Submission on Consumer Data Right Exposure Draft

Visa’s Perspectives and Recommendations

September 2018

September 7, 2018

The Treasury

Langton Crescent

Parkes ACT 2600

**RE: Submission on Consumer Data Right Exposure Draft**

Dear Madam/Sir,

Visa Inc. (“Visa”) welcomes the opportunity to comment on Treasury’s Exposure Draft of Consumer Data Right (CDR). As noted in Visa’s submission to the Review into Open Banking in Australia,[[1]](#footnote-1) Visa applauds Treasury’s focus on consumers through the CDR. Consumer control over how and when their data can be shared is important for enabling development of a transparent, equitable and innovative payments ecosystem. Below we provide an overview of Visa, offer our views on data use in the payments industry and provide perspective on Treasury’s CDR Exposure Draft.

About Visa

Visa is a global payments technology company that enables fast, secure and reliable electronic payments for clients around the world. Visa is not a bank and does not issue cards, extend credit or set rates and fees for account holders on Visa products. Rather, our advanced transaction-processing network facilitates authorisation, clearing and settlement of payment transactions. Today, Visa connects more than 3.2 billion Visa accounts and 46 million merchant locations in 200 countries and territories. Each transaction is enabled by a global network of over 16 thousand financial institution partners. In 2017, Visa’s global network managed $7.6 trillion in payments volume and over 169 billion total transactions.

Visa supports fair and open regulatory environments. We believe that the ongoing development of a safe, efficient, competitive and stable electronic payments system is essential to the growth and stability of the Australian economy. Electronic payments platforms, including Visa, contribute significantly to economic growth, development and the financial inclusion of all Australians.

Visa’s perspective on data use

The payments industry is evolving at a rapid pace. In 2016, electronic payments surpassed worldwide cash usage for the first time,[[2]](#footnote-2) in large part driven by new technology, rapid consumer adoption of mobile wallets and e-commerce growth. Payments providers are no longer constrained by wired infrastructure, enabling firms to reach the unbanked, the underserved, and entirely new merchant segments and ushering in a new era of anytime, anywhere commerce.[[3]](#footnote-3)

At the same time, data usage around the world is exploding. By some estimates, 90 percent of the world’s data was created in the last two years alone; by 2020, it is estimated that for every person in the world, 1.7MB of data will be created every second.[[4]](#footnote-4) Continued advances in artificial intelligence (AI) and cloud technologies, together with growth in connectivity through the proliferation of Internet of Things devices, could have profound impacts on global commerce, creating new use cases for payments and Visa technology. In such an environment, common understanding about the treatment of personal data is essential.

With new technologies comes new risks, and new policies necessitating the sharing of sensitive financial data should be cautiously implemented. As fraud and cyberattacks grow in sophistication and become more widespread, robust data protection measures are absolutely critical to protecting consumers. Furthermore, clear accountability rules between financial institutions and emerging players are also important in providing a level of certainty in the event of a security breach, fraud or other unlawful activity. After all, if new policies unnecessarily put consumers at risk, it would undermine the Government’s initiative and threaten the safety and security of the financial system.

For Visa, consumer trust in the payments system is paramount. To this end, Visa is relentless in fortifying the security of our network. Indeed, Visa was founded on the principle of secure innovation, and we strongly believe that businesses that facilitate digital transformation have a shared responsibility to work together. For us, this means an ambitious level of investment in innovative technologies, creating and sustaining world-leading security and ensuring a responsible approach to data.

Visa’s observations on Treasury’s Exposure Draft

Overall, Visa supports Treasury’s CDR Exposure Draft and its initiative to give consumers the right to safely manage their own data. In particular, we agree with Treasury’s four key principles for consumer data, namely that such data is 1) consumer focused, 2) encourages competition, 3) creates new business opportunities, and 4) is efficient and fair, with security and privacy in mind.[[5]](#footnote-5) Visa strongly supports Treasury’s perspective that the right will not require the private sector to hold consumer data “that they would not otherwise hold, other than the keeping of records in relation to a consumers’ use of the right.”[[6]](#footnote-6)

Given the importance of informed consumer consent to the CDR, Visa believes that the requirements should seek to fully inform consumers about associated risks, including data security risks. Understanding the sensitivity of financial data, consumers must know and understand the implications of opening account access to third parties, and third parties must take the necessary steps to protect the information being shared. Overall, while we understand that many of the implementation details will be further outlined in the rule-making processes, we have some concerns about some of the broad definitions within the CDR that are worth addressing briefly. For instance, “CDR data” is quite broadly defined in the Exposure Draft, and it is our recommendation that this definition be refined in future drafts to ensure proper application of the law.

We look forward to working with Treasury as the CDR is finalised, including forthcoming rules providing additional guidance on data standards and privacy safeguards. Below are a few insights and recommendations in response to the CDR Exposure Draft.

**On Privacy Safeguards (*Division 5*)**

Visa supports Treasury’s commitment to protect consumer privacy through the CDR and shares its high expectations for data quality and security. Visa recognises that consumer trust is paramount to our business, which is why we continue to invest in technologies that devalue sensitive data, utilise data intelligence, protect data systems from cyber threats, and empower consumers to monitor their transactions. Future rules relating to data privacy safeguards should take the consumer perspective into account, and include a clear model of consumer permissions, controls and safeguards to avoid damaging the trust that consumers place in the payment ecosystem as a whole.

When handling consumer data, Visa’s data policies and procedures ensure that consumers and their data are protected and treated with respect. Therefore, Visa supports Treasury’s efforts to ensure that all participants are following privacy safeguards through proposed assessments to be determined by a future *Information Commissioner*.

**On Data Standards (*Division 6*)**

Visa also supports Treasury’s efforts to encourage standardisation of financial data disclosures with the CDR. We believe that international data standards are essential to maintaining interoperability, efficiency and security among the financial technology community. We would, therefore, encourage that the final CDR and prospective *Data Standards Chair* adopt international data standards, but also caution against being overly prescriptive in assigning a single standard for disclosing data between CDR participants.

Importance of International Standards

We believe that international standards form the backbone of the digital payments industry, enabling ubiquity by maximising global interoperability and acceptance across digital payment systems. This creates a common approach, yet provides enough flexibility in implementation that preserves vigorous competition and the ability for differentiation across the various digital payment systems.

Many financial technology companies already use international standards developed by the private sector, so it is important that any future guidelines on standardisation do not unintentionally impede these efforts. International standards bodies—such as the International Organization for Standardization (ISO), the Payment Card Industry Security Standards Council (PCI SSC) and EMVCo—are creating standards that meet the ever-changing world of digital commerce. For instance, PCI has standards for how sensitive personal information can be shared in an online environment safely and securely, and ISO has standards for how PINs data can be stored without compromising security.

Moving away from international standards raises the potential for increased complexity for all parties, and would increase costs for Australian financial technology companies required to comply with both domestic and international standards. Higher costs to managing data will also likely discourage new financial technology companies from entering the market, which could reduce competition and slow the pace of innovation. Furthermore, domestic standards requirements could increase barriers for Australian financial technology companies looking to expand internationally, given the additional investment they need to make to support globally interoperable platforms to be able to move their business into other country markets.

Mandating domestic standards would also make it very difficult for international companies to do business with Australian firms. The costs of meeting these standards may deter businesses from investing in new products and services for Australian consumers.

Standards Governance

Finally, as the future *Data Standards Chair* reviews standards and establishes committees, advisory panels and consultative groups, it is imperative that industry experts be included in standards setting. Given the fast pace of financial innovation, it is important that standards allow for the rapid adoption of new technologies. Having the perspective of industry experts during the standards-setting process reduces the risk of unintended consequences, which may impede innovation, competition and security.

Conclusion

As financial technology evolves, we fully understand the importance of empowering consumers to share their data while maintaining data security and privacy. We believe that setting smart privacy guidelines and data standards that protect consumer data, but that also promote innovation and competition, is an important first step in empowering consumers. Visa welcomes the opportunity to provide our perspectives on the CDR Exposure Draft and looks forward to working with Treasury in the future.

Yours faithfully,



Group Country Manager

Australia, New Zealand & South Pacific

Visa AP (Australia) Pty Ltd

1. In March 2018, Visa submitted comments in response to Treasury’s *Review into Open Banking – Final Report*. We are including Visa’s Open Banking comments as an addendum. [↑](#footnote-ref-1)
2. Euromonitor Communications, *Consumer Card Transactions Overtake Cash Payments for the First Time in 2016*, found [here](https://blog.euromonitor.com/2016/09/consumer-card-transactions-overtake-cash-payments-first-time-2016.html). [↑](#footnote-ref-2)
3. In the U.S., the “gig economy,” represents more than a quarter of the workforce, according to McKinsey. [↑](#footnote-ref-3)
4. Domo, Data Never Sleeps 5.0 and 6.0, found [here](https://www.domo.com/learn/data-never-sleeps-5) and [here](https://www.domo.com/learn/data-never-sleeps-6#/), respectively. [↑](#footnote-ref-4)
5. Australian Government, Treasury, *Consumer Data Right*, May 9, 2018 [↑](#footnote-ref-5)
6. Ibid. [↑](#footnote-ref-6)