



Visa Inc.'s Submission to the  
*Review into Open Banking in Australia – Final Report*

March 2018





March 22, 2018

***By Electronic Delivery***

The Treasury  
Langton Crescent  
Parkes Act 2600

RE: Review into Open Banking in Australia – Final Report

Dear Sir/Madam:

Visa Inc. ("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. In 2017, Visa's global network managed \$7.3 trillion in payments volume and over 111 billion transactions.

Visa is committed to enabling our consumers and businesses to pay and be paid with confidence. Accordingly, we have focused our investments, partnerships, and expertise to enhance the security of our network. In 2016, we launched our Threat Intelligence Fusion Platform, a cyber-command and control center that provides integrated cybersecurity operations to further protect our data and assets. We are continually working to bolster the resilience of our infrastructure and application services to provide high availability of our client services.

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.

We welcome the opportunity to comment on Treasury's Review into Open Banking in Australia. Below we provide an overview of Visa's open API initiative (the Visa Developer Platform, or "VDP"); offer our perspective on Open Banking, generally; and finally provide our views with respect to Treasury's final report.

## **Enabling innovation and fintech development**

Technology is rapidly transforming the financial services landscape, changing the way consumers interact with their financial institutions by facilitating the payments process and offering new options for consumers, ultimately helping them make more informed and better financial decisions. In order to stay competitive in this rapidly evolving environment, many financial institutions are forging close partnerships with fintechs, and many are opening APIs to third parties, providing opportunities for new and creative service offerings.

Similarly, Visa is committed to staying at the forefront of innovation by putting greater emphasis on openness, collaboration and engagement with the wider economy. We believe that innovation can, and will, come from anyone, anywhere. There is a need for market players to collaborate in new ways and build partnerships with new types of service providers who are adding value to the payments system. Opening APIs to third parties can facilitate these collaborations.

### ***Visa's open API initiative***

In 2016, we launched the Visa Developer Platform (VDP), transforming our proprietary technology network, VisaNet, into the world's largest open commerce platform. VDP provides simplified access to many of Visa's most in-demand products and services through an open network of Visa APIs, allowing anyone to transform great ideas into new digital commerce experiences. VDP offers 90+ APIs, enabling access to some of the most popular Visa capabilities, providing developers with a safe testing environment for the development of new digital payments and commerce solutions. In Visa's experience, open platforms built on secure standards have a proven track record for scaling fast, adapting quickly, fostering innovation and delivering value.

While Visa's open API platform has been effective in enabling third-party developers to access Visa's technologies, opening account access to third parties is not without risk, especially with respect to security and privacy considerations. For Visa, safeguarding customer data is a primary responsibility, and we have designed our open platform with that in mind.

Visa believes that any open API standard should be flexible while prioritising security, providing clarity in relation to access requirements and allowing scalability for future innovations. Accordingly, we agree with Treasury that the UK model is an appropriate

starting point for the API standard. We caution against overly burdensome or unnecessary design and implementation requirements.

### **Visa's perspectives on Open Banking requirements**

Visa strongly supports fair, open and competitive regulatory environments and is committed to helping boost Australia's digital economy. At the same time, we note that the payments system is founded on the promise of securing billions of transactions a year. Consequently, consumer trust in this system is paramount. In recognition of this responsibility, Visa is relentless in fortifying the security of both our own systems and those of the broader payments sector.

Given the importance of security to the stability of the payments system, Visa suggests caution in the development and implementation of Open Banking requirements. We believe that financial institutions should have the flexibility to open their systems based on market demand and only once the right technology solutions and robust security and risk management protocols are in place. Doing so can help reduce business, financial, and security risks for financial institutions and other payment service providers.

Visa recognises that the financial services industry is evolving rapidly, largely driven by the emergence and growth of fintech firms and the development of a wide variety of technological solutions that facilitate the delivery of financial services. In such an environment, Visa believes that Open Banking should be market driven and agrees with Treasury that a regulatory approach should only be applied in the event of market failure.<sup>1</sup> If market forces are insufficient, Open Banking regulation should avoid an overly prescriptive approach and seek to minimise market disruption, while requiring transparency to account holders (including informed consent), addressing potential privacy concerns, ensuring robust security measures that do not compromise consumer ease of use, and establishing clear financial accountability rules should fraud or data breaches occur.

In addition to these general observations, we offer a set of core principles for Open Banking in the accompanying Appendix.

---

<sup>1</sup> The Australian Government the Treasury, "Review into Open Banking: giving customers choice, convenience, and confidence," December 2017, pg. 9.

## **Visa's observations on Treasury's final report**

Visa largely agrees with the recommendations offered in Treasury's Open Banking report and applauds Treasury's focus on consumers through the Consumer Data Right (CDR). While data sharing between banks and third parties may facilitate the development of new and innovative product solutions, consumer control over how and when their data can be shared is critical. Given the importance of informed consumer consent to the Open Banking regime, Visa believes that the requirements should seek to fully inform consumers about the associated risks – including data security risks – while at the same time avoiding the introduction of additional friction into the data sharing process.

With respect to the implementation timeline, Visa believes that financial institutions should be given enough time to ensure that the right security and risk management protocols are in place before opening their APIs to third parties. As highlighted above, robust security measures are critical for ensuring consumer trust in the financial services system. Financial institutions may need to invest in new technologies and update legacy systems before opening their systems. Allowing adequate time, potentially beyond the proposed 12-month period, may be required in order to help reduce security and other business risks for industry players.

### ***The potential for "write access" in Open Banking***

Visa also agrees with Treasury's recommendation not to include payment initiation, or "write access," as part of the Open Banking regime, at this time. As Treasury notes, write access allows third parties the ability to make payments from a customer's account on their behalf. Visa agrees with Treasury that consumer confidence in the security of Open Banking is integral to its success and that implementing write access before the security elements are fully tested could put the success of the regime at risk.

Further, we agree with Treasury that Australia's New Payments Platform (NPP) may ultimately make write access requirements through the Open Banking regime duplicative and unnecessary. Visa agrees with Treasury that the success of "read access," or data sharing, should be fully evaluated before consideration of write access requirements for Open Banking. Here again, we agree that any regulation in this area should only be made to address market failure.

### ***The potential for digital identity requirements in Open Banking***

Finally, Visa agrees with Treasury that a successful digital identity regime in Australia will facilitate the effectiveness of Open Banking. The U.S. National Institute for Standards and Technology (NIST) defines digital identity as the "unique representation of a subject

engaged in an online transaction.”<sup>2</sup> Visa believes that a secure digital identity verification process based on internationally-accepted principles has the potential to reduce friction in financial services. We are committed to working with industry stakeholders and clients to enable the development of a trusted and interoperable digital identity ecosystem, globally. Accordingly, Visa supports Treasury’s work to develop a digital identity framework as part of an Open Banking regime.

Again, Visa appreciates the opportunity to provide our perspectives on Treasury’s Open Banking report.

Sincerely,

A handwritten signature in black ink, appearing to read 'J Potter', written in a cursive style.

Julian Potter  
Group Country Manager  
Visa Australia, NZ & South Pacific

---

<sup>2</sup> NIST Special Publication 800-63-3, Digital Identity Guidelines, found [here](#).

## **Appendix:**

### **Visa's position on Open Banking regulations**

In general, Visa believes that governments should consider Open Banking requirements only when market forces are insufficient. In the event that governments are actively considering a regulatory approach to Open Banking, policymakers should refrain from an overly prescriptive regime. Visa has developed the following core principles to help guide policymakers in the development of Open Banking regulations.

#### **Ensure security and financial accountability**

- Visa supports robust data protection measures necessary to protect personal consumer information against fraud and other risks.
- Open Banking policies should ensure secure access, storage and use of financial data, without compromising convenience and ease of use for consumers; any accompanying authentication requirements should be based on risk analysis in order to appropriately balance payment security, while still facilitating user access.
- Safeguards of the information in the existing banking and payments ecosystem should be paramount.
- Clear accountability rules should be established between financial institutions and emerging players in order to provide a level of certainty in the event of a security breach, fraud or other unlawful activity.

#### **Support innovation and competition**

- Visa supports a fair, open and competitive regulatory environment that facilitates innovation in financial products and services.
- Policy development should consider the impact to the whole market and allow adequate time for public comment in order to fully understand system risk and help minimise market disruption.
- Industry players – both new entrants and incumbents – are best positioned to provide guidance on the nuances of the regulations being considered. Establishment of industry working groups, with diverse representation, can provide timely solutions and advice during the policy development and implementation process.

#### **Protect data and consumer privacy**

- Regulations must include provisions for consumer privacy protections and informed consumer consent.
- Given 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.