Mastercard
Australasia
Mastercard House
Level 3, 136 Customs Street West
Viaduct Precinct, Auckland 1010
New Zealand

tel +64 9 375 5020

www.mastercard.co.nz

Dynamic Policy Team
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

Via email: cyberresilience@rbnz.govt.nz

5 February 2021

To whom it may concern

Thank you for the opportunity to comment on the *Risk management guidance on cyber resilience and views on information gathering and sharing* consultation document. As a leader in facilitating global commerce via our safe, secure and innovative payments infrastructure, Mastercard is pleased to provide relevant insights on cyber security threats and the security protocols and built into our proprietary technology.

Mastercard is a technology company in the global payments industry connecting consumers, financial institutions, merchants, governments, digital partners, businesses and other organisations worldwide, enabling them to use electronic forms of payment instead of cash and cheques. Through Mastercard's unique and proprietary global payments network, which we refer to as our core network, we switch (authorise, clear and settle) payment transactions and deliver related products and services. Our payment solutions offer customers choice and flexibility and are designed to ensure safety and security for the global payments system.

Mastercard agrees the cyber threat landscape is evolving rapidly and supports the Reserve Bank of New Zealand's (RBNZ) intention to enhance the security and resilience of the local financial system. Cyber risks have been amplified by the COVID-19 pandemic as more payments have shifted online. As the RBNZ acknowledges in it's *The Future of Cash – Te Moni Anamata* workstream, New Zealand is well on the way to becoming a low cash use economy, making cyber security and the resilience of the financial sector a critical economic consideration.

Mastercard's approach to security and resilience

For payments networks around the world, cyber security risks have significantly increased in recent years, driven by the use of the internet and telecommunications technologies for financial transactions, and the increased sophistication and activities of organised crime, hackers, terrorists and other external parties. Cyber threats may derive from fraud or malice on the part of external or internal parties or may result from human error or accidental technological failure. Threats include cyber-attacks such as computer viruses, malicious code, phishing attacks or information security breaches and could lead to the misappropriation of consumer account and personal information, identity theft or severe disruption to the processing and settlement of payments in an economy.

Mastercard's freedom to operate relies entirely on our ability to provide secure processing, transmission and storage of confidential, proprietary and other information and technology in our computer systems and networks, as well as the systems of our third-party providers.

Our customers and other parties in the payments value chain, as well as account holders, rely on our digital technologies, computer systems, software and networks to conduct their businesses As a result, cyber security and the continued development and enhancement of our controls, processes and practices designed to protect our systems, computers, software, data and networks from attack, damage or unauthorised access is our highest priority.

As the developer and operator of digital payments technology, Mastercard makes extensive and ongoing investments in security, not only to protect our proprietary assets but across the payments ecosystem, supporting cardholders, merchants and financial institutions To maintain the security of our ecosystem, we offer integrated products and services that prevent, detect and respond to fraud and cyber-attacks and to ensure the safety of transactions made using Mastercard products along the entire payments value chain. We do this using a multi-layered safety and security strategy·

- **Prevent** - this layer protects infrastructure, devices and data from attacks An example is the development and use of EMV chip and contactless security technology to reduce fraud
- **Identify** – this layer allows us to help banks and merchants verify the authenticity of consumers during the payment process using various biometric technologies, including fingerprint, face and iris scanning, to verify card use and reduce fraud.
- **Detect** – this layer exposes fraudulent behaviour and cyber attacks and takes action to stop these activities. Our offerings include alerts when accounts are exposed to data breaches or security incidents and network-level monitoring on a global scale to help identify the occurrence of widespread fraud attacks when the customer (or their processor) may be unable to detect or defend against them.
- **Experience** – this layer improves security for merchants and cardholders, for example, by enhancing approvals for online and card-on-file payments, to the ability to differentiate legitimate consumers from fraudulent ones.

We also provide services that mitigate cyber risk in the payments ecosystem. For example, we recently launched Mastercard ThreatScan, an AI-powered solution that helps banks proactively identify potential vulnerabilities in their authorisation systems. The service works alongside an issuer's existing fraud tools, imitating known criminal transaction behaviour to identify potential weaknesses and prompt action to prevent security breaches.

The draft guidance

Mastercard agrees the RBNZ's "moderately active" policy stance is the optimal means of promoting cyber resilience within the financial sector. The proposed guidance, rather than a prescriptive checklist, enables businesses like Mastercard that are already well-advanced on mitigating cyber risk to meet the RBNZ's expectations to deliver a more robust financial system from current programs of work. Principles rather than prescription also means the guidance is positioned to drive more security-conscious cultures within organisations, as well as remain relevant in the face of evolving cyber threats. As a global company, we support basing the guidance on international standards and protocols, as this means we can deploy a consistent approach across our business as a whole and reduce unnecessary administrative burdens

Information gathering and sharing

Around the world, Mastercard works closely with system regulators and government authorities to share intelligence and insights on the cyber threat landscape, as well as report on cyber readiness and on incidents to the appropriate body in each jurisdiction. We broadly support the RBNZ's proposal for a coordinated and collaborative approach to information gathering and sharing to the extent that such an approach streamlines monitoring and reporting lines rather than imposing multiple obligations. However, Mastercard reserves its full support until we see more detail on the information required, the timing and format of

reports; relevant materiality thresholds; and other critical matters. We would be delighted to share our global experience on best practice cyber data collection and information sharing with RBNZ as to develop a bespoke framework for New Zealand.

Thank you again for the opportunity to comment on the consultation document. If you would like discuss any issue we have raised further or require additional information, please contact Chris Siorokos, Director, Public Policy – Australasia, on [redacted]

Yours sincerely

[redacted]

Ruth Riviere
Country Manager – New Zealand and Pacific Islands