National Security Group
Department of the Prime Minister and Cabinet
Level 8 Executive Wing, Parliament Buildings
Wellington 6011

By email only:
infrastructureresilience@dpmc.govt.nz

7 August 2023

Dear Sir / Madam

RE: **Strengthening the resilience of Aotearoa New Zealand's critical infrastructure system – consultation**

Mastercard welcomes the engagement by the Department of the Prime Minister and Cabinet (DPMC) with industry and we thank you for the opportunity to respond to the consultation to inform the development of options for regulatory reform to enhance the resilience of critical infrastructure in New Zealand.

Background on Mastercard

Mastercard is a technology company in the global payments industry that connects consumers, financial institutions, merchants, governments, digital partners, businesses, and other organizations worldwide enabling them to use electronic forms of payment.

Our core payment network supports what is often referred to as a "four party" payments network and includes the following participants: an account holder (a person or entity who holds a card or uses another device enabled for payment), an issuer (the account holder's financial institution), merchant and acquirer (the merchant's financial institution). Through our core payment network, we work with issuers and acquirers (who are participants on our network) to enable the routing of a transaction to the issuer for its approval, facilitate the exchange of financial transaction information between issuers and acquirers after a successfully conducted transaction, and settle the transaction by facilitating the exchange of funds between parties via settlement banks. We do not issue cards, extend credit, determine, or receive revenue from interest rates or other fees charged to account holders by issuers, or establish the rates charged by acquirers in connection

with merchants' acceptance of our products. In most cases, account holder relationships belong to, and are managed by, our customers.

An increasingly digital and interconnected world provides greater convenience and opportunities for people, businesses, and governments. At the same time, there is an increased need to strengthen protection against threat actors who seek to exploit this technology through increasingly sophisticated and innovative ways. The Mastercard network is designed to ensure safety and security everywhere we operate. We continuously invest in developing and delivering world-class, scalable cybersecurity solutions.

Consultation response

1. Mastercard is supportive of steps being taken in New Zealand to optimize approaches towards the resilience of critical infrastructure that are essential to the functioning of society, the economy, public safety and security, and the provision of public services, particularly given the unique hazards and threats posed by New Zealand's complex geography and potential costs associated with outages and failure.
2. In assessing reform options, we believe that the Government will take the right course by considering an iterative, principles-based, and proportionate approach to managing risks as we have seen work effectively in other markets.
3. Mastercard offers the following general and specific comments and feedback in relation to the consultation that we hope would be helpful to the DPMC:
    i. As a starting point, we believe the Government should undertake further consultation and information gathering to establish:
        a. whether and what infrastructure or infrastructure services are considered 'critical',
        b. an understanding of the roles different organisations play across different industries and sectors and their interdependencies, and
        c. a geographical connection between the critical infrastructure asset and New Zealand.

    This will help give certainty to affected entities as to their future regulatory obligations and how to meet them, recognising the regulatory burden and costs associated with the proposed enhanced critical infrastructure requirements in New Zealand.

ii. In general, we observe that any proposed regulatory framework should incorporate flexibility to include and accommodate robust risk management programs, processes and procedures that are designed for each businesses' operational needs and budgets to support the delivery of services that are critical to New Zealand and businesses.

iii. We agree with an approach to regulation that builds on existing and forthcoming laws to achieve broader resilience objectives.

iv. To future-proof New Zealand's emergency management regulatory regime we agree it makes sense to retain and implement the proposals in the Emergency Management Bill which is expected to be introduced in 2023, including a new definition for critical infrastructure; and note that the Bill will expand upon those entities already listed as 'lifeline utilities' to 'critical infrastructure' under the *Civil Defence Emergency Management Act 2002* (CDEM Act) as well as leverage the roles and responsibilities for hazard readiness, emergency response, and recovery that exist already in the CDEM Act.

Building a shared understanding of issues fundamental to system resilience

4. We agree with the principle that comprehensive sharing of information is necessary to foster a culture of trust and transparency.

5. We are supportive of enhanced, coordinated proportionate information sharing with, and between, critical infrastructure owners and operators on key issues impacting resilience and potential mechanisms for example, the reporting of cyber incidents.

6. Optimizing New Zealand's national cyber resilience and capabilities should extend to building upon existing information sharing networks, relationships, and frameworks to drive stronger intelligence and cyber threat sharing practices leveraging the expertise of the New Zealand Security Intelligence Service and Government Communications Security Bureau (GCSB). We note that from 31 August 2023, work will commence to create a dedicated new lead operational agency in New Zealand to strengthen cyber security readiness and response by integrating New Zealand's Computer Emergency Response Team (CERT NZ) into the National Cyber Security Centre (NCSC).

7. We caution that, without exemptions or protections that apply to the disclosure of certain sensitive information, there could be potential impacts to competition in a small, concentrated market such as New Zealand as a result of regulators having access to, and storing highly commercially sensitive information on systems other than those belonging to

the relevant organisation; as well as the additional risk that such information could be subject to disclosure pursuant to a request made under the *Official Information Act* (OIA).

8. Providing transparency, assurance and certainty to the industry and participants on the treatment of business sensitive and confidential information, including through the establishment of formal legislative powers and secrecy provisions to enable the collection of certain business-sensitive information, is necessary to ensure the full exchange of information and improve engagement with organisations.

Managing significant national security risks to the critical infrastructure system

9. We are supportive of the Government having greater powers to provide direction or intervene in the management of significant national security threats at a national level against strict criteria of recovery and prevention in the national interest. We think any such power should be exceptional and used as a last resort to avoid the potential for an open-ended power enabling Government intervention and oversight and the risk of determinations by sector or other regulator being open to challenge or reopened otherwise than in very limited situations.

10. Transparency on the proposed power is needed to give industry clarity about regulatory approaches and requirements in order to respond to future developments and prepare for compliance associated with such power; as well as to reduce regulatory burden and costs.

Creating clear accountabilities and accountability mechanisms for critical infrastructure resilience

11. Mastercard is supportive of and sees the benefit in having a single agency as the central coordinator for the resilience of New Zealand's critical infrastructure system, and to develop corresponding policy and regulatory requirements within that agency. This will help to provide certainty and reduce regulatory compliance burden.

12. Given that a level of resourcing and capability will be required, we believe it would be advantageous for an existing agency such as the Ministry of Business, Innovation and Employment (MBIE) to fulfil this function.

Further discussion

Mastercard appreciates the opportunity to comment on the proposed development of a regulatory approach to delivering a resilient critical infrastructure system. We would be pleased to meet with

the DPMC to discuss the contents of our submission further and to provide feedback on potential reform options.

If you would like to discuss the contents of our submission, or require additional information, please contact me via email at ruth.riviere@mastercard.com or Ali Steele, Senior Counsel at ali.steele@mastercard.com

Yours sincerely,

Ruth Riviere
Country Manager, New Zealand & Pacific Islands