29 August 2025

Consumer Policy Team
Building, Resources and Markets
Ministry of Business, Innovation & Employment
PO Box 1473

Wellington 6140
New Zealand

By email: ***consumerdataright@mbie.govt.nz***

ASB Bank Limited Submission on the Customer and Product Data (Banking and other Deposit-Taking) Regulations 2025 ("Designation Regulations") and the Customer and Product Data (General Requirements) Regulations 2025 ("General Regulations"), to be issued under the Customer and Product Data Act 2025 ("CPD Act")

ASB Bank Limited (**ASB**) welcomes the opportunity to provide feedback to the Ministry of Business, Innovation and Employment (**MBIE**) on the Designation Regulations and the General Regulations (together, the **Regulations**).

ASB supports the intent of the Regulations to facilitate data sharing and payment initiation under the Consumer Data Right (**CDR**) in a way that is secure, efficient and promotes innovation. While the draft Regulations represent a step toward that goal, there are important clarifications and amendments that we consider necessary to ensure successful implementation and avoid unnecessary risk for participants in the CDR regime.

Our key messages are:

1. **Relevant accounts:** The definition of "relevant account" in regulation 7(3) of the Designation Regulations is broad and appears to capture various categories of investment products that are not suitable for standardised data sharing, potentially introducing customer risk and imposing unnecessary operational burdens on Data Holders. ASB recommends that the regime focusses on the account types specified in the API Centre Open Banking Implementation Plan "Minimum Requirements for API Providers to meet" (at least for the initial phase of implementation).

2. **Designated data:** ASB recommends that the detail of designated data is reserved for technical standards, rather than prescribing specific data fields in the Regulations themselves. This approach is essential to ensure ongoing alignment with the Payments NZ API Standards (**API Standards**), which are designed to evolve over time, and reflect industry best practice. Many of the data types currently described in the draft Regulations do not currently align with the API Centre standards. Prescribing data fields within the Regulations risks creating ambiguity, inconsistency, and unnecessary operational complexity for customers, Data Holders and Accredited Requestors. This could introduce unintended uncertainty for the industry, which would put the desired outcomes of the Regulations at risk.

3. **Grounds for refusal need to align to existing financial compliance reasons:** Current ASB channels (mobile, web) and internal procedures are set up to comply with a multitude of other regulatory and industry requirements such as AML, sanctions, payments screening, and scam prevention as well as internal bank policies and operational processes. The ability to

act on these requirements for mobile and web channels is set out in Bank Terms and Conditions with the customer. It would seem impossible to replicate all those reasons into this regulation. Therefore, this new electronic channel **must** allow for Bank Terms and Conditions to also take effect in respect of actions instructed via this new API channel. The Regulations should make explicit use of the power in sections 16(1)(i) and 20(1)(h) to state that Data Holders may refuse to provide data or perform designated actions on any grounds that would entitle them to refuse or delay a payment or data access request under their standard terms and conditions for electronic facilities.

4. **Liability:** Liability is not clearly allocated for various material risks, including data breaches or inaccuracies, security incidents, intellectual property usage, loss caused by counterparty's breach or negligence, and excessive use of APIs by Accredited Requestors. The Regulations should make clear that once data is transferred to Accredited Requestors – or, where acting as an intermediary, their downstream partners – these entities are fully and solely responsible for compliance with the Privacy Act 2020 and other relevant liabilities (such as breach of confidence) in relation to that information. We have provided, in the Appendix, our previous analysis on suggested liability allocation for the various risks in the new ecosystem which was completed for ASB's submission to the API Centre. We submit it for your consideration as to unaddressed areas in the Regulation which if left unresolved, would likely require coverage through bilateral contracts.

5. **Insurance / guarantees:** The Regulations are unclear as to what "reasonably adequate" means in the context of insurance or guarantee arrangements for Accredited Requestors. In addition, Accredited Requestors are not required to *maintain* ongoing insurance or financial guarantees. This exposes Data Holders and customers to risk, if, for example, an Accredited Requestor becomes underinsured. Accredited Requestors should be required to provide continuous cover, with prompt notification obligations in the event of any lapse.

We set out these key recommendations in more detail in the schedule to this letter, as well as several other matters (in paragraph 7 of the schedule).

ASB would welcome the opportunity to engage further in relation to the development of the Regulations and would be happy to assist MBIE with any questions arising from our submission.

Yours faithfully

Jonathan Oram
Executive General Manager
Corporate Banking
ASB Bank Limited

Schedule: Submission on the draft Customer and Product Data (Banking and other Deposit-Taking) Regulations 2025 and the Customer and Product Data (General Requirements) Regulations 2025

Introduction

ASB is generally supportive of the proposals in the draft Regulations. However, this submission focusses on a number of key issues that we believe require reconsideration in order to ensure a balanced and effective implementation of the CDR within the banking sector.

1. Relevant accounts

a. The current definition of "relevant accounts" in regulation 7(3) of the Designation Regulations is overly broad and, as drafted, would capture a range of investment products that are not appropriate for inclusion in the CDR regime.

b. For example, the definition would capture units in Portfolio Investment Entity (PIE) funds. These products often involve pooled investments, variable returns, and a range of underlying assets. The structure, terms, and withdrawal conditions can vary significantly between PIE funds and providers. This complexity makes it difficult to standardise the data elements required for effective and secure data sharing under the CDR regime.

c. In addition, the current API Standards that underpin the CDR regime are designed primarily for core banking products such as transactional and savings accounts and do not capture information about PIE funds. Data Holders would therefore need to develop bespoke systems and processes to extract, standardise, and share complex investment data, which is not currently supported by the existing API infrastructure. That would be disproportionate given the focus of the CDR regime on facilitating data sharing for everyday products (such as, in a banking context, transactional and savings accounts as well as credit cards and other standard lending products).

ASB recommendation:

d. We strongly recommend that the scope of relevant accounts be narrowed to focus on core transactional and savings accounts and lending, in line with the ***Open banking implementation plan for Aotearoa New Zealand | API Centre*** **"***Minimum requirements for API Providers to meet*." If more complex investment products like PIE funds are intended to be subject to the CDR (which we do not consider necessary), we recommend that this occurs at a later stage as part of a phased approach.

2. Designated data

a. The current approach to the designation of data in the draft Designation Regulations risks significant inconsistency and operational challenges for Accredited Requestors and Data Holders, particularly in relation to alignment with the API Standards.

b. ASB's strong preference is that the details of designated data are reserved for the technical standards and are dealt with by cross-reference in the Regulations. This approach is essential for consistency with the API Standards, which are designed to evolve over time in response to industry developments and customer needs. Prescribing

data fields in the Regulations risks creating a static and potentially inconsistent framework that will be difficult to update and may quickly become misaligned with the API Standards.

c. To illustrate some of the key issues:

A. Regulation 7(1)(d) requires Data Holders to provide "particulars of each transaction" for a relevant account during the 2-year period before the time of the request. However, "particulars" is not defined, creating ambiguity as to whether this includes only standard customer-facing transaction details (such as date, amount, payee/payer, and reference) or extends to internal notes, operational codes, or other sensitive information.[1] Currently, this would create potential misalignment with the API Standards. (If the term "particulars" is retained in the Regulations it should be clearly defined to limit the scope of designated transaction data to information customarily provided to customers in standard account statements or online banking interfaces, and to expressly exclude internal notes, operational codes, or other proprietary information).

B. Any data fields considered necessary under Regulation 7(1)(e) should be addressed through the technical standards, and not within the Regulations. Our understanding is that MBIE supports the recent decision taken by the API Centre to remove the mandatory requirement for the StatementID/transaction endpoint from future standards and effect an exemption under the v2.3 Standard. On that basis, Regulation 7(1)(e) introduces further ambiguity and complexity since it covers a wide range of data that is not expected to be covered by future API Centre Account Information standards.

C. The reference to "customer" in Regulation 7(1)(a) could raise ambiguities because the person giving consent (i.e. the individual with authority to operate the account) may be different from the person or entity that owns the account. In addition, it is unclear what data is required in the current drafting. As previously stated, we believe that the details of designated data should be reserved for the technical standards and dealt with by cross-reference in the Regulations.

D. There is a structural inconsistency between the draft Regulations and the API Standards. The current drafting represents the API Standards irregularly across different categories. For example, the provisions relating to relevant account data (regulation 7(1)(a)) and statement data (regulation 7(1)(e)) combine both mandatory data points and optional illustrative examples, whereas the transaction data provision (reg 7(1)(d)) does not follow this approach and instead provides only certain examples.

E. It is unclear whether the reference to the "name of the account" in regulation 7(1)(b)(ii) refers to a) the product name, b) a customer-assigned nickname to the account, or c) the party name associated with the account. This lack of clarity risks inconsistent implementation and unnecessary complexity. It also highlights why such matters of detail are best addressed through the technical standards, which can provide sufficient granularity and flexibility to ensure

[1] The word "particulars" is inherently broad and undefined in the context of the Regulations. Its use has created some uncertainty in other contexts. For example, in the context of disclosure obligations under the Credit Contracts and Consumer Finance Act 2003 (**CCCFA**).

consistency across the banking sector, rather than being prescribed in the Regulations.

d. The maximum period of 6 months for statement data under limb (e) is too short and is inconsistent with the 2-year period for transaction data. This limited time period is inadequate to support valid customer use cases such as a credit assessment of a business that has seasonal variances in activity.

ASB recommendation:

e. ASB recommends that the Regulations reserve the detail of designated data for the technical standards (based on the API Standards) and with clear cross-references to those standards. If the Regulations do specify data categories, they should be limited to the minimum mandatory requirements of the API Standards, with clear definitions to avoid ambiguity and ensure consistency. Alignment with the API Standards is necessary to reduce material operational risk for Data Holders (given the need to create complex new processes that would be duplicative and costly without any benefit to customers).

f. Specifically with respect to sections 7(1)(e) and 7(1)(f) relating to statements, ASB recommends that reference to statements as designated data be limited to a copy of a statement that "the data holder has sent or made available to the customer during the [defined time period before the time of the request under section 15 of the Act]".

The designation should apply to up to 2 years of statement copies, ensuring consistency and supporting customer use cases that require access to historical data.

3. Grounds for refusing data sharing and payments must align to existing financial risk and compliance reasons

a. Sections 16(1)(i) and 20(1)(h) of the CPD Act allows for regulations to prescribe circumstances in which a Data Holder may or must refuse to provide data or complete a payment in response to a request. This is in addition to the other grounds for refusal set out in sections 16 and 20, such as risks to safety or financial harm.

b. It is essential when releasing payments and data to ensure that the CDR does not inadvertently override or dilute the careful risk controls, compliance obligations, and operational safeguards that Data Holders rely on to protect customers, manage legal and regulatory risk, and maintain the integrity of their systems. These reasons are set out in Bank Terms and Conditions with Customers which govern the release of payments and data via the existing channels and electronic facilities (web and mobile). It is important that CDR does not try to create a new regulatory framework that overrides all those risk and compliance controls only for this channel.

c. We suggest that the Regulations create additional reasons that may be used to refuse to provide data or action a request where the Data Holder reasonably considers that doing so would contribute to a breach of any laws/regulations/sanctions in New Zealand or overseas, *as well as* the other reasonable grounds that apply to their other web and mobile channels under Bank Terms and Conditions. This would better ensure equivalency between the CDR regime and the terms that apply to customers' use of digital banking channels under existing account terms and conditions and enable existing compliance processes to be relied on for this additional channel.

d. For example, under ASB's Personal Banking Terms and Conditions, ASB may refuse to act on an instruction or suspend an account for a variety of reasons, including incomplete or inaccurate information, non-compliance with tax or identification requirements, insufficient funds, unclear instructions, suspected fraud or illegality, breach of acceptable use policies, unusual account activity, insolvency, disputes over account ownership, legal requirements, or sanctions compliance. These grounds are broader and more nuanced than those set out in the CPD Act, reflecting the complex and evolving risk environment in which banks operate. As demonstrated by the list, many of these are not "laws", so the grounds for refusal needs to be broader than simply 'compliance with law'.

e. It is therefore critical that the Regulations explicitly recognise and preserve the ability of Data Holders to refuse requests on any grounds that would apply under their standard terms and conditions for electronic banking channels.[2] This also aligns with section 89 of the CPD Act, which provides a defence for Data Holders where a contravention is due to matters beyond their control and they have taken reasonable precautions and exercised due diligence.

ASB Recommendation:

f. ASB recommends that the Regulations should make explicit use of the power in sections 16(1)(i) and 20(1)(h) to make clear that Data Holders may refuse to provide data or perform designated actions on any grounds that would entitle them to refuse or delay a payment or data access request under their standard terms and conditions for electronic facilities.

4. Liability

a. Liability for material risks, including data breaches and security incidents, is not clearly allocated under the current draft Regulations. This creates significant uncertainty for Data Holders, Accredited Requestors and customers.

b. In particular, once customer data is transferred to an Accredited Requestor, or to their downstream partners when acting as intermediaries, it is essential that responsibility for compliance obligations (including under the Privacy Act 2020) is clearly and solely assigned to the Accredited Requestor. Without such an explicit allocation, Data Holders may be unfairly exposed to ongoing liability for data they no longer control and had released on reasonable grounds, and customers will lack certainty as to who is accountable for the protection and appropriate use of their personal information.

ASB Recommendation:

c. ASB recommends that the Regulations be amended to state explicitly that, once data is transferred to an Accredited Requestor (or, where acting as an intermediary, their downstream partners), those parties are solely responsible for compliance with law and regulations pertaining to the data (including the Privacy Act 2020 and the law on breach of confidence) and all related obligations in respect of that information. Accredited Requestors should also be required to indemnify Data Holders for any losses arising from

[2] This could be subject to additional controls or requirements set out in the Regulations, although we submit that is unnecessary where Data Holders are already required to ensure their terms are not unduly restrictive, given other statutory frameworks such as the Unfair Contract Terms regime under the Fair Trading Act 1989.

breaches or unauthorised use of data post-transfer, including use by downstream partners.

d. We have appended the Liability Model work that ASB has previously shared with MBIE for further context. This identifies risks in the ecosystem, and proposes an allocation of risk amongst participants. We would kindly request consideration of this work, as there are risks identified within it which are not covered by the Act or draft Regulations, and would otherwise have to continue to be covered by bilateral contracts.

e. These are categorised into the following:

A. Issues relevant to Customer Data or Action Initiation

1. Reliance on non-compliant or outdated consents
2. Unauthorised or fraudulent requests
3. Security and data breaches
4. Delays and refusal
5. Data errors and inaccuracies
6. Risks of mental/physical harm to customers
7. Payment initiation to high-risk recipients and AML / sanctions compliance

B. Issues as between Data Holders and Accredited Requestors

1. Loss caused by counterparty's breach, fraud, negligence, etc.
2. Insurance adequate to meet losses to counterparty and customers
3. Change in status / conditions / accreditation
4. Intellectual property usage
5. Excessive use of the APIs by Accredited Requestors

5. Insurance / guarantees

a. Regulation 13 of the General Regulations establishes that, as a condition of accreditation, Accredited Requestors must demonstrate that they have "reasonably adequate" cover for liabilities. This can be satisfied by holding one or more contracts of insurance, guarantees, or by maintaining financial resources (self-insurance) to cover potential liabilities to customers and Data Holders.

b. The Regulation does not define what constitutes "reasonably adequate" cover in practical or quantitative terms. There is no minimum threshold, benchmark, or guidance as to what level or type of cover is expected for different classes of Accredited Requestors or activities. This creates uncertainty for both applicants and Data Holders, and risks inconsistent application by the regulator.

c. In addition, the Regulation only requires Accredited Requestors to demonstrate adequate cover at the point of accreditation. There is no explicit obligation to maintain such cover on a continuous basis throughout the period of accreditation. Nor is there any requirement to notify the regulator or affected Data Holders if the insurance or guarantee lapses, is reduced, or otherwise becomes inadequate. This creates a significant risk that, over time, Accredited Requestors may become underinsured or uninsured, leaving customers and Data Holders exposed in the event of a loss.

ASB Recommendation:

d. ASB recommends amending regulation 13 of the General Regulations to require that Accredited Requestors must maintain "reasonably adequate" insurance or financial

guarantees at all times during the period of accreditation, not just at the point of application or renewal. This should be an express, ongoing obligation.

e. In addition, ASB recommends introducing:

   A. a specific requirement that Accredited Requestors must promptly notify both the regulator and all affected Data Holders if there is any lapse or material change in the insurance or guarantee arrangements. Notification should be required within a specified period (e.g., within 5 working days of the Accredited Requestor becoming aware of the change);

   B. a right for the regulator to suspend or revoke accreditation if an Accredited Requestor fails to maintain adequate cover (or fails to notify any lapse). Data Holders should also be entitled to suspend data sharing or designated actions with an Accredited Requestor upon receiving notice (or otherwise becoming aware) that adequate cover is not in place; and

   C. further detail on what is expected in terms of "reasonably adequate" cover under the Regulations, including minimum levels, types of risks to be covered (e.g., professional indemnity, cyber liability), and the specific requirements that will apply for the insurer or guarantor (e.g., a minimum credit rating for insurers).

6. Definition of "electronic facility"

a. The current definition of "electronic facility" in regulation 4 of the Designation Regulations is broad and risks unintentionally capturing a range of services that are not appropriate for inclusion within the scope of the Regulations.

ASB Recommendation:

a. ASB recommends that the definition of "electronic facility" should be updated to make clear that it is limited to standard internet banking and mobile application channels maintained by or on behalf of the Data Holder, and that it excludes services such as ATMs and other channels designed to facilitate information exchange with enterprise resource planning (ERP) systems, and accounting platforms. These services are fundamentally different from the mobile app and website-based systems that are the intended focus of the CDR regime.

b. Regulation 8(2)(e) should also be updated to state that designated payment actions are limited to those that can be made via an "electronic facility" (based on the updated definition recommended above), thereby excluding payments that cannot currently be made through these digital channels.

7. Other points

a. **Access process**

Regulation 6(2) of the General Regulations states that Data Holders must provide Accredited Requestors with access to their systems within five working days of receiving notice of accreditation. However, the regulation is unclear as to what constitutes "access" and what technical or security requirements must be met before integration can occur. It is not clear whether this refers to access to a QA (quality assurance)

environment, or full production access.

ASB recommends that the Regulations are amended to clarify both (i) the point at which the five-day period for providing access commences (i.e. which should be when the Accredited Requestor has satisfied all published technical and security requirements); and (ii) the type of access that must be provided within that period, with a clear distinction between QA and production environments. ASB also recommends that the Regulations provide clear guidance on the technical, security, and onboarding requirements that must be satisfied prior to granting access (and related notice requirements data holders must comply with) and clarify that the five-day period commences only once the Accredited Requestor has met all such requirements.

b. **Joint accounts**

The draft Regulations lack sufficient clarity regarding the obligations of Data Holders in respect of joint or multi-signatory accounts. While section 21 of the CPA Act anticipates that regulations will address the treatment of such accounts, the current Designation Regulations do not directly respond to this – other than noting that designated payments are limited to those that do not require the authorisation of 2 or more persons (regulation 8(2)(d)). There is no further provision for how Data Holders should manage data sharing for joint or multi-signatory accounts.

The draft Regulations should make clear that, for joint or multi-signatory accounts, Data Holders are only required to perform actions and share data in accordance with the account operating authorities that apply to electronic facilities. This means that if a bank's standard electronic facilities allow a single authorised party to view, share data or make a payment, the same rule should apply under the CDR regime. This approach ensures consistency with existing customer authorities, avoids confusion, and maintains the integrity of established account controls.

c. **Loss recovery**

The draft Regulations, together with the CPD Act, do not provide Data Holders with a practical mechanism to recover low-value operational losses from Accredited Requestors. While the CPD Act envisages regulations for recovery of such amounts (see section 59 of the Act), the current draft Regulations do not respond to that. In practice, the primary recourse for Data Holders would be to initiate proceedings which is not proportionate for low-value claims. The absence of a streamlined recovery process also weakens incentives for Accredited Requestors to maintain high operational standards.

We recommend that the Regulations provide for a simple, standardised process by which a Data Holder can notify an Accredited Requestor of an operational loss (a "loss notice"). Upon receipt of a valid loss notice, the Accredited Requestor should be required to pay the specified amount within a defined period (e.g. 20 working days), unless the loss is disputed in good faith.

d. **Recovery relating to consent mismanagement**

Section 40(3) of the CPD Act places obligations on both Data Holders and Accredited Requestors to ensure that the systems are able to give immediate effect to the ending of an authorisation. While this obligation is acknowledged, there is a potential for ambiguity around liability exposure for Data Holders if an Accredited Requestor's system fails to meet this requirement.

This could result in a Data Holder continuing to provide access to data where authorisation no longer exists. The draft Regulations do not clearly provide loss recovery pathways for Data Holders or customers where the above scenario occurs. This may create uncertainty, risk of disputes and may unfairly expose Data Holders to loss, if they provide data based on ineffective consent management.

e. **Implementation & timing**

Based on ASB's discussions with MBIE, it is our understanding that the primary objective for the 1 December 2025 commencement of the Regulations is for data holders to have a live system operational in accordance with the API Standards. If the Regulations do not fully align with the API Standards, then there should be an extended transition period to allow for additional implementation of changes.

As a related point, new functionality, initiatives, and products introduced by Data Holders have the potential to create new categories of data and risks that may not be fully anticipated by the existing CDR regime and Regulations. To ensure that these innovations can be safely and effectively integrated into the open banking framework, we recommend that the Regulations provide for a grace period during which such new offerings can be tested and assessed outside the full scope of CDR compliance obligations. This approach would allow Data Holders and Accredited Requestors to identify and address any operational, security, or compliance challenges in a controlled environment, reducing the risk of unintended consequences or regulatory breaches.

f. **Use of the CDR framework to provide other data available via the "electronic facility" / "electronic system"**

It would be beneficial to allow ecosystem participants to supply data beyond "designated data" via the APIs and rely on this framework, instead of needing bilateral contracts for the additional data. For example, if a customer were to request a small scope increase to the CDR data with some additional fields, it would be useful to have this also governed by these regulations rather than needing to enter a contract for that small amount.

This could be done by allowing participants to use the 'electronic system' mentioned in the Act (which is not a defined term) to supply additional data beyond designated data (so would not meet definition of regulated data service) but still rely on protections afforded under the regulations with respect to liability.

ASB appreciates the opportunity to submit on the draft Regulations. ASB would welcome the opportunity to discuss any aspects of our submission further with MBIE, and to share insights that may enhance the ongoing development of the draft Regulations.