

29 August 2025

Ministry of Innovation, Business, Innovation and Employment
Wellington

By email: consumerdataright@mbie.govt.nz

SUBMISSION on Exposure Draft Customer and Product Data (General Requirements) Regulations 2025

1. Introduction

Thank you for the opportunity to make a submission on the Exposure Draft Customer and Product Data (General Requirements) Regulations 2025 (the Regulations). This submission is from Consumer NZ, an independent, non-profit organisation dedicated to championing and empowering consumers in Aotearoa. Consumer NZ has a reputation for being fair, impartial and providing comprehensive consumer information and advice.

Contact: Aneleise Gawn
Consumer NZ
Private Bag 6996
Wellington 6141
Phone: 04 384 7963
Email: aneleise@consumer.org.nz

2. Comments on the Regulations

We broadly support the Regulations as a foundation for a safe and competitive open banking regime. However, given the two-week time frame for making submissions we have been unable to undertake a

clause-by-clause analysis of the Regulations and only wish to make the following high-level comments.

System access

We support the requirement for data holders to give accredited requestors access to their systems within 5 working days of receiving written notice that the accredited requestor has become accredited. We consider this is a positive step for competition and ensures a relatively prompt service.

General accreditation requirements

We support the requirement for accredited requestors to hold adequate insurance or other financial coverage. We consider this is an important consumer protection.

Charges

We are concerned with the lack of detail about charges. As stated in previous submissions, we do not think data holders should be able to charge for providing data held about customers.

Also, if data holders (banks) are allowed to charge excessive or opaque fees to accredited requestors these costs will likely be passed on to consumers. Such fees may deter innovation, entrench incumbents, and restrict consumer choice.

Reporting requirements

Requiring accredited requestors to report major events such as insolvency, litigation, or change of control is crucial for consumer trust and integrity in the system.

Annual reminders to consumers about active authorisations is a positive step toward reducing permission fatigue and unwanted ongoing access.

However, we encourage consideration to be given to a mechanism that would allow consumers to see and manage their active consents at any time, not just once a year.

Addressing insecure credential sharing practices

Finally, we consider further thought should be given to the issue of insecure credential-sharing practices, such as requiring consumers to enter their online banking usernames and passwords into third-party platforms (e.g. screen-scraping or credential-harvesting practices). These

methods, while currently used by some payment providers in New Zealand, undermine basic cybersecurity hygiene and have contributed to the normalisation of risky behaviour i.e. consumers willingly sharing their banking credentials, making them more vulnerable to scams.

In the UK, third parties have to use regulated, secure, API-based access and implement strong customer authentication. This has effectively outlawed screen-scraping services. The Australian government is also considering a ban on screen-scraping.

Thank you for the opportunity to provide comment.

ENDS