ASB Bank Limited
PO Box 35, Shortland Street
Auckland 1140, New Zealand
[redacted]
CX10087 Auckland DX Sort
asb.co.nz

9 May 2024

Retail Payment System Regulation
Commerce Commission
Level 9
44 The Terrace
Wellington 6011

By email: paymentsteam@comcom.govt.nz
[redacted]

ASB response to Commerce Commission consultation on proposal to recommend designation of the interbank payment network

ASB Bank Limited (**ASB**) welcomes the opportunity to provide feedback on the proposal to recommend designation of the interbank payment network under the Retail Payment System Act 2022 (**RPSA**).

On behalf of ASB, I would like to thank the Commerce Commission (**Commission**) for its ongoing engagement with ASB, including at a meeting with the Commission, MBIE and the Reserve Bank of New Zealand in February. We appreciated the opportunity to discuss New Zealand's approach to open banking and payments, as well as the broader regulatory environment. We see great value in these engagements and look forward to continuing to work together on the best way to transform New Zealand's digital economy for the long-term benefit of consumers and businesses.

ASB is committed to modernising New Zealand's payments ecosystem. We are working hard to meet this year's open banking deadlines and will continue to engage openly with the Commission and with third party providers on open banking. That being said, combatting the rising number of fraud and scams in New Zealand remains our top priority. We have committed [redacted] this financial year to tackling fraud, scams and financial crime and continue to prioritise investment in our systems that best ensure our customers' data and money is kept safe.

Our general views on the proposals outlined in the consultation paper (**Paper**) are set out in more detail in Appendix 1 to this letter.

In summary, ASB submits:

Safety and security must be paramount

- To ensure we maintain consumer trust and confidence and continue to protect Kiwis from the threat of fraud, scams and cyber-crime, New Zealand needs a safe (and trusted), easy, and efficient way for people to make payments and receive additional value and insight from their payments data.
- Designation of the interbank payments network could be useful to support a "thriving API enabled ecosystem" if the Commission were to reprioritise the delivery roadmap from v2.3 features to focus on real-time fraud mitigations first, in light of rapidly growing and evolving fraud and scams in New Zealand.
- The Commission should take an iterative approach to the expectations it sets out in its open letter dated 22 February 2024. While we consider we are well placed to meet these expectations, commitments to timeframes should be re-examined in line with a shift in focus from v2.3 to a next iteration that prioritises combatting fraud and scams.

Getting the sequencing right is critical for the safety and security of customers' money and information, the long-term uptake of open banking and benefits to New Zealand consumers

- We are of the view that for New Zealand to be truly productive, inclusive and innovative , we need a strong digital ecosystem that enables safe data exchange and identity verification coupled with a modern, secure, and efficient payments system. Customers need to trust that their money and information will be kept safe before they will utilise any open banking framework (however well designed or speedily implemented).
- To realise this, New Zealand must prioritise the introduction of a digital identity regime, enabling people to share their identity digitally to organisations in a secure and trusted way.
- While we appreciate there have been commitments made in previous years to deliver an agreed scope of open banking, the payments and banking environments have changed significantly, particularly due to rising fraud and scams. To support consumers' trust in open banking systems, banks should focus on investing in functionality which creates value at scale or works towards enhancing safety and security for New Zealanders' assets and data.

Designation will only be effective if regulatory powers are used consistently, for all participants – 'regulate the activity, not the entity'

- We urge the Commission to consider the purpose of designation and its intended beneficiaries. If the intent is to regulate to increase competition then the Commerce Commission is the natural regulator. However, if the intent is ultimately to provide New Zealanders with more options and enable cheaper, faster and safer payments, then another regulator may be more appropriate.
- Designation should cover **ALL** market participants, including global platforms , fintechs, providers, schemes and so on.
- Designation of all participants will ensure there is a level playing field for a thriving API enabled ecosystem, including shared ongoing investment into infrastructure, enabling fair pricing and beneficial outcomes for all consumers, including protections regardless of the means by which they make payments.
- ASB agrees that the Commission should consult and agree with industry on what the designation will look like and how the Commission will use its regulatory powers.
- ASB also considers that any recommendation to designate the interbank payments network should take into account the Minister's intent to return to a 'twin peaks' model of regulation i.e. with the FMA as the sole conduct regulator.

If you have any questions on any aspect of our submission please reach out to [redacted], Head of Government Relations and Regulatory Affairs [redacted]

We look forward to further discussing how New Zealand can build a world class digital infrastructure which puts New Zealander's safety and security at its heart.

Ngā mihi nui.

[redacted]

[redacted]
EGM Personal Banking, ASB Bank

14004 0001A 0823

Appendix 1: ASB's general views on the proposals to recommend designation

1. Introduction

The scale of New Zealand's interbank payments network is significant, facilitating around $1.75 trillion in payments in 2023. New Zealand's payment network settles every 30 minutes, seven days a week, between 9am and midnight.

With payments at the heart of much of what New Zealanders do every day, it is essential they have complete trust and confidence in New Zealand's payments system, now and into the future. This is against a backdrop of heightened competition in the payments space, with global providers like Apple taking over as a primary payments method overseas. In Australia, 47% (and growing) of all in-store card payments by CBA customers are made using mobile wallets, and of those in-store mobile wallet payments, over 80% occur via Apple Pay.

In response to the evolving needs of New Zealanders and changing nature of the payments landscape, ASB has been working hard to innovate, upgrading and updating our core systems and improving digital experiences for customers. This is against a backdrop of persistent regulatory change over the past 5-7 years, resulting in over [redacted] being spent on regulatory initiatives within that timeframe alone.

Key regulatory changes have included the Reserve Bank of New Zealand (**RBNZ**) capital reviews, the Deposit Takers Act and Deposit Compensation Scheme, BS11 implementation, the new Conduct for Financial Institutions (CoFI) regime and the Financial Advice Provider (FAP) regime. Alongside this, ASB has been working steadily to implement open banking and to modernise its payment platforms as a prerequisite for the impending industry modernisation programme. Over the past 12 months the banking sector has come under increasing political, regulatory and public pressure to deliver on these initiatives. Only so much change can be absorbed at once, regardless of how much capital we have to invest. Investment is not the binding constraint, rather change saturation and availability of skilled resource constrain us. Furthermore, the more change initiatives that are implemented to our mission critical systems at the same time, the greater the chance of complications and issues arising. It is essential that we limit the degree of delivery risk at any one time to ensure these systems remain operational and resilient throughout the change process and ongoing.

In this context, the following principles should be reflected upon when considering the appropriate sequencing of open banking and other initiatives/changes in the payments ecosystem:

- safety and security of customers' money and data as the paramount consideration;
- whether required changes meet other compliance requirements for banks e.g. given international obligations such as SWIFT ISO20022 mandates; and
- whether the changes offer significant value for customers.

2. Safety and security must be paramount

Consumers are demanding better fraud and scam protection from banks

The New Zealand economy must be underpinned by strong digital infrastructure, which is more broad than just open banking or payments, to enable safe data exchange and coupled with a robust, centralised means of identity verification. Customers need to be confident that they can reliably transact in a safe and secure manner.

To realise this, New Zealand must prioritise the introduction of confirmation of payee technology and a digital identity regime, enabling people to share their identity digitally to organisations in a secure and trusted way. This would lay the foundation for an open banking, payments, and digital interactions system that is safe and secure and which is underpinned by rich data, real time fraud detection and counterparty verification. Doing so would result in a system which is trusted, and therefore used, by consumers.

Regulatory environment is already overly complex, hampering innovation

A holistic consumer-centric approach to regulation

In determining whether designation is necessary, we urge the Commission to consider the purpose of that potential designation and its intended beneficiary. If the intent is to regulate to increase competition and create greater opportunities for fintechs and others to enter the market and expand, then the Commerce Commission is the natural regulator. However, if the intent is ultimately to provide New Zealanders with more options, enable switching between banks, support customers to more easily access their banking data, and enable cheaper, faster and safer payments, then it is appropriate for the Financial Markets Authority (**FMA**) to regulate (as the financial services sector conduct regulator).

A return to twin peaks regulation

Minister Bayly announced in late January that he intended to return financial services regulation to a twin peaks model. This is where there is a sole prudential regulator (RBNZ) and a conduct regulator (FMA).

In mid-April Minister Bayly and Minister Bishop released details on how the CCCFA would initially be reformed, including responsibility for the CCCFA moving to the FMA. On Sunday 21 April Minister Bayly announced his proposed changes to the CCCFA and confirmed his intention to move regulation of consumer credit from the Commission to the FMA.

In the event the Commission decides to designate interbank payments under the Retail Payments Act, this would dilute the intended traditional twin peaks model that the Minister is aiming for.

The Commission, in its draft report for the competition study into personal banking services (published 21 March 2024) found that the burden of New Zealand's regulatory environment "is very high and imposes a significant barrier to new entry. For all existing providers, it has constrained growth and innovation due to resources being deployed to keeping up with regulatory change."[1]Designating interbank payments, particularly where that results in regular specific oversight by another regulator alongside the RBNZ and FMA, would further add to this regulatory burden. We note the FMA is purely a financial service regulator and does not currently have a mandate to oversee all payments. However, given Minister's Bayly's comments, the FMA's remit may expand in any event.

A level playing field

Regulation should relate to an activity not an entity. The purpose of designation proposals should be to increase competition to the long-term benefit of New Zealanders, without compromising financial stability. Appropriate protections must exist to ensure good outcomes for customers, irrespective of who they transact with. By not regulating all participants in an equal manner it creates a two-tier system – where consumers have different levels of recourse and rights depending on the provider they obtain goods and services from. This creates disparity and confusion for consumers, but perhaps more importantly means certain consumers will miss out on the apparent benefits merely by virtue of who they happen to deal with.

Where a payment services provider is not regulated and it becomes insolvent, the return of funds to customers could be delayed and customers may not get all of their money back. Administration cases

[1] Commerce Commission's draft report for the market study into personal banking services, p157.

involving payment institutions and electronic money institutions in the UK have taken years to resolve in some cases, with customers left without access to their money for prolonged periods and finally receiving reduced monies after the cost of distribution. The UK Government introduced the Payment and Electronic Money Institution Insolvency Regulations in 2021 after six cases where Payment Institutions and Electronic Money Institutions became involved in insolvency proceedings (three of which started in 2018), and only one institution had returned funds to customers at that time.

Regulation over payments must therefore include all participants in payments including, for example, Apple. Apple Pay has now surpassed Mastercard in total transaction values globally. This payment method is growing in New Zealand and now represents 5% of total credit card spending and 10% of debit card spending.

Apple controls more than 80% of the payments made via cell phones in Australia, with Apple currently able to charge whatever it likes for those payments. Apple also prevents bank apps from making tap-and-go payments, unless they are routed through Apple Pay and charges banks for payments using bank cards stored in iPhones.

It is vital that all participants active in payments are subject to the same level of regulatory oversight, with customers able to benefit equally from the apparent benefits of such regulatory oversight, regardless of which entity processes or facilitates that payment.

Appropriate sequencing of reforms that prioritises the safety and security of customers' money and information, promotes the long-term take up of open banking and benefits to New Zealand consumers

Awareness of open banking remains low and New Zealanders seem to be unclear of the benefits it offers them. They are however, very aware of, and concerned by, cyber security, fraud and scams.

ASB supports a reduction in the AML/KYC onboarding obligations where they create barriers for consumers in accessing or switching banking services, provided those obligations are not important for reducing or mitigating financial crime risks (i.e. address verification could be removed). In addition, AML reporting entity obligations should be amended to allow providers to rely on customer identity verification that has already been carried out by banks, government or other trusted bodies.

Developing a national Digital Identity scheme is a crucial next step. Digital IDs are increasingly used to verify payers and payees. A national Digital ID system would enable fast and reliable verification of individuals, businesses, and machines by public and private sector organisations without the need for repeated collection of identity information. This would have the benefits of:

- decreasing the risk associated with the repeated collection of the necessary information;
- making access to services for customers faster, easier and more efficient, and potentially producing significant productivity gains for organisations;
- decreasing friction in the customer switching process; and
- significantly improving access to public and private sector services, reducing barriers for customers and communities in more vulnerable circumstances to access services.

3. ASB is an active supporter of the joint initiative recently inaugurated by Payments New Zealand and Digital Identity New Zealand to investigate a framework for digital identity, verifiable credentials, and their use with the payments ecosystem.**Delivery of open banking (v2.3 and beyond) needs to be dynamic and iterative –**

ASB is committed to delivering API v2.1 in 2024, having dedicated [redacted] of investment in the past financial year for the delivery of open banking. We are continuing to progress the implementation of systems and processes required to support open banking. ASB recently began onboarding our first open banking partners, who reported excellent feedback on our due diligence process and documentation.

However, as set out above, with rising incidents of fraud and scams, safety must be the first priority. In order for open banking to succeed and to deliver its intended benefits to consumers it must protect and certainly must not do anything to undermine the integrity of the payments ecosystem. It's critically important the system is not only secure, but that New Zealanders have absolute confidence in its security. ASB understands from UK bank HSBC that retrospective crime prevention controls had to be built in the UK's open banking framework, as these were not prioritised upfront. We are keen to ensure New Zealand does not repeat this mistake.[2]

ASB has therefore reviewed the current scope of v2.3 and considers there is more important functionality that should be delivered ahead of what is currently in scope. The scope of v2.3 was tabled, discussed and agreed over a period of three years and, in that same timeframe, New Zealand has seen an upsurge of fraud and scams, that are becoming increasingly more sophisticated. We therefore believe delivery of open banking and other payments initiatives should be dynamic and iterative, requiring regular review, re-validation and reprioritisation/sequencing in the best interests of New Zealand consumers and businesses. With this in mind, our proposed review and resequencing of v2.3 is outlined in Appendix 2.

As the Commission will see in Appendix 2, developing the confirmation of payee (**COP**) functionality must be a first priority. This work is well progressed and scheduled to begin rolling out at the end of 2024. We consider the API Centre should prioritise the development of standardised API specifications to support the confirmation of payee initiative and avoid any duplication that would result from developing COP APIs and lifecycle management outside the API Centre. ASB is happy to support the API Centre in undertaking this work, which needs to be urgently prioritised.

Some further important considerations to ensure open banking is successful are to:

- ensure all regulators are aligned;
- consider who should bear the cost of operationalising;
- consider who is liable if things go wrong (e.g., if a third-party provider fails); and
- consider senior manager liability and consumer protection against data breaches or asset losses.

4. Next steps

ASB supports collaboration to establish digital identity services which leverage the work already underway by various private sector parties and the Department of Internal Affairs, including the trust framework the API Centre proposes to develop through its partnering project. Opportunity exists also to leverage and learn from work done by banks on Connect ID in Australia. ASB is of the view Payments NZ should lead this work on a fit-for-purpose digital ID scheme which is also likely to require standardised APIs.

Collaboration will also be vital between Payments NZ, the Commission and the wider industry to develop a roadmap for the delivery of open banking and a digital payments infrastructure which is safe, secure and has the trust and confidence of New Zealanders. The roadmap could include continued commitments to prioritise API functionality as outlined in Appendix 2. However, we consider the proposed implementation plan for v2.3 should be amended to ensure the key priorities set out in this submission are appropriately baked in, and the feedback on v2.3 deliverables and timeframes outlined the Appendix 2 are taken into account.

[2] 38% of crime in the United Kingdom is now fraud and scams and New Zealand should do anything we can to avoid a similar scenario.

ASB Bank Limited

Appendix 2 - ASB proposed prioritisation and sequencing of open banking delivery

Ref	Description	ASB Feedback	Delivery Date
	Confirmation of Payee	The banking industry is working hard to deliver Confirmation of Payee **(COP)** by the end of 2024. However, development of COP will need to align with the development of the Account Name functionality referred to at 3a below. The API Centre should prioritise the design of specifications for a standardised API for the Account Name to avoid duplicative efforts.	Roll out to commence **by the end of 2024**
V2.3 (1)	Payment Initiation - Enduring Consent	ASB fully supports the inclusion of Payment Initiation in the Plan. Potential use cases are clear and there is significant benefit to customers and participants.	Delivery to be reconsidered in light of need for standardised APIs for COP
V2.3 (2)	Security Profile – Decoupled (CIBA) Flow	ASB is fully supportive of the Decoupled Flow implementation as potential use cases are clear and there is significant benefit to customers and participants.	Delivery to be reconsidered in light of need for standardised APIs for COP
V2.3 (3a)	Account Information – Party	**Account name and Type**: ASB supports this development as the use cases and value of Account Name and Type are clear. As discussed above, we also consider it is critical to align with the COP work to ensure there is not a duplication of standardized APIs or use of different security methodologies for similar data points.	Delivery to be reconsidered in light of need for standardised APIs for COP
		Contact details and address: ASB is not supportive of the inclusion of this functionality in the Plan at this time. The value of contact details and address data is not clear – currency of this data will be a challenge for participants due to customers not keeping this data up to date, particularly as online statements have become more common. ASB considers there is an unacceptable level of risk to the ecosystem associated with sharing data of dubious quality. We believe this can be provided more accurately by customers directly.	Defer delivery to a future date
V2.3 (3b)	Account Information – Statement	ASB is not supportive of the inclusion in the Plan at this time. While ASB would be able to support the statement file endpoint for personal customers, there is no equivalent in our online channels for either transaction history by statement ID or for statement files for business customers and we are unable to make these available via Open Banking APIs. Considering the availability of transaction history in v2.1, we do not consider making personal banking statement files available via Open Banking APIs will deliver meaningful value to the ecosystem.	Defer delivery to a future date
V2.3 (4a)	Web channel support – consent management	ASB considers there is limited value in adding support for consent management and revocation in our web channels. Statistics show the use of web channels is declining rapidly while Mobile App usage is by far the most common form of interaction for our customers.[6] This would not impact the experience of our third parties and so we question the value of its inclusion in the Plan.	Defer delivery to a future date

V2.3 (4b)	Web Channel support – authentication	ASB strongly opposes adding consent authorisation, via either redirect or decoupled flow, into our web channels and request the removal of this from the Plan. Since the scope of v2.3 was initially agreed, the rising incidents of fraud and scams in New Zealand means we need to reconsider whether this flow is advisable in the current environment. ASB is concerned that the user behaviour that this endorses is well known to put our customers at increased risk of Phishing attacks. ASB's Fraud and Information Security teams' concerns are outlined below: • While ASB has full confidence in the technical authentication of the open banking proposal, the behaviours that this encourages and endorses will leave the public far more vulnerable to fraud and scams. • The proposed experience is indistinguishable from a typical malicious phishing flow for the vast majority of the general public. • This functionality would be effectively teaching the public to accept a redirect from a third-party site which then prompts them to provide their banking credentials. This flow would be in direct conflict to guidance we provide to the public on how to avoid falling victim to fraud and scams. • If we continue to deliver open banking leveraging this pattern, we cannot see a way that we can change our guidance and messaging to delineate between an open banking flow and a fraud flow.	ASB does not support this development