# Submission on discussion document: *Options for establishing a consumer data right in New Zealand*

## Your name and organisation

| | |
|---|---|
| **Name** | Lucy Jezard |
| **Organisation** | Mastercard |

## Responses to discussion document questions

**Does New Zealand need a consumer data right?**

1 *Are there any additional problems that are preventing greater data portability in New Zealand that have not been identified in this discussion document?*

- As a major participant in the global payments industry, Mastercard has a stake in policy development affecting financial systems in countries where we operate. In responding to the Inquiry, we consider the interests and perspectives of consumers, businesses, industry participants and other stakeholders in the payments industry as well as the financial system.
- Our perspective is further informed by our role as a trusted service provider to a significant number of retail banks worldwide, our experience of payment services regulation and our role in receiving and processing data in the context of our wider business. Accordingly, our response focusses primarily on the finance sector.
- An important factor as part of a consumer data right is that with everything becoming digital, we need to look ahead and ensure consumers are fully informed as to how their data will be used and protected.
- Any sustainable and growing business ecosystem must drive value to those that participate. A key component of value is commercial (fees and charges) viability. A set of commercial principles laid out would assist in investment and growth; as opposed to a compliance or tick box approach from participants.

2 *Do you agree with the potential benefits, costs or risks associated with a consumer data right as outlined in this discussion document? Why/why not?*

- Mastercard believes MBIE has captured the benefits and challenges well in this section.
- We agree that the principal driver for developing a consumer data right is centralised on consumer choice, convenience and innovation in how consumers allow the use of their data to provide better experiences and benefits in banking, such as enhanced ways to understand and manage their finances.
- The key adoption risks are security and data privacy – specifically around consumer education and how consumers can safely share their data with a good understanding

of what it means. As consumers, we're constantly reminded not to share secure details and be wary of phishing. A CDR will be asking consumers to start doing the opposite. Ensuring the right security measures are in place is paramount, followed by an obligation to ensure consumers know how to do this safely and can proactively control their data. Therefore, data recipients must be subject to clear and high standards as to the protection of data and expectations for the necessary control environment (including how it will be overseen) should be worked through as part of developing the CDR.

- In response to section 12 (page 9) regarding digital acceleration as an outcome of COVID-19, we agree that a CDR in the banking sector could see the development of alternate payment solutions providing reduced fees, greater convenience and security. However, we also believe that businesses and consumers in New Zealand already have access to a number of safe, simple, secure and cost-effective ways to pay, and be paid – in store, on mobile and online. As we work together to create the convenient and secure payment systems of the future, we require business models that allow for continuous investment to deliver these outcomes. Please see appendix for further information.

| | |
|---|---|
| 3 | *Are there additional benefits, costs or risks that have not been explored in the above discussion on a consumer data right?* |

- **Risk:** CDR success is dependent upon consumer awareness and willingness to share their data. RFi Research (2018) shows that whilst consumers indicate a level of trust in banks to maintain the privacy and security of their personal information, rated 7.7 out of 10, this confidence drops when asked the same of Fintechs and tech giants, rated as low as 2.9 out of 10. We know trust and security is incredibly important, so promoting awareness and education will be paramount. The objective is to encourage rapid adoption of the consumer data right, avoiding the low and slow take-up as seen in some other markets. If consumers are unwilling or unable to easily share their data, there is a risk to the return on investment for market entrants
- **Risk:** data is compromised in transit or via intrusion into recipient's technology that causes third parties to secure and use this data. Much like intrusions into merchants' payment gateways where consumers' personal and card information is taken.
- **Cost:** compliance costs – Australia's CDR has demonstrated that legislation has a large compliance/regulatory burden, to the extent that other major programmes of work had to be put on hold in order to deliver CDR to market.
- **Cost:** an accreditation entity needs to be considered – how to set this up and then maintained on real-time/regular basis rather than a one-off instance. Included in this are the onboarding and directory services (API calls), how these are both managed and maintained.
- **Risk:** an accreditation entity should be rigorously vetted to ensure appropriately high levels of security standard are maintained and that privacy controls, including access to and use of data, are in place. This should be done upfront and on an ongoing basis.
- **Risk:** liability and enforcement – working through how liability is determined as standards should be clearly articulated and appropriately calibrated; additional

factors to consider are safe harbour and who would be responsible for enforcing these rules.

- **Cost:** facilitating redress when something goes wrong – who is responsible for managing and maintaining this requirement, including the associated cost.

4 *What would the costs and benefits be of applying the consumer data right to businesses and other entities, in addition to individuals?*

- There is a general advantage of a consumer data right with a broader application that increases competition, encompasses speed, simplicity and ensure that consumers are getting the right product, at the right time for their needs; this applies to both consumers and businesses.
- **Benefit:** certain segments such as small and medium business (SMB) SMB could benefit. SMB is often considered an underserved segment and a CDR could greatly improve customisation, meeting the personalised needs for not only SMBs, also for their end customers. Examples of this could be improved cashflow and reduced approval times for accessing working capital; improved SMB onboarding and reconciliation; liquidity management.
- **Benefit:** specific industry verticals that have a natural complimentary relationship could be augmented by the application of a CDR. Compounding the benefits across both selected industry verticals and consumers
- **Risk:** the ability of all businesses to support a CDR, i.e. small businesses may not have the resources to manage and leverage this in the most effective way. For example, insufficient digitised financial records which can be used to drive insights and enable decisions. This would equally extend to education – a consumer and business owner has different data sets and decisions to make. Ensuring they have enough education and understanding to make informed decisions. There should also be a level playing field so that new or existing players are not disadvantaged.

5 *Do you have any comments on the types of data that we propose be included or excluded from a consumer data right (i.e. 'consumer data' and 'product data')?*

- Only consumer data that can be utilised to drive a more refined insight, decision or position should be accessed. Asking for data that does not improve the consumer's position or knowledge and is only for the sake of asking should not be shared.
- **Product Data:** we can see the potential for this to enhance the consumer experience through transparency and broader knowledge of the product, such as fees or costs, plus the benefits and risks of the product allowing the consumer to make a more informed choice before purchase.
- **Derived Data:** we see a CDR being able to set forth principles that help the industry to distinguish 'provided' or 'observed' data from derived data. Such principles should be specifically applied to each sector by industry or Government interpretation. We respect the shared interest and ownership of data by both the holder and the consumer. We also note that intellectual property ownership improves societal benefits and accelerates competition and innovation – consistent with the aims of the CDR. This necessary tension should be addressed via legislative principles.

6 *What would the costs and benefits be of including both read access and write access in a consumer data right?*

- **The Collective Power of *Read* and *Write*:** *Read* access is foundational to a CDR; with *write* access delivering the outcomes the CDR seeks.
    - Lacking *write* access, the CDR is a tool for consumers to *access* their data; it is not a means by which consumers can easily *act* upon the insights they derive (or empower others to easily act on their behalf).
    - We appreciate the motivation to take a staged approach; however, we argue that the transformative power of the CDR resides not in the ability to *access* data, but in its ability to *action* it with consent from the consumer.
    - If personal information is to be equally protected and valued under the law, as are personal financial resources, then the cost/benefit evaluations of the former should be subject to the same risk thresholds as the latter. That is, the risk mitigants required for *read* access should be strong enough to mitigate the risks of *write* access as well.

**BENEFITS:**

- ***Read* delivers insights**: Read access delivers foundational benefits of open data, enabling consumers to view and interpret their financial circumstances. Benefits of read access include:
    - **Account aggregation**: simplified customer experience by consolidating various account data into one dashboard, including multi-user aggregation that delivers transparency across businesses and households.
    - **Personal financial management:** providing consumers with enriched insights, services that categorize and allow self-categorization, provide consumer financial health scoring, offer socio-demographic peer benchmarking, and more. Financial management for SMB includes liquidity and cash management (forecasting based on historical data and spend patterns); aggregated view of all accounts; tracking and automaton of recurring payments with easier reconciliation; improved credit scoring to serve underbanked SMB.
    - **Enhanced credit profiling:** providers can improve credit scoring and increase access by augmenting risk models with account information data – particularly those with "thin files" – to both improve the veracity of credit reporting and increase access to financial products.
    - **Decreased switching costs:** competitive financial providers may, with customer consent, utilise account information to more easily 'port' a consumer's financial accounts (automatic payments, salary deposits, etc.) to a new provider.

**RISKS:**

- ***Write* creates action:** Write access empowers the third party in the relationship between consumers and financial institutions to act in different ways than with read access. The standing or accreditation of that third party is critically important. The CDR construct is intended to provide a considered way to engage with this issue.

However, given the increased risks associated with write access, there are specific issues to be addressed as write access is considered and developed:

- **Fraud, data security and wrongful use of data provided:** we note that the industry is still working through security and other issues relating to read access. We think that the approach should be sequential with these issues relating to read access being resolved before write access implementation moves ahead. Phased implementation and gradually expanding functionality will ensure all stakeholders have sufficient adoption time to address related technological challenges.

  A key point is stakeholder reassurance that the write access framework has adequate safeguards and protections for consumers in relation to fraud and data security and to minimize the risk of data breaches. As has been regularly demonstrated, fraudsters will quickly exploit any system weakness. In the case of write access, this is of particular concern for vulnerable consumer groups, all the more so if this goes to transactions for which dispute resolution mechanisms are not fully developed.

  Further, if data is provided for a specific purpose related to the processing of a payment or is otherwise intended to change the relationship of the consumer and the relevant financial institution, it should not also be used so as to change the relationship of the consumer with the third party providing open banking services.

- **Collaboration around problem and dispute resolution:** given the potentially increased risks with write access (as outlined above) we believe that the Government must ensure that these rules are robust enough to deal with the points of difference between read and write access. The industry needs a standardised way of dealing with communications and issues, even before they turn into actual disputes. Mastercard urges MBIE to consult with industry and consumer stakeholders to ensure that the CDR dispute resolution mechanisms are enabled that are fit for purpose, in an environment with write access. We hope this will be in a way that balances the needs of participants and encourages uptake of services within the data sharing ecosystem. We note here that industry enabled solutions do have a potential role: we make this comment as an organisation that supports our network participants in resolving issues arising (e.g. via our chargeback mechanism) across our global network.

**OTHER CONSIDERATIONS:**

- ***Read* access bears most of the risk**: the risks of *read* access are the improper exposure of personally identifiable information. As such, the CDR should seek to:
  - **Prescribe a plain-language, consistent consent management process:** consumer trust is predicated on clear, informed consent. The ecosystem should not permit third parties to create bespoke, confusing, or term-laden consent processes; rather, an industry-wide approach should be taken.

- **Implement and maintain real-time directory services:** upon which data holders can legally rely when approving a response to a *read* API request, as attestation to the accreditation of the third party.
- **Actively monitor and 'score' the ecosystem for fraud:** the CDR should consider implementing a service that actively *risk scores* the API behaviour across the network, in much the same way Mastercard detects network fraud, based on abnormal activities of third parties. The identification of suspected fraud, based on a score, should constitute good reason for a data holder to decline *read* requests for cause, even when requested by an accredited entity.
- **Deploy mitigants via technical service providers that aggregate API calls:** De-risk the ecosystem by relying on intermediaries to implement and support the enforcement of the mitigants, at scale. For example, ensure that a technical service provider builds real time directory checks, actively monitors fraud, and/or utilises a common consent module across data recipients. This reduces variation amongst third parties and reduces risk. We envisage that as part of the value chain, the technical service provider will be competitive, i.e. one central infrastructure could introduce systemic risk. It would be helpful if the CDR recognises a role to be played by technical intermediaries.

## What form could a consumer data right take in New Zealand?

| | |
|---|---|
| 7 | *Do you have any comments on the outcomes that we are seeking to achieve? Are there any additional outcomes that we should seek to achieve?* |

- Mastercard agrees with the proposed outcomes – starting with the consumer, empowering them with control of their data and ultimately the opportunity to source better products, leading to improved money management for long-term financial health.
- Increased transparency should also be an outcome. Having a clear understanding of how their data will be used will enable consumers to better exercise control over their data.
- Increased innovation and enabling new parties into the ecosystem are paramount to bring about positive outcomes for consumers.
- Outcomes should include principles such as speed and simplicity, i.e. decision times, improved customer experience, and the right product, at the right time for consumers as their needs evolve over time.
- Defined and measurable outcomes should be developed to assess and ensure the outcomes are achieving what we all intend them to – e.g. SMB improved decisioning times in order to access working capital reduces from X days to Y days.

| | |
|---|---|
| 8 | *Do you have any comments on our proposed criteria for assessing options? Are there any additional factors that should be considered?* |

- The criteria proposed are relevant and keep the consumer at the centre. Trust is critical for consumers to have the confidence in the CDR.

- **Trust** – we suggest this is broadened to include dispute resolution and issues such as consent – i.e. if data is shared securely, but without consent, how do we maintain trust by supporting consumers when something goes wrong, even if the right safeguards in place.
- **Simplicity** – we suggest that simplicity is key to support consumers' access into sharing data. Removing complexity that is likely to prevent consumers from understanding a CDR and supporting consumers on how to use it effectively, with informed decision-making in place.
- **Reach** – this is key as it will provide consistency for consumers to understand how they can share their data, including the benefits and risks. If the option is not scalable across industries, this could lead to confusion for consumers, resulting in less adoption and therefore the benefits of a successful CDR may not be realised.

| | |
|---|---|
| 9 | *Do you have any comments on the discussion of Option one: Status quo?* |

- **New Zealand is a valuable global testing ground for industry-led innovation** to the extent that unless New Zealand's regulation materially mirrors other regimes and enforces conformity beyond baseline enablement, we risk ceding our 'test market' status to other larger or more lucrative jurisdictions globally. Innovation requires an instigating force; in this case, a principles-based, enablement-focused CDR may provide the impetus to accelerate industry-led innovation. It is crucial for a CDR to establish the lowest common denominator necessary to seed innovation, not to prescribe the innovation itself.
- **The Payments New Zealand API Centre** to which Mastercard is a party continues to be a crucial contributor to standardising the technical aspects of the CDR when applied to the banking sector. However, with a *status quo*, Payments New Zealand is unable to prescribe commercial adoption, and the technical focus will remain in the banking sector.

| | |
|---|---|
| 10 | *Do you have any comments on the discussion of Option two: A sectoral-designation process?* |

- **Sector designation is appropriate and effective for the New Zealand CDR.** This approach enables the Parliament to define market-wide principles (trust, simplicity, reach), that permeate across sectors. Industry and Government can thereafter set forth the most pragmatic, efficacious approach to deliver against the principles.
- **Up-front multi-sector designation is useful**. When several sectors are designated from the outset (e.g., financial services, telco, dairy), this encircles the conversation and mitigates against siloed implementations of the CDR principles.

| | |
|---|---|
| 11 | *Do you have any comments on the discussion of Option three: An economy-wide consumer data right?* |

- Whilst this approach would provide a consistent and standardised application across the entire economy and provide a more uniform experience for consumers, this could take a significant amount of time to deploy and risk certain innovations, as broad rules would need to be applied that aren't sector specific.

| | |
|---|---|
| | • For the Australian CDR, banks struggled to find the technology talent or resource required to build API suites. We envisage that this issue would be compounded if all industries were required to implement at the same time. We have seen in Europe that despite several years in preparation, they are still struggling to implement at the required level.<br>• As suggested, this option may be more difficult to manage across the entire economy, requiring significant time and resource to effectively govern.<br>• If CDR is applied economy-wide this would create greater risk for fraud as there would be a wider inclusion of sectors that may not have the appropriate and required security and fraud measures; applying across the entire market would compound this issue. |
| 12 | *Do you have any comments on the discussion of Option four: Sector-specific approach?* |
| | • A sector-specific approach would allow tailored solutions to certain industry issues (that could differ widely between industries) without having to reverse engineer the secondary legislation to fit a potentially semi-relevant regulatory framework as described in Option 2.<br>• This approach works well for markets that have the right level of legislative governance and controls, such as the financial sector. However, we suggest that some sectors would benefit more from Option 2, where there is less rigor around legislation compared to financial services, and where there is strong propensity to adopt new technologies.<br>• Considering the end consumer, more education and awareness would be required, even more so than Option 2 as data sharing experiences would be different with varying rigor around security, consent and the specific uses of data. The risk is these could vary significantly across the different sectors without an overarching framework to provide consistency and standardisation. |
| 13 | *This discussion document outlines four possible options to establish a consumer data right in New Zealand. Are there any other viable options?* |
| | • Mastercard does not have any further comments. |
| 14 | *Do you have any comments on our initial analysis of the four options against our assessment criteria?* |
| | • Mastercard does not have any further comments. |
| 15 | *Do you agree or disagree with our assessment that Option two is most likely to achieve the best outcome using the assessment criteria?* |
| | We agree with the assessment that Option 2 is most appropriate; however, we note that: |

- **It requires secondary legislation**: in theory, the industry should develop the appropriate APIs; in the event they do not do this within a reasonable time, then secondary legislation would be necessary.
- **Timing expectations must be reasonable:** the roll-out of open banking to other multiple industries will take a long time (e.g. Energy and Telco in the Australian CDR). It seems presumptive to include principles for all industries in New Zealand now, then applying this legislation in 5 to 20 years' time, assuming the principles that we operate under won't change.

**How could a consumer data right be designed?**

16 *Do you agree with the key elements of a data portability regime as outlined in this section? Are there any elements that should be changed, added or removed?*

- We agree in principle with the key elements as outlined.

17 *Do you have any feedback on our discussion of any of these key elements?*

- Mastercard agrees that an Accreditation Regime is vital to ensure consumer trust and assuring data protection – consumers knowing that when they share their data, it will be used properly, for their benefit, safely and securely. An accreditation regime must ensure appropriately high levels of security standards are maintained and that privacy controls, including access to and use of data, are in place.
- It is important to note that that the provision of these key elements in legislation should not preclude the private sector from offering goods and services that would benefit these key elements, e.g. Part F.
- As part of building trust in a CDR there must be clear consequences for data recipients who breach requirements on them, up to and including ceasing to be an authorized data recipient. There need to be arrangements and oversight of the deletion of data by a data recipient in breach of requirements on them. A CDR enforcement regime could be administered by the government or through an appropriate agency.

18 *Are there any areas where you think that more detail should be included in primary legislation?*

Mastercard believes that a strategy to combine CDR with digital identity platforms could create the opportunity for significant consumer benefit in frictionless product switching, increased competition and better serve the future CDR industries.

**Seamless product switching:**

- When consumers apply for new financial products (bank accounts, credit cards, personal loans, mortgages) a crucial task for them is to prove their identity and to allow the financial institution (or Reporting Entity) to perform related KYC obligations.

- Using an Australian data point: even in digital or online channels, up to 30%[1] of consumers are unable to present sufficient identity documentation, or be found on credit bureau data sources, so as to allow them to automatically be approved for a new financial product; we propose this would be similar in New Zealand. Typically, these consumers must manually upload documentation, visit bank branches or post-office outlets to complete their verification, often leading to significant consumer frustration.

- The benefits brought by the CDR for a consumer to digitally prove their income and expense data through bank transaction data will be undermined to the extent that consumers have no choice but to use manual and inefficient identity verification processes when they are attempting to switch products.

- From a consumer's perspective, where their original identity verification result (or KYC status) could be shared from their existing Data Holder to the Data Recipient, would result in substantial productivity benefits for industry. It would greatly reduce friction in switching products and likely lead to higher satisfaction with outcomes flowing from the CDR.

- A framework in New Zealand could improve upon the Australian CDR implementation by including additional identity attributes such as Date of Birth (not currently supported in Australia), as well as a distinct KYC assurance/flag of an individual where that data is being shared by banks or other financial institutions for an AML purpose.

**Minimisation:**

- Accredited third parties should minimise the data collected, collecting only the information than is necessary, and this would help to avoid an undesirable "data maximisation" approach.

**Consent:**

- The ability to withdraw consent for the use of CDR data should be also made available through the channel of the data holder. The reason is that individual consumers, when withdrawing consent, will likely withdraw consent for both collection and use at the same time. As such, if consumers approach their bank to withdraw, they are likely to make a combined request which covers both collection and use.
- In order to meet consumer expectations, and to reduce consumer frustration, consumers should be able to withdraw consent for use with any entity that has their data.

| | |
|---|---|
| 19 | *How could a consumer data right be designed to protect the interests of vulnerable consumers?* |

- Regulatory agencies must extensively consult with a broad range of user groups to ensure they are fully represented in the formulation of any consumer data right.

[1] ***https://www.digitalid.com/business***

- The enablement of third parties to act on behalf of consenting consumers disproportionality affects vulnerable consumer groups. This speaks to the need for robust accreditation (and brand signalling of the same).
- We suggest significant consideration of needs and the creation of a defining set of principles to empower vulnerable customers and support a consistent approach.
- Consumer education on how to participate in sharing data is critical to ensure people are fully informed on how to safely and securely share their data, with consent and how their data will get used being critical for all consumers, especially more vulnerable consumers.
- Ensuring appropriate controls are embedded with the API ecosystem to ensure that parties that might abuse more vulnerable customers are discovered and acted upon quickly or their identity is knowable.

| | |
|---|---|
| 20 | *Do you have any suggestions for considering how Te Tiriti o Waitangi should shape the introduction of a consumer data right in New Zealand?* |

- Engagement with local Iwi and Hapu is critical to ensure Te Tiriti o Waitangi is implemented for the benefit of Maori in Aotearoa.

| | |
|---|---|
| 21 | *How could a consumer data right be designed to ensure that the needs of disabled people or those with accessibility issues are met?* |

- A consumer data right would need to carefully consider the needs of all consumer groups to allow access. Regulatory agencies extensively consult with user groups to ensure they are represented in the formulation of a CDR.
- Ensure proposed CDR legislation reflects the principle that the data recipients who utilise the CDR regime are entrusted with ensuring the wide accessibility of the data to end consumers
- Consider the application of global accessibility standards (such as WCAG 2.0) in secondary and tertiary legislation or regulation, where appropriate.

| | |
|---|---|
| 22 | *To what extent should we be considering compatibility with overseas jurisdictions at this stage in the development of a consumer data right in New Zealand?* |

- Mastercard suggests we have interoperable specifications, regardless of the regulatory regime, in order to future-proof opportunities and support global scale.
- Given the levels of global mobility (COVID restrictions notwithstanding), interoperable standard and data sharing would enable non-NZ Nationals to open accounts more easily, a well-known pain point. More broadly, this would support migration in general, a popular use case is mobility between Australia and New Zealand, with many moving across the Tasman that would stand to benefit from such interoperability.

| | |
|---|---|
| 23 | *Do you have any comments on where a consumer data right would best sit in legislation?* |

- Mastercard does not have any comments on this.

| | |
|---|---|
| 24 | *Do you have any comments on the arrangements for establishing any new bodies to oversee parts of a consumer data right?* |

- Any new body that oversees the consumer data right, should be based on input from a broad representation of New Zealand consumers and business sectors, and not simply comprise of payments representatives.
- Inclusion is essential, encompassing diverse backgrounds and demographics, such as:
  - specialist interest groups
  - consumer groups
  - those with technical and strategic experience
  - varied age, cultures and genders
- Inclusion of representatives from both Financial Services, FinTech and broader industries (e.g. telecommunication and energy).
- Inclusion of overseas experts from other jurisdictions (Australian CDR, PSD2 & UK CMA 9).
- We believe that successful implementation of CDR in New Zealand could be done with a relatively 'light touch' oversight, without necessarily overburdening the industry with costly and extensive regulatory structures. We would be more than happy to share our perspective, based on advising multiple regulators globally on the topic over the last few years.

| | |
|---|---|
| 25 | *What are the pros or cons of having multiple regulators, or a single regulator, involved in a consumer data right?* |

Multiple regulators

- Pro's
  - Avoids concentration of power within one regulator, prevents abuse of power and lessens impact of potential poor governance / decision making
- Cons
  - Double handling of issues leading to inefficiencies of time and resource
  - Overlap or duplication of responsibilities or gaps in regulation, especially between strategic and technical responsibilities
  - Has the potential to add confusion and complexity for new entrants into the market, trying to understand how to participate.

| | |
|---|---|
| 26 | *If government decides to establish a consumer data right, do you have any suggestions of how its effectiveness could be measured?* |

Principals of speed, simplicity, increased competition and consumer choice with better outcomes, consider some of the following:

- More frequent product changes/improvements
- Number of companies accredited under regime

- Total number of API calls
- The rate of switching (%)
- Consumer benefits (choice, reduced application (decision) times, better outcomes (lower rates), greater personalisation and the right product at the right time
- Number of consumers who have shared/released their data to third parties
- Number or write-access payments made

## Other comments

- A further comment from Mastercard is the importance of defining an additional ecosystem entity who provides a technology or intermediary service that allows one third party to access multiple data providers. This will enable scale and reduced cost by allowing parties to connect once through such an intermediary service. As seen in Europe the number of connections between data recipients and owners is significant, adding build and control complexity to those entities. A recognised connector brings connection scale and reduces cost. With this connector seeing participants and data they can add additional checks and monitoring functions to ensure those that connect are permitted to do so, as well as data use rules are adhered to as per the agreed rules. There should also be a clear definition for such a role to ensure efficient scale and adoption.

- Mastercard does not see any necessary change to the oversight of data privacy regulation in New Zealand as the result of the establishment of a CDR.

# Appendix 1

**Electronic payments: costs and value**

To truly understand the "costs" inherent in any form of payment, it is important to account for the value derived from different options. In the case of electronic payments, both paying by card and accepting cards provides tremendous benefits to participants and to the economy as a whole. These benefits are supported by interchange.

Businesses pay their banks a Merchant Service Fee (MSF), made up of interchange, a fee to their bank, the processing or switching fee (charged by the payment network or e-commerce gateway, e.g. Paymark or Verifone, charging the acquirer per transaction) and a scheme fee. The amount businesses pay per transaction is determined by their bank. Some businesses also pay terminal rental fees and a direct monthly fee to Paymark or Verifone.

**Safety and security** – Interchange and scheme fees covers the cost of fraud protection, so cardholders are protected in the rare event of a fraudulent transaction. For example, in the event of a stolen card, Mastercard cardholders are protected from fraud or unauthorized transactions under Mastercard's Zero Liability Policy. Investment in EMV chip technology has also enhanced the anti-fraud capability of cards, making them almost impossible to counterfeit and adding an extra layer of protection not possible with magnetic stripe cards.

**Schemes and eftpos compared**

eftpos is often misunderstood as a "free" payment option, because there is no interchange involved in transactions on this network. But, in the absence of interchange, while still incurring costs, banks had not been able to invest in innovation or advanced security and identity verification technologies to the same level as the international networks. The focus of the international schemes has been making their networks more secure and innovative. As a result, scheme products have significant extra functionality and safety features – such as zero liability on fraud and global acceptance in store and online - compared to domestic eftpos cards.

A great example of this is EMV chip technology, an innovation that protects card data and is almost impossible to counterfeit, as compared with magnetic stripe technology. This is now a core safety feature on cards around the world and has substantially reduced the incidence of card skimming. It is also the functionality which allows consumers to use a digital version of a Mastercard on their phone to make contactless transactions. We are now bringing this same concept to online transactions through tokenization, which will significantly enhance the security of these transactions.

<<END>>