Submission on discussion document: *Unlocking value from our customer data*

Your name and organisation

Name	Privacy of natural persons
Organisation (if applicable)	Visa
Contact details	Privacy of natural persons

[Double click on check boxes, then select 'checked' if you wish to select any of the following.]

☒ The Privacy Act 2020 applies to submissions. Please check the box if you do not wish your name or other personal information to be included in any information about submissions that MBIE may publish.

☐ MBIE intends to upload submissions received to MBIE's website at ***www.mbie.govt.nz***. If you do not want your submission to be placed on our website, please check the box and type an explanation below.

I do not want my submission placed on MBIE's website because… [Insert text]

Please check if your submission contains confidential information:

☐ I would like my submission (or identified parts of my submission) to be kept confidential, and **have stated below** my reasons and grounds under the Official Information Act that I believe apply, for consideration by MBIE.

I would like my submission (or identified parts of my submission) to be kept confidential because… [Insert text]

24 July 2023

Consumer Policy Team
Building, Resources and Markets
Ministry of Business, Innovation & Employment
PO Box 1473
Wellington 6140
New Zealand

Submitted by electronic mail: ***consumerdataright@mbie.govt.nz***

Dear Consumer Policy Team representative,

Visa welcomes the opportunity to share our perspectives on the exposure draft of the Customer and Product Data Bill (the draft law) and the accompanying discussion document to set standards and safeguards for customer and product data exchange.

In responding to the consultation paper, Visa's submission focuses on several topics, including customer consent as well as proposed obligations on data holders and accredited requestors. In addition, we provide our perspectives on a number of specific questions in MBIE's paper, such as the draft law's clarity on storage and security requirements and definitions surrounding fraud and risk.

In addition, Visa recognises the impact our business can have in enabling everyone throughout the world to participate in the global economy. Financial empowerment – including through data-sharing – improves livelihoods and ultimately bolsters communities. This, in turn, supports employment, creates jobs, helps businesses thrive and drives economic growth.

As a result, Visa supports MBIE's recognition that the draft law creates opportunities to support by-Māori, for-Māori data initiatives, business-to-business applications and improved accessibility and inclusion.[1]

Visa is available to provide further details on our submission if helpful.

Yours sincerely,

(signed Privacy of natural persons
Country Manager – New Zealand and South Pacific
Visa International Asia Pacific New Zealand Ltd Visa Worldwide (NZ) Limited

Overview

As a company that values our longstanding relationship with the New Zealand Government, Visa is committed to working with the Ministry of Business, Innovation and Employment (MBIE) as it considers the most appropriate data-sharing model for the country's residents and businesses. More specifically, we appreciate the continued opportunities to collaborate with MBIE and other New Zealand government bodies to fulfil the objectives of the Consumer Data Right (CDR) in New Zealand and, on this occasion, the exposure draft of the Customer and Product Data Bill (the draft law). We appreciate the thoughtful approach MBIE has taken to the consultation process, which is fundamental in building a regulatory framework that can benefit New Zealand consumers, businesses and the broader economy. At this stage of the development of the data sharing framework, stakeholder engagement is crucial to help MBIE navigate the complexities of the ever-evolving products and services in the open data ecosystem in New Zealand and ensure that a data-sharing ecosystem will succeed.

[1] Ministry of Business, Innovation and Employment (2023), ***Unlocking value from our customer data - discussion document (mbie.govt.nz)***, p5.

For more than 60 years, Visa has enabled people, businesses and governments to make and receive payments across the globe. As a global payments technology company, we connect financial institutions, merchants and governments around the world with consumers. In line with the words of the Minister for Commerce and Consumer Affairs, Duncan Webb, Visa believes that "critical to any data sharing is trust."[2] Trust underpins everything Visa does, and building trust begins with a commitment to privacy and security.

Along with trust, consumer education and consumer consent are critical pillars for ensuring the success of data-sharing frameworks. Visa believes individuals and businesses should have confidence that their data is safe, and a successful consumer data-sharing framework should place consumer control at the centre of data management, supported by robust data use principles and practices.

Visa also believes that a consumer data-sharing framework should be flexible, market-driven and agile enough to encourage innovation and allow different technologies and business models to emerge across all levels of the value chain. Importantly, any consumer data-sharing framework should provide consumers with appropriate levels of protection, while continuing to foster innovation and efficiency.

As consumer data sharing flourishes in New Zealand, different roles will emerge – from service providers to developers – and Visa encourages MBIE to avoid prescriptive rules that will run the risk of stifling these dynamics. Specifically, participants in the ecosystem should be free to manage the terms of their commercial relationships, allowing for new business models to emerge which will, in turn, lead to new products and services for the benefit of consumers.

This will be important not just in the early stages of consumer data sharing in New Zealand, but also later when gaps in products, services or providers may become evident, and industry will need to create marketplace solutions. Prescriptive mandates that result in limiting commercial relationships or the design and delivery of products and services could not only hinder innovation at large but may unnecessarily delay the uptake of data sharing.

Visa shares these perspectives with MBIE and after having closely consulted and collaborated with governments across the globe on their respective data-sharing policies. We believe the approach outlined above can contribute to New Zealand's long-term economic growth and international competitiveness, as well as delivering broad benefits to consumers and businesses.

We have responded to specific questions in the discussion document in the section that follows.

[2] Ministry of Business, Innovation and Employment (2023), ***Unlocking value from our customer data - discussion document (mbie.govt.nz)***, p4.

Responses to discussion document questions

How will the draft law interact with protections under the Privacy Act?	
1.	**Does the proposed approach for the interaction between the draft law and the Privacy Act achieve our objective of relying on Privacy Act protections where possible? Have we disapplied the right parts of the Privacy Act?**
	Visa supports MBIE's proposed approach of relying extensively on the existing protections under the Privacy Act. As the draft law is intended to improve customer access to, and control of, their data, it is eminently sensible to utilise the existing access rights and protections available under the Privacy Act, following New Zealand's overhaul of its privacy legislation in 2020. It is encouraging to see the clear recognition of the overlap between personal information and customer data and the interdependency between privacy legislation and any new legislation on access to, and exchange of, customer data. In other jurisdictions which have been contemplating the introduction of similar open data legislation, there has sometimes been an unfortunate tendency to develop these new laws on a completely standalone basis, in isolation from existing privacy laws, with the potential for conflicting legal obligations or industry standards. Given the broad applicability of the Privacy Act, the reliance on existing protections under the Act and the avoidance of unnecessary replication should reduce complexity and ensure consistency for all participants in the open data ecosystem. In particular, it is helpful to adopt a standardised approach to data requests while also facilitating ease of access to customer data and recognising the continued ability to access personal information under the Privacy Act. While the provisions of the Privacy Act which have been disapplied under Section 46 appear correct, it is possible that certain other sections of the Privacy Act (such as Sections 49-54) could in some cases, if not disapplied, potentially have a limiting impact upon data requests. In addition, when treating all requests for personal information such as IPP6 requests, complaints or contraventions, it is important to consider the substantial differences between an individual's request for access to their own data and a company's request for customer data.
Consent settings: respecting and protecting customers' authority over their data	
2.	**Should there be a maximum duration for customer consent? What conditions should apply?**
	Visa believes in empowering consumers with tools to easily access, manage and use their financial information. For consent-based regimes like the draft law proposed in the discussion document, it is imperative that consumers understand what they are consenting to when they share their data. When presented with an opportunity to enable financial services or access information which requires consumers to share their personal data, consumers should be provided with clear information. This should include what data they are sharing, who may use the data they share, for what purposes and over what periods the data will be used, and clear, simple and consistent information about their choices and how to manage their data-sharing permissions.

	Visa supports MBIE's objective of preventing consent fatigue and customer frustration.[3] We completed a recent survey involving 2,000 New Zealand customers as part the Visa Consumer Empowerment Study[4], and observed that "duration" is one of the key factors regarding customer consent acceptance. Visa believes that providing the option for customers to choose the duration of data access can increase trust and data-sharing confidence in the organisations offering these consent experiences. In addition, to avoid service abandonment, we propose that it is also desirable for the accredited requestor and/or data holders to provide the customer with the ability to extend the initial consent before expiry, with a customer authorisation. Furthermore, other time-based attributes should be taken into consideration, including: • Timespan – how much data will be accessed (e.g., three months of transactions for a lending scenario where a customer is applying for a loan) and • Frequency – how often the data will be accessed (e.g., once a day or every time the app is accessed for a personal finance budgeting tool). Providing time-based attributes specificity for consumers as it relates to the duration, timespan and frequency of data access can help to promote greater customer transparency and clarity in consent experiences. The following should also be considered regarding action initiation consent: • The duration of the ongoing "action initiation" consent. Visa suggests an approach that would allow data holders (with the agreement of the customer) to set a timeframe for consent renewal for specific use-cases (e.g., recurring payments). • The duration of "short lived/one-off" consent requests for action initiation (e.g., one-off payment initiation consent can last for up to 24 hours). Finally, at a broad level, we support the position provided for in the draft law that consumers must "be able to view and withdraw consent at any time".[5] We believe empowering consumers to make informed consent decisions also includes providing them with the right to withdraw their consent at any time and to be presented with an efficient means to do so.
4.	**Do you agree with the proposed conditions for authorisation ending? If not, what would you change and why?**
	Visa supports MBIE's intention to set the conditions for the ending of the authorised consent. This approach should provide customers with comfort that their authorisation ceases when their account is closed or when the accredited data requestor is suspended. In addition to these examples, we encourage MBIE to consider ending consent authorisation when a customer deletes the application and/or removes the service provided under the draft law. Nevertheless, we believe that transparency and customer awareness are paramount and that sending a notification to customers when these circumstances occur is necessary.
6.	**What are your views on the proposed obligations on data holders and accredited requestors in relation to consent, control, and accountability? Should any of them be changed? Is there anything missing?**

[3] Ministry of Business, Innovation and Employment (2023), ***Unlocking value from our customer data - discussion document (mbie.govt.nz)***, p25. Chapter 1, Point 64

[4] Visa Consumer Empowerment Study (2020 – 2022). Research was commissioned by Visa Inc. and conducted on representative samples of identified market adult online populations across age, gender, and region.

[5] Ministry of Business, Innovation and Employment (2023), ***Unlocking value from our customer data - discussion document (mbie.govt.nz)***, p25. Chapter 1, Point 66.

	As mentioned above, Visa recently surveyed 2,000 New Zealanders and found that 73 per cent want to take more direct control of their data or have the option to have more control of their data. This is in line with our global research regarding third-party data access requests. Visa encourages education and easily accessible and intuitive tools to enable customers' control of their data. In addition, we support transparency and clarity serving as guiding principles to drive adoption. We believe that ecosystem adoption of a consistent consent experience (e.g., that the "look and feel" of the experiences are similar) can also yield greater customer consent acceptance. To help address the consistency of users' consent experiences, Visa encourages the industry to adopt a common framework for consent experiences (e.g., adoption of "core" consent attributes, such as primary purpose, secondary purpose, duration, timespan and frequency). In this regard, it is important to note that Visa's recent Consumer Empowerment Study suggests that setting an industry standard for consent provisioning designed to educate New Zealand consumers should increase their trust and enhance data-sharing comfort.
Care during exchange: standards	
7.	**Do you think the procedural requirements for making standards are appropriate? What else should be considered?**
	Interoperable standards are the backbone of data exchange, fostering trust amongst participants, creating a level playing field, enabling a frictionless consumer experience and supporting scalability in the future. In that vein, Visa commends MBIE for crafting a standard-setting process that not only intends to build on industry-led work already underway but considers impacts to international trade and investment. As MBIE considers the development and implementation of technical standards, Visa recommends that it includes representatives from sectors that may wish to participate in the data-sharing economy. As an example, financial institutions, as well as members of the broader financial ecosystem including payment networks, will be important contributors to innovation and emerging technologies. Besides promoting trust, consistent and interoperable data-sharing protocols and consent standards reduce costs, accelerate the uptake of data sharing in the ecosystem and help incentivise the creation of new and innovative products and services.
8.	**Do you think the draft law is clear enough about how its storage and security requirements interact with the Privacy Act?**

	Visa recognises that storage and security requirements under the draft law will be the subject to further regulations and standards in due course. In addition, we support the intention to build on existing standards and industry protocols already being developed within the banking and payments sector. However, the draft law does not appear to address the interaction between storage and security requirements under the Privacy Act in much detail – for example, the draft law includes a definition of IPP 5 but does not refer to this principle anywhere else. While Section 48 provides that a contravention of CPD storage and security requirements relating to personal information should be addressed under the Privacy Act, the draft law does not appear to indicate to what extent the CPD storage and security requirements should be based on or aligned with the equivalent requirements under the Privacy Act. As recognised in the consultation document, in cases where there will be a potential overlap in regulatory jurisdiction (such as a failure to implement appropriate security standards), it will be important to clarify respective regulatory roles and processes and the ability for regulators to share information instead of duplicating investigations.
10.	**What risks or issues should the government be aware of, when starting with banking for standard setting? For example, could the high security standards of banking API's create barriers to entry?**
	In a successful information sharing ecosystem, Application Programming Interfaces (APIs) allow covered data providers to define the scope of data sharing and permit consumers to manage access to their information. Visa believes that a well-functioning data exchange ecosystem ideally involves an API-first approach to consumer-authorised data access, in alignment with MBIE's objectives to seek the "direct, secure and standardised"[6] transfer of customer and product data and privacy protections. Visa believes API standards should be interoperable, have high security standards, meet certain performance and availability requirements and allow APIs to be commercially viable. In addition, Visa believes in a technology-neutral approach, so that industry is not locked into specifications and standards that will be outdated in the future. To that end, broad representation and active participation from industry participants in the designated sectors' ecosystems is more likely to ensure the development of APIs that work universally for all participants and across multiple use cases - with an appropriate focus on the consumer experience.
Trust: accreditation of requestors	
11.	**Should there be a class of accreditation for intermediaries? If so, what conditions should apply?**
	As noted above, any consumer data-sharing model needs to be flexible enough to allow competition to thrive at all levels of the value chain. This supports an environment where ecosystem participants can provide additional value and economic efficiency, while also incentivising future innovation. For consumers, this environment creates a sense of security in data sharing and facilitates data sharing to create value for consumers without the need to establish multiple connections. Visa recognises that there will be a variety of providers in the New Zealand data sharing ecosystem, which may vary in the types of services they support. These providers will not

[6] Ministry of Business, Innovation and Employment (2023), ***Unlocking value from our customer data - discussion document (mbie.govt.nz)***, p9. Introduction, Point 13.

	necessarily seek to provide services akin to those of accredited requestors or data holders and, therefore, should not be expected to be accredited as such. Visa agrees with MBIE that "while there are overlaps between the concept of outsourced providers and the Australian concept of intermediaries, they refer to different things.[7]" Notably, an outsourced provider does not necessarily need to be defined as a data holder or an accredited requestor. Given the evolving nature of data movement, Visa supports MBIE's inclusion of outsourced providers and the flexible nature by which they are defined. These entities can provide valuable services such as cybersecurity, encryption technology and fraud and risk monitoring to drive participant and consumer trust in New Zealand's data-sharing ecosystem. A secure environment for enabling data availability, in turn, makes it easier for developers and accredited entities to create services that consumers can trust across multiple accounts. In addition to the examples provided above and in points 95 and 96 of the discussion document, Visa suggests that accredited requestors may utilise outsourcing models (e.g., storage or technology outsourcing arrangements) to enhance the efficiency of their offerings, provided such arrangements are subject to appropriate security requirements and controls.
Unlocking value for all	
16.	**What are specific use cases which should be designed for, or encouraged for, business (including small businesses)?**
	Visa believes that a successful regulatory framework is principles-based and sufficiently flexible to encourage innovation and allow different technologies and business models to emerge across all levels of the value chain. A flexible regulatory framework can boost the broad adoption of the proposed law and more easily adapt to future innovation. Visa encourages greater participation of businesses (from micro to larger) in the digital economy and through the regime. A more robust and vibrant ecosystem of financial technologies and participants – powered by the broader use of permissioned data – can help individuals and businesses unlock economic opportunities by enabling streamlined access to new or more appropriate financial products and services, in addition to traditional banking services. The draft law can promote simplified product comparisons and selection, better business cash-flow management services and business optimisation. Visa also believes that the design should allow for the possibility of the disclosure of designated data by an accredited person to non-accredited third parties. Extending the proposed law in this manner is likely to increase uptake of the Customer Product and Data regime, by lowering the barrier of entry to innovative for fintechs and other small- to medium-sized businesses, such as accountants.
Preliminary provisions	
21.	**What is your feedback on the purpose statement?**

[7] Ministry of Business, Innovation and Employment (2023), ***Unlocking value from our customer data - discussion document (mbie.govt.nz)***, p30. Chapter 1, Point 95.

	Visa commends MBIE on purpose statement in the exposure draft of the Customer and Product Data Bill (the draft law). While data sharing between data holders and third parties may facilitate the development of new and innovative products, consumer control over how and when data can be shared is critical. Given the centrality of informed customer consent in the draft law, Visa believes that the customer should be fully informed about the associated risks, including data security risks, while at the same time avoiding the introduction of additional friction into the data sharing process.
22.	**Do you agree with the territorial application? If not, what would you change and why?**
	Visa supports MBIE's proposed approach of basing the scope of territorial application of the draft law on the position under the Privacy Act. As mentioned above, having a close alignment between the draft law and existing privacy legislation should reduce complexity and ensure consistency for all participants in the open data ecosystem. As noted in MBIE's consultation, the application of the draft law's requirements will be limited to organisations which apply for accreditation or are brought into the scheme via designation regulations, meaning the territorial scope will in practice not be as extensive as is the case under the Privacy Act.
Regulated data services	
23.	**Do you think it is appropriate that the draft law does not allow a data holder to decline a valid request?**
	In Visa's view, it is appropriate that the draft law does not allow a data holder to decline a valid request. However, we acknowledge the discussion document does broadly reference situations where a decline is permitted, including: (1) Requests which are under duress (physical or mental) or could cause harm and (2) Requests where there is a risk of fraud. [8] Visa recommends refining the parameters in the draft law to ensure declines are permitted in the appropriate circumstances and can be systematically or logically applied and requests restricted or denied where possible. For context, we offer the following example – an account holder's account has been fraudulently taken over and the fraudulent user aims to update the phone number or address linked to the account to further bypass two-factor authentication procedures or receive new products provisioned to the new address (like a credit card delivered to new address). In this example, the fraudulent user attempts to transition the account holder's information to a matched and known fraudster's phone number or postal address and is detected in advance of the change request being applied. In order to determine and enable methods to appropriately decline requests (data or action), it would be useful to recognise and support scenarios where a suitable and reasonable denial of data request or action is allowed. We recommend that the following scenarios should also permit a decline: • Address/contact details update (Request side/Action originator risk) – A fraudulent user aims to update information and a suspected address or contact information

[8] Ministry of Business, Innovation and Employment (2023), ***Unlocking value from our customer data - discussion document (mbie.govt.nz)***, p46. Chapter 2, Point 167.

contains indicators that identify that the nominated updated information is high risk. Denials in this case should be permitted.

- Requesting a payment (Request side/Action originator risk) – A fraudulent user aims to make payments and suspect indicators present in the users requested action, such as high-risk IP address networks (e.g., overseas (non-NZ) or frequent fraudulent networks) being used to originate such requests could be high risk. Denials in this case should be permitted.
- Requesting a payment (Receive side/Recipient risk) – An account holder aims to make a payment to an entity and suspect indicators highlight that the beneficiary account is being used for a money mule account or behaviour or has been raised as causing duress, harm or fraud. This would logically be extended to receive side risk monitoring, such as money mule accounts, in the spirit of supporting anti-money laundering. Denials in this case should be permitted.
- Requesting a payment (Receive side/Recipient risk) – Similar to the example above, an account holder aims to make a payment to an entity and suspect indicators highlight the entity should not be permitted to accept payments due to known misrepresentation of their products or services. Denials in this case should be permitted.

Furthermore, if MBIE is considering applying a provision that allows a proactive user level opt-out, the user level pre-configured opt-out should supersede and permit a decline on an incoming valid request (that contravenes specific rules of the opt-out request). For example, if a user makes the decision to not permit/block/deny data or action requests from an unwanted business line (e.g., gambling), this decision should be honoured. This decline response would continue to be on a valid request.

About Visa

Visa is a world leader in digital payments, facilitating transactions between consumers, merchants, financial institutions and government entities across more than 200 countries and territories. Our mission is to connect the world through the most innovative, convenient, reliable and secure payments network, enabling individuals, businesses and economies to thrive. We believe that economies that include everyone everywhere, uplift everyone everywhere and see access as foundational to the future of money movement.

Building the future of commerce

In New Zealand, Visa has a physical presence in Auckland. Together with our New Zealand financial institution, fintech and merchant partners, as well as our technology partners, we are committed to building a future of commerce that fosters the country's economic growth and innovation. One way we are realising this is through Visa Partner Portal and Fintech Fast Track. The programs provide New Zealand fintechs with access to Visa's technologies, networks and solutions, enabling businesses to scale their solutions for the benefit of consumers, businesses and the economy. An active member of New Zealand's technology community, Visa also supports the prestigious Hi-Tech Awards in the category of Best Hi-Tech Solution for the Public Good.

Visa also operated a fully owned subsidiary, Visa Spend Clarity Enterprise, a leading software-as-a-service technology company providing payments and transaction management solutions for financial institutions and their corporate customers. Visa Spend Clarity Enterprise is headquartered in Auckland and supports more than 170,000 organisations in 178 countries.

Additionally, Visa is a member of Digital Boost, Digital Identity NZ and Fintech NZ and contributes to these groupings, especially through our global experience and perspectives. We also have a close relationship with Payments New Zealand, Retail New Zealand and the New Zealand Bankers Association, and we regularly consult with them on matters relating to the New Zealand payments ecosystem.

Enabling convenience, security, and trust

As a network business built on partnerships, Visa continues to enable new payment flows and expand acceptance, ensuring that every New Zealander can pay, and be paid, in a convenient and secure way. We work with the broader payments ecosystem to ensure security is at the forefront of such technology, including tokenisation, AI-powered fraud prevention, biometrics and digital identity solutions. In 2019, Visa launched the Future of Security Roadmap, outlining how New Zealand can collectively work towards a more secure payments ecosystem through industry initiatives and standards.

Supporting New Zealand businesses

Enabling New Zealand businesses to thrive is at the heart of Visa's mission. As the trend towards digital continues, Visa is committed to enabling New Zealand businesses to adapt and grow through payments innovation. In 2020, we launched Where You Shop Matters, an initiative to connect consumers with local businesses in their communities, with Visa's e-commerce tools helping to support small businesses selling to an increasingly online consumer base. During reduced COVID-19 alert levels, Visa's Back to Business Locator Tool helped to promote New Zealand businesses open and trading through an online directory powered by VisaNet.

To learn more, visit www.visa.co.nz.