Senior Adviser
Financial System and Services Division
The Treasury
Langton Crescent
PARKES ACT 2600
Email: fsi@treasury.gov.au

31 March 2015

Dear Sir/Madam

Visa Submission to the Government's Review of the Financial System Inquiry's (FSI) final report

Visa Inc. welcomes the opportunity to respond to the Government's review of the Financial System Inquiry's (FSI) final report released on 7 December 2014.

Visa has actively participated in the FSI through two submissions presented to the FSI Panel in March 2014 and August 2014, along with previous reviews conducted by other agencies such as the Reserve Bank of Australia (RBA) over the preceding decade. In each of our submissions to these reviews, Visa has stressed the need for balanced, equally applied regulation that fosters innovation and security in electronic payments. We stand by these positions.

We acknowledge the recent work of the FSI, following the Government's explicit inclusion of payments regulation in the FSI Terms of Reference.

Since the release of the FSI Report in late 2014, the Payments System Board (PSB) of the RBA has released its *Review of Card Payments Regulation* (RBA Review). We understand the RBA Review will now deal with all key payments regulatory issues under the current powers afforded to the RBA by the *Payment System (Regulation) Act 1998* (PSRA). Visa will work constructively within the RBA Review.

Beyond the RBA Review, this submission specifically addresses ongoing concerns over the PSRA itself, the need for a strong position from Treasury on regulatory level playing fields and two other issues in the FSI Final Report of relevance to Visa, namely the issues of cyber-security and digital identity.

We believe our policy proposals align with a regulatory framework that will:

- encourage the growth of electronic payments and the digital economy for the benefit of both consumers and retailers;

- promote fair and vigorous competition among the many payment providers, including non-traditional new technologies as well as traditional payment systems/electronic card schemes;
- enhance transparency;
- protect consumers and respond to their evolving needs;
- encourage greater public and private sector collaboration on matters of cyber-security, including the active sharing of information and intelligence; and
- amend regulations to ensure technology neutrality.

If you have any further questions regarding our response contained in this submission, please do not hesitate to contact Ms Taleen Shamlian, Head of Government Affairs & Public Policy, Australia, New Zealand & the South Pacific (e: tshamlia@visa.com) at any stage.

Yours sincerely

Stephen Karpin
Group Country Manager
Australia, New Zealand and the South Pacific

Visa Submission to the Commonwealth Treasury Review into the Findings of the Australian Financial System Inquiry

31 March 2015

SUMMARY

Visa Inc. is a global payments technology company that connects consumers, businesses, financial institutions and governments in more than 200 countries and territories worldwide. Visa is proud to adhere to our corporate mission of being the best way to pay and be paid, for everyone, everywhere. That is, we aspire to be "everywhere you want to be" and we deliver on this through the world's largest retail electronic payments network.

In the four quarters ending December 2014, Visa's global network encompassed 2.3 billion cards making around 98 billion transactions through 14,300 financial institutions. These participants transacted US$7.4 trillion in total volume of which US$4.8 trillion was payment volume. Around 2.3 million ATMs were also connected to our system.

This activity is in turn powered by one of the world's most advanced processing networks, VisaNet, which is capable of handling more than 47,000 transactions per second reliably, conveniently and securely. Electronic payments have increasingly been adopted by Australian consumers, retailers, businesses and governments as an efficient, effective and secure means of enabling payment transactions. Electronic payments regulation needs to be reflective of this success, focused on the future and cognisant of the risks of over-regulation and unlevel regulatory impacts.

In light of these issues, Visa has actively participated in the Federal Government's 2013-14 Financial System Inquiry (FSI), along with reviews conducted by other agencies such as the Reserve Bank of Australia (RBA) over the preceding decade. In each of our submissions to these reviews Visa has stressed the need for balanced, equally applied and innovation enabling approaches to regulation of electronic payments. We stand by these positions.

We acknowledge the recent work of the FSI, following the Government's explicit inclusion of payments regulation in the FSI Terms of Reference. The FSI very clearly raised concerns with the way interchange is regulated in Australia, and in particular, the lack of competitive neutrality of the current framework. We acknowledge this work as the clearest statement of this fundamental challenge to the Australian payments regulatory landscape, which, as outlined in previous Visa submissions, has impacted Australian merchants to the cost of A$770 million since the unlevel playing field was first established[1].

Since the release of the FSI Report in late 2014, the Payments System Board (PSB) of the RBA has released its *Review of Card Payments Regulation* (RBA Review). We understand the RBA Review will now deal with all key payments regulatory issues under the current powers afforded to the *Payment System (Regulation) Act 1998* (PSRA). Visa will work constructively within the RBA Review.

[1] Deloitte Access Economics Report as the Attachment to Visa's second submission. See fsi.gov.au

Beyond the RBA Review, in this submission we address ongoing concerns over the PSRA itself, the need for a strong position from Treasury on regulatory level playing fields and two other issues in the FSI Final Report of relevance to Visa, namely the issues of cyber-security and digital identity.

RECOMMENDATIONS

1. The PSRA, a legacy Act originally drafted almost two decades ago and no longer reflective of the current or future payments landscape, should be reviewed by the Treasury, on behalf of the Federal Government.

2. As part of the review proposed in Recommendation 1, consideration should be given to amending the PSRA to ensure it is future proofed by updating the definition of a "payment system" and delivers a level regulatory playing field by incorporating a basic licensing system and equal regulation for all like payment systems.

3. Treasury should advise the Federal Treasurer and wider Federal Government that regardless of the outcomes of the RBA Review process it supports a level playing field in relation to the regulation of interchange and interchange-like fees across all comparative electronic payment schemes.

4. Support the FSI report's Recommendation 38, calling for a formal framework for cyber-security information sharing and response to threats to be established via an industry Memorandum of Understanding. Government should also consider how security standards can best mitigate against cyber threats, while at the same time allowing organisations a cost-effective path to compliance.

5. In the rapidly evolving world of payments, we support the FSI report's Recommendation 39, to amend regulations in financial services to be technology neutral. We support the FSI's recommendation that a working group be established to prioritise areas to review the regulations, and support other non-financial system sector players, such as telecommunications sector, to participate in these forums. Government policy guidelines should also explicitly incorporate technology neutrality as additional criteria for assessing the impact of regulations to the financial services sector.

KEY ISSUES

A. LEGISLATIVE FRAMEWORK

A review is overdue

The PSRA was passed in 1998, some 17 years ago. It arose from the work of the Wallis Inquiry in 1996, some 19 years ago. Two-decades is a long period of time for any legislation to remain unreviewed and unamended in any substantive manner. This is particularly so when the legislation relates to an area that is so closely aligned to technology, financial services and innovation. If for no other reason than the passage of time, to ensure good public policy outcomes are being appropriately achieved, it is our view that the PSRA should be formally reviewed by the Treasury for the Federal Government.

Beyond the issue of needing assessment due to the passage of a substantial period of time, we believe that the PSRA is problematically structured in a manner that facilitates piecemeal implementation and has allowed the development of inefficient and anti-merchant and anti-consumer public policy outcomes.

Lack of automatic application

Under the PSRA, the RBA has discretion to take certain actions in relation to payment system operators, namely it may, among other things "designate" a particular payment system as being subject to its regulation and then set "standards" for safety and efficiency for that system, with such standards being open to cover issues such as technical requirements, procedures, performance benchmarks and pricing. Specifically, under Division 2 of the PSRA, the RBA has discretion to designate a payments scheme as a "payments system" under the Act. Specifically, under Section 11 of the PSRA, the RBA designates payment systems if it deems it is in the "public interest" to do so.

This is not merely an academic concern. Since the promulgation of the PSRA, the powers to designate and apply standards have in fact been deployed in a manner that has meant only some "payment systems" in Australia are regulated whilst others are not. The RBA has regulated traditional four-party model schemes, being Visa and MasterCard, who were in operation at the commencement of the PSRA, but has not regulated traditional three-party model schemes, namely American Express and Diners Card, even as those schemes opened their traditional 'closed loop' model to become four party (Amex Global Network Services, or "GNS", and Diners Card companion cards). Further, new entrant four-party modelled schemes, namely UnionPay, have been excluded from designation.

The net effect of the PSRA structure is that, unlike other regulated sectors where the impact of regulation is automatically applied to all current and future new entrant participants, payment schemes may or may not be regulated solely at the discretion of the regulator. That is, whilst the Australian Prudential Regulatory Authority (APRA) and the Australian Securities and Investments Commission (ASIC) do not have discretion to determine that what is plainly a

banking institution or a corporate entity are in fact not such and are then not regulated as such, under the PSRA, the RBA holds such discretion in relation to payment systems.

Equally, several wholly new models of payment system have entered the Australian market and remain unregulated in any way. Examples of these include PayPal , crypto wallets, ApplePay, payment facilitators and Google Wallet. These will undoubtedly be joined by many others in the future.

Fair and equitable application of the regulations is likely best achieved by requiring payment system operators to seek a license prior to commencing operations in Australia. This is analogous to most other regulated sectors, including banking and company regulation. This would also apply to incumbent operators, including currently regulated four-party model schemes and unregulated new entrant four-party model and three-party model schemes. Furthermore, this license requirement would extend to new non-traditional payment system operators such as PayPal.

Definition of a "payments system"

In addition, the scope and definition of what constitutes a "payment system" under the PSRA is problematic in our view.

Section 7 (Definitions) of the PSRA defines a "payments system" as:

> *"a funds transfer system that facilitates the circulation of money, and includes any instruments and procedures that relate to that system".*

Whilst this current definition would appear sufficiently wide to capture both existing three-party model payment systems and new entrant four-party model systems (i.e., we submit that the American Express GNS business, Diners companion cards and any UnionPay business all should meet this definition) in relation to non-traditional models of payment system, such as PayPal, Google Wallet and any number of yet unforeseen entrants and models, this definition may require amendment to increase its scope, clarity and future-readiness.

As such, there is a need to deal with the current challenges to competition and efficiency in the payments market, capturing current, new and future market entrants in recognition of an ever-evolving payments industry by revisiting the definition and scope of payment systems under the PSRA.

Legislative Framework Recommendations

1. *The PSRA, a legacy Act originally drafted almost two decades ago and no longer reflective of the current or future payments landscape, should be reviewed by the Federal Treasury, on behalf of the Federal Government.*

2. *As part of the review proposed in Recommendation 1, consideration should be given to amending the PSRA to ensure it is future proofed by updating the definition of a "payment system" and delivers a level regulatory playing field by incorporating a basic licensing system and equal regulation for all like payment systems.*

B. ENDORSEMENT OF A LEVEL PLAYING FIELD

As mentioned above Visa is now fully engaged in the recently commenced RBA Review. As with our submissions to the FSI and earlier submissions to RBA processes, Visa will again outline the competitive advantages afforded to payment schemes that operate outside the regulations. In the case of American Express, this unlevel playing field has facilitated the rise of companion cards. We note that the stage one consultation paper for the RBA Review states:

> *"The emergence of American Express companion card arrangements is likely to have led to an increase in the overall issuance of American Express cards and increased the average number of credit cards consumers hold. This may have adversely affected the competitive position of other card schemes" (page 32, RBA Review)*

Visa contends this is indeed the case. As part of our engagement in the RBA Review, Visa will again outline the strong empirical case that illustrates the impact of the unlevel regulatory playing field.

We do however feel that the Treasury review of the FSI outcomes presents an important parallel opportunity for the Federal Treasury to clearly advise the Federal Treasurer and Federal Government that there is and currently remains an unlevel playing field in the regulation of retail credit card payment systems in Australia and that, regardless of the outcomes of the RBA Review process, Federal Treasury supports a level playing field in relation to the regulation across all comparative electronic payment schemes for all the many reasons established in our FSI submissions.

Endorsement of a Level Playing Field Recommendation

3. *Treasury should advise the Federal Treasurer and wider Federal Government that regardless of the outcomes of the RBA Review process it supports a level playing field in relation to the regulation of interchange and interchange-like fees across all comparative electronic payment schemes.*

C. CYBER-SECURITY

As observed in the FSI report, cyber-security is critical to ensuring the resilience of the financial system. The potential threat from cyber-crime is becoming ever more apparent with the growth in interconnectivity, increasing network speeds and the broad distribution of technology. Cyber-crimes can come in many forms, ranging from criminal data breaches to denial-of-service style attacks on processing systems. A cyber-crime induced crisis in the financial system could lead to significant consumer detriment and lack of confidence in the financial system, especially if a cyber-attack was carried out at a significant scale.

As discussed in our previous FSI submission, Visa takes cyber security very seriously. Fighting fraud and protecting cardholders is fundamental to Visa's success. Visa invests significantly in advanced fraud-fighting technologies as well as developing innovative programs to protect cardholders, merchants and network participants . Visa's global fraud rate is at historic lows – fewer than six cents of every $100 transacted on a Visa card is lost to fraud. In the event that fraud does occur in Australia, Visa cardholders are protected through Visa's *Zero Liability Policy*, which guarantees that cardholders are not liable for fraudulent or unauthorised purchases made with their Visa card. Moreover, our investments in technologies (such as EMV and the roll out of chip-and-PIN cards in Australia) have had a noticeable and reducing effect on fraud rates (see our earlier submission). We have also published *What To Do If Compromised guide* for Visa clients or members, merchants, agents, and third-party service providers.[2] It contains step-by-step instructions on how to respond to a data breach and provides specific time frames for the delivery of information or reports.

Visa fully supports the FSI's *Recommendation 38* regarding policy proposals that seek to mitigate against cyber security attacks.

The Cyber Security Strategy (CSS) was released in 2009, and has not been revised since then. In the meantime, cyber threats to Australians have increased as they have become more reliant on ecommerce as part of their daily lives. This is important given that 83 percent of compromises in Australia involved ecommerce merchants (in 2013). Re-evaluating Australia's cyber security strategy would be an important first step for Government.

Visa strongly believes that security is a shared responsibility and all participants in the payment system have a role to play in protecting it. Visa is fully committed to educating, sharing best practice and collaborating with all key stakeholders to strengthen the payments infrastructure. As discussed in our previous submission, Visa works very closely with a range of stakeholders – including government and law enforcement – to improve data security and minimise fraud. In Australia, we coordinate and drive industry-wide initiatives such as the Australian Industry Working Group on Security. More recently, Visa is participating in an industry-wide exercise with the Attorney General's department having oversight.

[2] Visa's *What To Do If Compromised guide* can be found at:
http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

However, we feel that more could be done and in a more structured and frequent way, including through a more formal group of stakeholders that can better communicate, collaborate, inform and share intelligence. We feel that this approach will be critical going forward.

We support the FSI's recommendation that the Government should better coordinate and clarify the roles of the public and private sectors in a financial system cyber-crisis to ensure a rapid, coordinated and effective response. Visa recommends that this goal be established via a Memorandum of Understanding across government, financial institutions, law enforcement agencies (such as the Australian Security Intelligence Organisation, Australian Federal Police, Australian Crime Commission, and State police) and other industry players.

While not actively considered in the FSI report, Visa believes that the best form of mitigating cyber threats is to continue to enhance and invest in lifting security standards and practices across industries and critical infrastructure sectors. To this end, we believe that the Treasury and Government should consider opportunities to set clear and high goals and to establish standards that are risk-based, while at the same time, allowing organisations to adapt to their own solutions. Setting standards is crucial to ensuring interoperability while at the same time allowing a cost-effective path to compliance for organisations.

For example, global payment brands (including Visa Inc.) established the Payment Card Industry (PCI) Security Standards Council to develop, maintain and manage the PCI Security Standards. The Standards cover everything from the point of entry of card data into a system, to how the data is processed, through to secure payment applications. We seek to protect and educate industry players such as merchants, processors, financial institutions, and any other organizations that store, process, and transmit cardholder data, around the world.[3]

In Australia, standards should also take into consideration that a one-size-fits-all solution will be inappropriate given the size, complexity, and industry dynamics of the player (e.g. compare a mid-size grocery chain to a global hotel chain). The key is that players can meet strong security standards without compromising their operational goals. In fact, operational goals are further enhanced when all players cooperate at a higher standard.

Cyber-Security Recommendation

4. *Support the FSI report's Recommendation 38, calling for a formal framework for cyber-security information sharing and response to threats to be established via an industry Memorandum of Understanding. Government should also consider how security standards can best mitigate against cyber threats, while at the same time allowing organisations a cost-effective path to compliance.*

[3] Further information can be found at: https://www.pcisecuritystandards.org/index.php

D. TECHNOLOGY NEUTRALITY

As one of the FSI report's key themes, technology has transformed financial services in the 17 years since the Wallis Inquiry report. Looking forward to the next 17 years – or even the next five, or ten – we are likely to see emerging technologies change everything again.

It is impossible to predict exactly what the financial landscape will look like in the future, especially in the rapidly evolving world of payments. Payments innovation is being driven in large part by consumer choice. Consumers want faster, more convenient transactions, which new form factors like contactless cards and mobile payments give them. Sixty per cent of all face-to-face Visa transactions in Australia are now made using Visa payWave. When we compare this to the forty per cent of all transactions a year ago, this is a significant increase. In the next 12 months, we may also see cloud-based mobile payments take off in the Australian market too.

The speed of innovation means it's critical for the Government to recommend changes that give the financial system ample room to adapt to future developments, both predicted and unforeseen. We support the FSI's intent to ensure that technology is neutral to ensure that any mode of technology is agnostic to the regulations supporting its innovation, access and use. We support an industry working group on these matters to identify areas of priority in the regulation of technology. We would also support inviting the non-financial system sector, such as telecommunication players given the increasing reliance on handsets for payments. Government policy guidelines should also explicitly incorporate technology neutrality as additional criteria for assessing the impact of regulations to the financial services sector.

Technology Neutrality Recommendation

5. *In the rapidly evolving world of payments, we support the FSI report's Recommendation 39, to amend regulations in financial services to be technology neutral. We support the FSI's recommendation that a working group be established to prioritise areas to review the regulations, and support other non-financial system sector players, such as telecommunications sector, to participate in these forums. Government policy guidelines should also explicitly incorporate technology neutrality as additional criteria for assessing the impact of regulations to the financial services sector.*