payments standards (i.e. the standards relevant to retail payments which may include payment consents, payment initiation, and/or payment-related event notifications).

The nature of BECS's role in the clearing and settling of bulk electronic payment instruments is very different to the API Centre's role in providing a common access method through the use of standardised APIs for payment and non-payment functions. The designation as currently drafted puts both BECS and the API Centre under the same network umbrella. Our recommendations in relation to designation more clearly delineate between the two. This adds clarity and separates access methods from payment instruments. Standardised APIs are one of many access methods. Impersonated access (i.e., using screen scraping and reverse engineering techniques) is another example of an access method.

Impersonated access methods should be included in any designation

8. We recommend the Commission changes its terminology and uses “impersonated access” instead of “sub-optimal methods”.
9. We recommend that as an initial step, impersonated access methods are designated.

We note the Commission has been referring to “sub-optimal access methods” in its consultation paper and in its letter to participants of New Zealand's retail payment system. We do not support the use of the term “sub-optimal access methods” which we consider to be incorrect and misleading. We do not agree that organisations using customer credentials in order to impersonate them, which undermines a key layer of security for customers and banks, is merely “sub-optimal”. This characterisation risks inadvertently conveying a meaning of legitimacy or endorsement by the Commission. We recommend the Commission uses the term “impersonated access”, which correctly describes the situation when one party uses the credentials of another party to access a system.

Impersonated access methods, used to facilitate screen scraping and reverse engineering techniques, are currently not included in the designation. However, as impersonated access methods are a common way to initiate a retail payment between a consumer and a merchant, it is our view that the Commission should designate these access methods as this will provide the basis from which the Commission can, and should, take a stronger stance. If the Commission does not consider it possible to designate impersonated access networks, we propose that the Commission establishes some other form of regulatory oversight.

We note that while standardised API access methods have Payments NZ as a network operator, non-standardised impersonated access methods do not have any common operator or associated rule set. They are undertaken individually by some third-party payment providers (who we note are participant classes listed in the proposed designation). Each third-party payment provider using non-standardised impersonated access methods is, therefore, their own operator.

We believe that a competitive retail payments landscape should not require customers to compromise their online safety. We summarise below three key reasons why impersonated access methods should be designated. As we consider these to be materially important reasons, we expand on each of them in Appendix 1:

1. A level playing field: Not including impersonated access in a designation will create an imbalance between payment system access methods. This creates a risk that the designated method could require significantly more investment in time and effort, whereas the impersonated access method becomes inherently more attractive due to the lower requirements.
2. Poor customer control: Customers have limited controls over data access and functionality once their credentials have been disclosed to the impersonator. As access is ‘all or nothing,’ customers cannot choose to selectively disclose information or place bounds on payments to be processed.
3. No transparent identification of third party payment providers: As the third party using impersonated access is not required to identify themselves to the data holder, the

impersonator appears as the customer. This makes it very difficult for the data holder to distinguish between the customer and impersonator, which makes risk mitigation and applying good security practices difficult.

While designating impersonated access may prove detrimental in the short term for legitimate actors using that method, it may have a positive impact on curtailing bad actors using this approach for attempted data security breaches or other fraudulent activity.

Any exercise of powers should include the phasing out of impersonated access methods and a transition to secure and compliant standardised API access methods

10. We recommend that the Commission considers exercising its potential powers to phase out impersonated access methods and require a transition to standardised API access methods.

In the Commission's open letter to participants of New Zealand's retail payment system it states at A5 that: *"The functionality of the API standards, and therefore the APIs built by the banks, should allow for use cases that are currently serviced by suboptimal access methods (for example, screen scraping or reverse engineered mobile APIs) to encourage providers to switch to using APIs..."*.

The Commission's reference to the development of standardised API functionality that could create new pathways for third parties using impersonated access techniques to transition to safer, more secure and compliant standardised APIs is one part of the equation. We believe that requiring action from only one side (the API standards pull side) is unlikely to achieve any meaningful impact. Even if perfectly aligned API functionality were available, there would still be no compulsion for third-party payments providers to stop using impersonated access methods. Indeed, they still have incentives to continue using impersonated access methods due to their comparatively lower overheads, their greater flexibility, and the lack of obligations to comply with security standards or customer protections.

We believe it would be more effective if the Commission exercised its powers on both the push side (i.e., a managed phase-out of impersonated access) and the pull side (in order to underpin the development of a thriving API enabled ecosystem). We believe this two-sided approach is the most effective way to address longstanding risks and issues, benefiting the wider payments ecosystem and its consumers. It also supports competition by levelling the playing field for all third party payment providers. As such, we propose that the Commission should focus on phasing out impersonated access methods and transitioning those third party payment providers to the use of standardised APIs. The API Centre could support engaging industry and regulatory stakeholders and collating evidence to help formulate an appropriate strategy to achieve that more ambitious outcome.

Other overlapping payments regulation should prevail over the Commission's designation of retail payments

11. We recommend that any designation should explicitly state that it yields to any overlapping FMI designation or CPD legislation.
12. We recommend that any designation and resulting exercise of powers should act as a bridge to CPD only, and then step back.
13. We recommend the duration of the Commission's designation should only be 5 years, to better align with the CPD.

We note the Commission's response to the general theme of feedback received on previous submissions concerning the relationship of any designation with other regulation, such as the forthcoming CPD legislation and designation under the FMI Act. The Commission positions its potential designation as a bridge to expedite open banking progress ahead of the full effectiveness of the CPD regime.

We note the Commission's statement that there might be a technical overlap between the proposed designation and the FMI Act due to the broad definition of network infrastructure in the RPS Act. The Commission also states that the proposed designation does not, in itself, create any regulation and, because of this, there would be no regulatory overlap as an immediate consequence of the proposed designation.

However, we have significant concerns about the relationship between the Commission's proposed designation and other potentially overlapping regulatory frameworks. The Commission suggests that any issues could be resolved as the process is worked through. In our view, this approach is unsatisfactory and risks significant unintended consequences and unnecessarily heightens regulatory uncertainty. We believe, however, that these concerns could be readily addressed if the Commission were to clearly articulate how the Commission's proposed designation sits in relation to other regimes.

We acknowledge that the Commission is obligated to consider the FMI Act when making a designation recommendation under section 12. Additionally, the Commission is required to consult the Reserve Bank under section 13 before making such a recommendation, if the network includes any part of a system that is a designated FMI. The Reserve Bank has indicated that the settlement before interchange system and high value clearing system managed by Payments NZ may be candidates for FMI designation but, as of now, no designation has been made.

The drafting of the Commission's current designation includes "*the Payments NZ membership rules that relate to the BECS participants*". This will almost certainly overlap with the anticipated FMI designation of the settlement before interchange system by the Reserve Bank. In that event, any changes to those BECS rules would be subject to the approval of the Reserve Bank. These changes could also necessitate the approval of the Commission if a directive is issued under section 24(2) of the RPS Act.

We consider that it is inappropriate to have two different designation regimes existing over the same set of rules operated by the same body (Payments NZ). This scenario would create a great deal of uncertainty (and potential unintended consequences) for the regulated and for the

regulators. It would certainly add to the cost of regulation. Moreover, it would be at odds with the principles of regulatory effectiveness and coordination as promoted by the Council of Financial Regulators.

We believe that considerations under the FMI Act are far more relevant to the membership rules for BECS (which are closely linked to the settlement before interchange system rules) than to any proposed designation under the RPS Act. Furthermore, we fail to see the relevance of the BECS membership rules in the context of the outcomes the Commission is looking to achieve in relation to a thriving API enabled ecosystem. Therefore, we recommend that the wording of the Commission's designation should not include BECS membership rules at all.

We also recommend that the Commission's designation includes explicit clarification that, in instances where the Commission's designation of retail payments coincides with an FMI designation, the latter will always take precedence.

The Commission's designation is proposed to remain in effect for 10 years. It is projected that the CPD legislation might take about 4 years to become fully effective. The relationship between the Commission's designation of retail payments and CPD legislation for the remaining six years remains unclear. For instance, there is ambiguity regarding which of the following two medium term scenarios are contemplated by the Commission and MBIE with respect to open banking:

1. Bridge then step back: Any designation by the Commission over open banking acts as a bridge to CPD. CPD then becomes the main regulatory framework for open banking. In this scenario the Commission's use of designated powers in relation to open banking should 'step back' once CPD is fully in force.
2. Co-regulatory model: A co-regulatory framework, where both the Commission's designation and CPD (MBIE) jointly regulate open banking, with clearly delineated roles and responsibilities.

We believe that it is reasonable for the Commission and MBIE to articulate what the target state of regulation is for open banking (i.e. is it 1 or 2 above, or something else?)

We consider that ultimately, and in due course, the CPD legislation will be the better vehicle for open banking and should be the primary framework for its operation and regulation. As such, we recommend option 1 above. For instance, aspects such as open banking standards, implementation dates, and regulated partnering obligations should ultimately be managed via the CPD regime.

This draws from lessons in both Australia and the UK where different regulators have co-regulatory responsibilities over open banking, and this has ended up being unwieldy and inefficient. This approach is also most consistent with the Commission's positioning of its powers acting as a bridge to accelerate open banking's progress until the CPD legislation is in place. We do, however, consider it important that any designation by the Commission include specific language to ensure that where its designation of retail payments directly overlaps with the CPD legislation, the CPD legislation will always take precedence (as suggested in the case of the FMI Act).

Adopting this recommendation would markedly increase certainty and avoid unintended consequences. It would also have no adverse impact on the Commission's stated objectives which, in any event, should have been achieved by then.

In light of this, we think the duration of the Commission's designation should be 5 years, not 10 years. A 5-year horizon would align with the CPD legislation being fully effective and provide an opportunity to realign the regulatory landscape to accommodate the Commission's role. In the context of open banking, 10 years is a very long duration. Open banking itself is relatively new and is somewhat in its infancy (Open Banking Limited – formerly OBIE – in the UK is only 8 years old). It is important to facilitate flexibility because of this.

We do not agree with the assertion in the consultation paper (at paragraph 3.80) that: *“Having a designation in place would likely incentivise quicker resolution of any issues as they arise and could reduce the incentives to occur in the first instance. We consider this could provide greater certainty for banks and third party providers and importantly their investors to move forward with the development of the API enabled payments ecosystem.”*

In our view, the opposite is a more likely outcome. In particular, designation by itself, without a clearly articulated pathway ahead, is likely to increase uncertainty and inhibit progress as organisations wait for regulatory certainty before investing further in the ecosystem. It creates risk when the nature of future regulation cannot be readily determined. This is further compounded if the scope of designation remains excessively broad, as it is currently in relation to both BECS and the API Centre.

The API Centre's expectations of any regulatory backstop are that it reinforces industry momentum and bridges to CPD

14. We recommend the Commission only exercise its powers (if designation proceeds) to act as a regulatory backstop to reinforce industry momentum and provide a temporary bridge to CPD.

Payments NZ considers the Commission's stated goals are broadly aligned to our own payments system and modernisation goals. However, as noted earlier, there is a risk that the Commission's use of its powers may overlap with the future CPD regime and unnecessarily cover areas not relevant to retail payments. Accordingly, we recommend that any use of the Commission's potential powers provide a regulatory backstop that focuses on:

1. compliance with existing industry solutions;
2. ensuring momentum of a published Standards delivery roadmap;
3. encouraging uptake, e.g. setting expectations that government agencies actively use open banking enabled payments solutions and deter organisations from using impersonated access.

We do not support the Commission imposing requirements in relation to new API standards versions and functionality (see paragraph 9.125.2 of the draft market study report). This would undermine the value of our quantitative industry-wide demand analysis and the supporting engagement model (i.e. the voice of the market) that informs the roadmap. It would also create uncertainty for current and future open banking third parties and threaten the integrity of the API Centre as a standards body. Our approach to determining the standards roadmap balances, amongst other things, demand, feasibility, risk and customer benefits (including choice).

We note that, from our engagement with Third Parties, there has been very little demand for product information APIs. Further, we are not aware of any jurisdiction that has common APIs for opening and closing a bank account. Given the prevalence of multi-banked consumers in Aotearoa, we do not see justification for prioritising standardised APIs for opening and closing bank accounts in the near term. We also are unclear about how these fits within the Commission's remit relating to retail payments.

The Commission considers adopting our approach for drafting the designation scope statement, which could assist the practical application of any designation

15. We recommend that the Commission gives serious consideration to adopting our proposed approach for drafting the designation scope statement (if designation proceeds)

Many of our recommendations provided in our submission involve making modifications to the Commission's proposed scope of designation statement. To help bring all of our recommendations together, we have consolidated them into the summary below. This summary also makes some initial suggestions for how the designation scope could be framed:

1. Framing the scope of designation - A summary of how our recommendations could introduce the scope of designation statement include:
 - Reposition the designation to cover the retail payment network instead of the "interbank payments network".
 - Limit designated retail payments to account to account payments only, and only in the context of open banking.
 - Separate the designation of the API Centre's role and that of BECS, even if Payments NZ is referenced as an operator twice.

2. A more targeted scope over BECS – We do not consider it necessary to designate BECS. However, if the Commission does proceed, a summary of how our recommendations could be applied in relation to BECS include:
 - Payments NZ remaining as the operator;
 - the membership rules in relation to BECS being excluded;
 - Direct Credits being specified as the designated payment instrument (i.e. instead of all payment instruments) and limited only to the context of open banking;
 - referencing that any designation of a financial market infrastructure under the FMI Act prevails over the Retail Payments Systems designation (should they intersect).

3. Frame the scope of designation to cover multiple access methods – Our suggestion for how to apply our recommendations regarding standardised APIs and impersonated access methods to the scope of designation statement include:
 - more clearly separating payment instruments from access methods;
 - framing the designation so that it can cover more than one access method.

4. The API Centre - A summary of how our recommendations could be applied to the scope of designation statement in relation to the API Centre include:
 - referring to retail payment access methods using standardised API;
 - identifying Payments NZ as the operator.
 - only including API Centre standards for payments (i.e. not Account Information) - this should include the non-functional standards, guidelines, frameworks and policies relating to those standards;
 - referencing that the CPD legislation and/or regulation prevails over the Retail Payments Systems designation (should they intersect).

5. Impersonated Access methods - A summary of how our recommendations could be applied to the scope of designation statement in relation to the impersonated access methods are:
 - including impersonated access methods in the designation.
 - referring to them as retail payment access methods using non-standardised interfaces (or impersonated access methods).
 - making any third party payment provider who operates non-standardised access methods for the purposes of initiating a retail payment a network operator (we suggest covering all those operators generically and not list the specific third party payment provider entities).

6. Duration of designation – We suggest making any designation last for 5 years.

5. API Centre's role and response to the Commission's expectations

Payments NZ and our API Centre are committed to working towards the Commission's expectations in relation to increasing transparency and meeting the future needs of payments and open banking

In its open letter to participants of New Zealand's retail payment system dated 22 February 2024, the Commission set out expectations for payment system participants. Six of these expectations are directed at Payments NZ (per Annex B). We agree that wider consultation and transparency will benefit current and future participants of a thriving API-enabled open banking ecosystem and will result in products and services that better meet consumers' needs¹.

We remain committed to working with industry to deliver standards that enable innovative solutions to come to market. In response to the Commission's expectations, the API Centre has commenced new initiatives, such as an expanded engagement programme that will include fintechs and other non-member organisations, and increasing the content shared with the public on its website. This is in addition to the significant work programme already underway at the API Centre. We believe that Payments NZ and the API Centre are well-placed to continue leading open banking in Aotearoa.

We acknowledge the Commission's views on the progress of open banking in Aotearoa. We do, however, consider that many of the issues outlined in the Commission's papers are historical and note that major efforts have been made to address these, some of which are set out below:

- to address issues of API Provider implementation timeliness, the API Centre now has powers to set minimum requirements (including implementation dates) that API Providers must meet to ensure that a standardised API is technically and operationally ready for use with Third Parties. There are currently two 2024 implementation milestones for API Providers which have been published publicly on the API Centre website;
- to address transparency, the API Centre collates implementation progress reports from API Providers which are published publicly and updated regularly;
- to address issues in relation to partnering between API Providers and Third Parties, we have taken the proactive step of seeking the Commission's authorisation to co-design an accreditation and partnering framework. In our application to the Commission for authorisation, we emphasised the benefits such a framework would provide for competition, ongoing innovation, and good outcomes for consumers and businesses.

Other concerns covered in the Commission's papers are already on the work plan, such as availability and performance, and the standards development roadmap. The API Centre recognises it still has some work to do to see open banking widely used in Aotearoa. We are committed to leading open banking for Aotearoa and will continue to evolve our approach, our governance and our work programme.

¹ Annex B, B2 The Commission's letter to payment system participants:
https://comcom.govt.nz/_data/assets/pdf_file/0017/344132/Retail-Payment-System-Update-on-our-Payments-Between-Bank-Accounts-work-22-February-2024.pdf

We take the opportunity to respond to some of the Commission's commentary (in its draft report) with respect to Payments NZ and the API Centre.

There is a strong theme that the API Council's progress and performance is hindered because it is operating under delegated authority from the Payments NZ board where directors are appointed by shareholders. It is important to note that there are three independent directors on the board (including an independent Chair) and all directors have obligations under the Payments NZ constitution and the Companies Act 1993 to act in the best interest of the Company (even if those interests conflict with the interests of their appointing shareholder). Similarly, API Council members, which includes three independent members and an even balance of API Providers (i.e. banks) and Third Parties, must also act in the best interests of the API Centre. We are not aware of any instance where our governance structure has been responsible for adversely shaping a particular outcome for open banking.

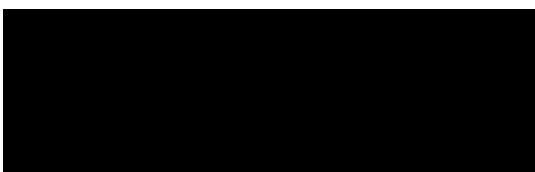
It is noted in paragraph 3.57 of the consultation paper that exemptions could also potentially hinder the timely delivery of an API enabled payments eco-system. We do not accept that this is the case and note that there are clear criteria that must be met before an exemption is granted, namely that any exemption will not:

- undermine the integrity, security, and efficiency of the API Centre;
- have an unreasonable impact on any API Standards User;
- undermine the integrity, security, and efficiency of a Standardised API; and
- have an unreasonable impact on a Customer's interests

This is a high threshold. In addition, all API Centre standards users are given the opportunity to review and make a submission on any application for an exemption. We suggest that it is premature to hypothesise on possible impacts of the exemptions process at this early stage of the first implementation cycle in 2024. We would also observe that having the ability to grant exemptions is commonplace in financial services regulation, both in New Zealand and overseas. More pertinently, it exists for the purposes of the CDR regime in Australia and for the open banking regime in the UK.

We thank the Commission for the opportunity to respond on this consultation. We hope you find that our recommendations constructively drive towards a thriving open banking ecosystem for Aotearoa.

Ngā mihi,



Steve Wiggins
Chief Executive
Payments NZ Limited

Appendix 1: Supplementary information on why designating impersonated actors is of paramount importance

Recommendation 9 proposes that impersonated access methods be designated. The supporting rationale outlined three supporting reasons. We expand further on these reasons below:

Level playing field

Any decision on designation that does not include impersonated access could create an undesirable imbalance between payment systems methods. Designating only one access method risks the designated method requiring materially more investment in time and effort, whereas the un-designated would become inherently more attractive due to the lower requirements. In the interests of creating a level playing field, we recommend that impersonated access and similar methods are also designated. Failure to do so risks creating unintended consequences and driving activity away from methods that offer strong customer protections and create level playing fields (and hence competition) through open standards such as APIs.

Impersonated access is normally implemented using a form of the 'manipulator in the middle'² attack (i.e., man-in-the-middle), which is an inherently unsafe practice. Some of the largest data security breaches in the world have used this method³. We suggest avoiding any outcome that may favour methods that rely on known unsafe practices that are easily exploitable, and methods that are safer and designed to eliminate this vulnerability (and others) should be preferred. Safe practices are better for creating level playing fields and increasing competition while also increasing customer data protection.

Customer control

With impersonated access, customers have limited controls over data access and functionality used once their credentials have been disclosed to the impersonator. There is no explicitly granted consent at the data holder to release data from those entrusted to holding it, and the data holder can only act as though it is the customer themselves. Customers cannot choose to selectively disclose information or place bounds on payments to be processed. Access in this sense is all-or-nothing, with the customer unable to control the scope of data or functions or the time for which is possible. If a customer wishes to disallow access at the data holder, then they must change their credentials with the data holder. This trust model greatly favours the impersonator, and customers are at greater risk than with other methods that require explicit consent and ensure this is available at the third party and data holder.

Third party identification

Impersonated access is so named because the third party using this method is not required to identify themselves to the data holder. Because the impersonator sits between the customer and data holder and uses the credentials supplied by the customer, the impersonator appears not as themselves but as the customer. While this favours legitimate actors using impersonation by providing full access, it can be very difficult to distinguish between the customer and impersonator and risk mitigation is much more difficult. Data holders are unable to apply reasonable measures to meet good security practices such as data minimisation or appropriate

² https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack

³ <https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack#:~:text=Examples%20of%20Man%2DIn%2DThe%2DMiddle%20attacks>

access controls since they cannot confidently assess all actors; the impersonator is hidden behind the customer identity. In this scenario, non-repudiation becomes extremely difficult and customer trust with the impersonator is taken to an extreme level; the impersonator can perform any action the customer themselves can. Any compromise of the impersonator could result in full access to all customer credentials they hold, creating a concentrated risk of customer credential exposure.

If impersonated access is not designated, then it risks undermining customer trust since this could be perceived as a tacit endorsement of methods that do not require all parties to be strongly identified. Customer trust and confidence are key to the uptake of safer methods with authentication (and authorisation) of all parties required to enable that trust.