Feedback response on exposure drafts of Open Banking regulations under the Customer and Product Data Act

Volley Payments Limited

29 August 2025

Introduction

We thank MBIE for the opportunity to provide feedback on the draft of Open Banking regulations under the Customer and Product Data Act. We also acknowledge and appreciate the work undertaken by MBIE in developing this regulation.

About us

Volley is a peer-to-peer payments app and acceptance platform for New Zealand, built on top of Open Banking APIs. Our payment app allows Kiwis to create and share payment requests with friends. Payments can be approved by using existing bank apps without needing to install the Volley app. Our acceptance platform enables businesses to easily accept funds using payment links or QR codes. Volley is integrated with ANZ, ASB, BNZ and Westpac and uses both account information and payment initiation.

We're committed to standards-based access methods and operate exclusively with contractual Open Banking APIs. We strongly support the transition to regulated Open Banking. This regulatory framework is essential for ensuring accredited requestors deliver safe, secure and trusted services to Kiwis.

Our feedback is based on our extensive experience in the Open Banking industry in New Zealand, both as a third-party participant and as a contributing member to standards development via the API Centre.

Feedback

Section 6 (Banking and other Deposit Taking)

Section 6 designates data holders under the Customer and Product Data Act. The proposed draft designates five banks; ANZ, ASB, BNZ, Westpac and Kiwibank, plus any deposit takers that choose to opt in.

We commend designating these banks, however the designation does not cover other registered banks such as TSB Bank, The Co-operative Bank and Heartland Bank. The omission of these banks restricts accredited requestors from providing services that cover the full consumer market. Therefore, customers of these banks won't be able to access the same Open Banking enabled services as customers of the designated banks.

We recommend expanding data holder designation to include at least; TSB, The Co-operative Bank and Heartland Bank. This would provide wider coverage for New Zealand consumers, improve accredited requestor participation and ensures Open Banking promotes fair market competition rather than entrenching market structures.

Section 9 (Banking and other Deposit Taking)

Section 9 establishes classes for accredited requestors, as either intermediary or non-intermediary and further distinguishes these classes between entities making requests as data requestors or payment initiators. The current class definitions appear to assume a commercial relationship exists between all parties involved in a data or payment transaction, which suggests a gap for existing non-commercial use cases enabled by the Open Banking standards including peer-to-peer payments.

As an example of a typical peer-to-peer payment scenario supported today by the standards, a user (B) creates a peer-to-peer payment through an accredited requestor (A) and shares it with their friend (C). The friend then

uses the same accredited requestor (A) to approve a payment from their account (C) to the original user (B).

The intermediary definition in subsection (2) is unclear with regards to this peer-to-peer scenario because it requires a contract between B and the customer (C) for goods/services and states that the data sharing/payment facilitation must be "reasonably necessary" for B to provide goods/services to C. Since this is a non-commercial transaction, there's usually no contract between the user (B) and the friend (C).

When assessing against the non-intermediary class, the primary purpose of the accredited requestor (A) making the request is to fulfil the user's (B) payment request rather than providing services to the friend (C). The second requirement may also fail as the test assumes the user (B) provides goods or services to the friend (C), but in a peer-to-peer transaction, no such commercial relationship or provision of goods and services may exist.

We suggest further clarity from MBIE over the accredited requestor classes is necessary, particularly for non-commercial use cases which are already supported by the Open Banking standards, such as peer-to-peer payments. Regulatory support for peer-to-peer payments will also ensure parity between designated actions and exisiting customer actions via traditional bank channels, allowing for any payment that can be made from a banking app to be similarly performed by an accredited requestor.

General observations

Use of unregulated access methods

We note that the exposure drafts do not yet consider the ongoing usage of unregulated access methods (also known as screen-scraping or reverse engineered APIs) by accredited requestors.

While Volley acknowledges that there is a need for a "transition period", where existing unregulated access methods will continue to be used before widespread uptake of regulated access and standards, we believe that regulations must adopt a clear position on the allowing operation of access methods for accredited requestors under the consumer data right regime.

Risks to consumers due to use of unregulated access methods

Volley would like to note that unregulated access methods pose ongoing and present risks to consumers not seen in standards-based access methods:

- **Lack of consent controls:** where regulated standards-based access gives consumers explicit control over the data they share or payments they approve to accredited requestors, unregulated access methods involve customers giving their banking credentials to a third-party, which they store (usually in the form of a long-lived token) and use to repeatedly access the customer's bank account, with no limitations to prevent usage outside of the implied consent given by the customer.
- **Behavioural conditioning to phishing scams:** unregulated access methods have resulted in consumers being conditioned to provide their bank account credentials to third-party websites. Scammers are able to easily target this behaviour by creating high quality fakes (either of the bank website, or a realistic looking third-party service) that leverage this same behaviour to steal credentials and gain full control of customer bank accounts via phishing. Volley would also like to note that thanks to new AI-

based tools, creating realistic scams is now easier than ever before and we expect the incidence of these types of phishing scams will increase as a result.

- **Bypassing of data transfer rules:** unregulated access methods like screen-scraping are able to access account data or execute payments that contradict data transfer and execution rules set out in standards that will be adopted under the CPD.

Regulated standards-based access methods offer an opportunity

Standards-based access methods solve these problems and offer a real opportunity to significantly reduce the prevalence of common credential-stealing scams, however the degree to which this will be realised depends on education of consumers towards secure methods of authentication (OAuth, via standards) and away from credential sharing.

Volley recommend that regulations create a clear distinction for consumers to understand when they are using regulated standards-based access methods as opposed to higher-risk unregulated access methods, including:

- Clear determination of the specific standards methods of data access that are expected to be provided by data holders and adopted by data requestors.
- A requirement that accredited requestors must not offer standards-based access methods in tandem with unregulated access methods within the same product or service. For clarity, our suggestion would be that unregulated access methods can still be available as a “legacy” product, and data requestors should use the transition period to migrate their activity from one product to the other.
- A requirement that accredited requestors should present a warning to consumers on legacy products that use unregulated access methods.

Risks introduced by a passive mitigation of unregulated access

Frollo, a third-party Open Banking provider accredited under the equivalent Australian CDR regime, recently released a report on the State of Open Banking. In this report they state that the current approach of the CDR regulation has been to “[rely] on a passive deterrent: assuming that increased use of multi-factor authentication and stronger security controls will make screen scraping unviable over time.” The authors concluded that "without a clear position from the government, we're in a grey zone, which creates confusion for consumers, adds compliance risk for industry, and undermines the core promise of the CDR," and that "the government needs a clear, unambiguous policy outlining the sunset of screen scraping – or, at the very least, it needs to implement strict guardrails.”

In New Zealand, we face a similar scenario where there’s no clear guidance or policy outlining the phasing out of unregulated access methods. We believe this will create significant consumer confusion, fail to reduce the prevalence of phishing scams and ultimately undermine the core tenet of the CPD Act to “[empower] consumers to access, control, and share their data securely”.

Thanks

We thank MBIE for considering our feedback. We appreciate the chance to share our thoughts and welcome further opportunities for industry engagement.