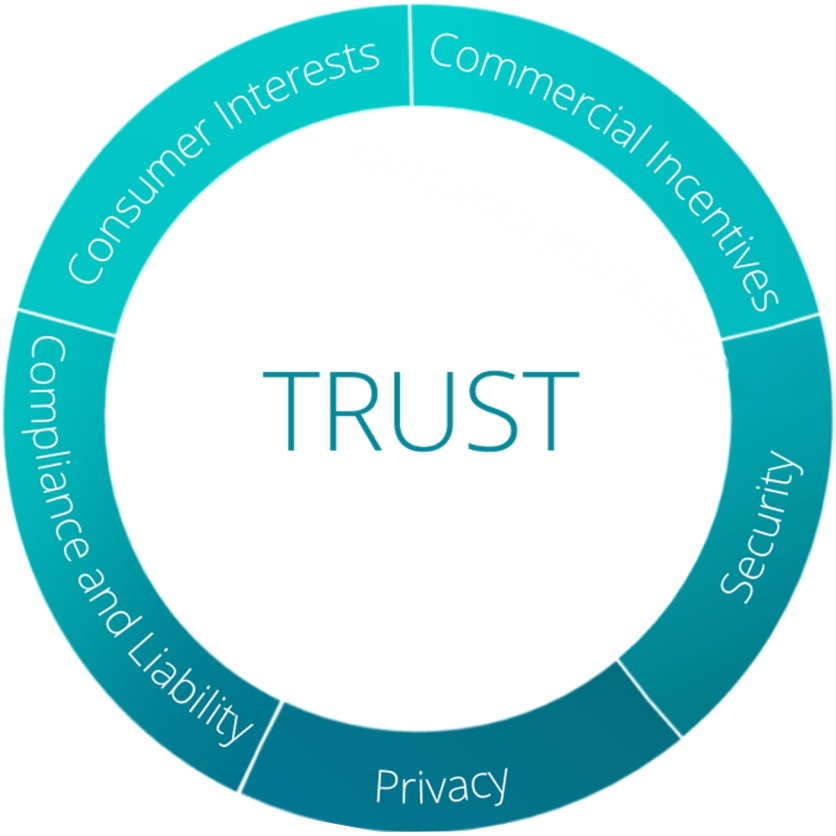


# TRUSTED DATA SHARING:

## NOW AND IN THE FUTURE

Australian Payments Clearing Association

Submission to the Productivity Commission Inquiry into

Data Availability and Use

**July 2016**

Australian Payments Clearing Association Limited ABN 12 055 136 519
Level 6, 14 Martin Place, Sydney NSW 2000 Telephone +61 2 9216 4888 Facsimile +61 2 9221 8057 www.apca.com.au

# Contents

# Executive Summary

Trust is the cornerstone of data sharing. It is at the centre of the many and varied data sharing arrangements in place today.

Trust is also the foundation of the Australian payments system. This system plays a crucial role in Australia's economy and as the economy becomes more digital, it generates increasing amounts of data.

The data generated by participants in Australia's payments system is high value data. It is used to solve problems, deliver benefits and meet obligations. For example:

- The industry shares fraud and financial crime data to ensure maximum resilience
- Financial institutions share payments data with a range of private sector organisations to create new products and services
- Governments use payments data to help improve public services and regulate Australia's financial system

Importantly, current approaches to data sharing are effective because they successfully protect consumers, maintain trust and balance the commercial interests of stakeholders. This is achieved through alignment of five core requirements:

## Consumer interests, security, privacy, commercial incentives, compliance and liability.

Aligning these requirements gives consumers the control they want, while providing safety and protection. It also provides the returns necessary to continue to justify investments in developing and attaching intellectual property to datasets.

Data sharing delivers improved efficiency, innovation and value for consumers. It should be maximised for opportunities to achieve 'common good', where there are clear commercial incentives and the security and privacy needs of consumers are met.

Internationally, governments are pursuing open data policies and this provides interesting context. However, these policies are yet to be applied in practice and their ability to effectively align the core requirements of data sharing is untested.

Current data sharing arrangements have created a vibrant marketplace and provide a strong platform for a future where data sharing continues. These arrangements maintain trust, address the needs of all participants and should be used as the basis of future data sharing.

The ultimate success of the future of data sharing is reliant on how trust is established and maintained as more data is made available in the digital economy. The Australian Payments Clearing Association (APCA) – as the payments industry body with a track record of delivering collaborative industry outcomes – welcomes the opportunity to work with all stakeholders to ensure trust in data sharing. Maintaining trust in payments data is critical to the continued overall confidence in Australia's payments system.

# Introduction

The Australian Payments Clearing Association (APCA) – as the industry association and self-regulatory body for Australian payments – has an ongoing role in examining the opportunities and challenges of payments data sharing.

### The purpose of this submission

We have prepared this submission to the *Productivity Commission Inquiry into Data Availability and Use* to share our experience in generating value and providing consumer and business benefits through payments data sharing.

Our collaborative approach and experience brokering data sharing arrangements provides positive groundwork for the future.

APCA's submission focusses on payments data only. It outlines the core requirements necessary to ensure continued success in data sharing.

### How this submission was prepared

The Australian payments market is diverse. To prepare this submission, APCA formed an industry working group that reflects the diversity of the market.

The participants have expressed willingness and commitment to collaborate. This is inherent in the establishment and make-up of this working group. This includes exploring how the core requirements of consumer interests, security, privacy, commercial incentives, compliance and liability might be aligned within a framework that helps manage the desire to 'enhance consumer outcomes, better inform decision making, and facilitate greater efficiency and innovation in the financial system and the broader economy'.[1]

### Participants in APCA's working group include:

- Australian Settlements Limited (ASL)
- Australia and New Zealand Banking Group Limited (ANZ)
- Commonwealth Bank of Australia (CBA)
- Cuscal Limited (Cuscal)
- National Australia Bank Limited (NAB)
- The Reserve Bank of Australia (RBA)*
- Tyro Payments Limited (Tyro)
- Westpac Banking Corporation (WBC)

**The RBA is represented by its Banking Department which provides transactional banking services to government.*

[1] Financial System Inquiry. *Data access and use.*

APCA also sought the views of a broad range of stakeholders including consumer groups, payments schemes, research organisations, FinTech organisations and other industry bodies through written correspondence, roundtables and a series of face-to-face meetings.

APCA acknowledges the time and insights provided by these stakeholders.

### What is payments data?

Payments data is broadly defined as any data collected and stored electronically when a payment occurs. This data is generated when a payment is initiated via:

*Credit/debit card transactions*


*Mobile Wallet Transactions*

*ATM Withdrawals*

*Electronic funds transfers: direct debits, direct credits, internet banking Pay Anyone, mobile payments*

*Cash withdrawals and deposits*

*Cheque Transactions*

## The payments system is critical to Australia's financial system and the data it generates is highly valuable

Consumers interact with and rely on the Australian payments system every day. As one of the core components of Australia's financial system, the payments system plays a crucial role in Australia's economy.

Australia's payments habits are increasingly digital[2] and as a Deloitte report[3] recently identified, this means much more data can be captured with each payment.

Payments data is also increasingly valuable. The report identifies:

> *'Payments data is more valuable than ever, thanks to improvements in the ability to handle, consolidate and interpret it.'*

Because of these improvements, participants in Australia's payments system are able to share increasing amounts of data. This generates value for a range of stakeholders:

- **Policy makers and regulators** use payments data to assess various aspects of the financial system and the economy
- **Governments** use payments data to improve services
- **Consumers'** lives are improved when payments data is used to solve consumer protection problems and deliver innovation in products and services
- **Businesses** collect, analyse and use data to help improve customer experience and receive a return on their investment

Examples are provided in *Table 1* of this submission.

Payments data has the potential to provide even greater value to consumers. Financial institutions continue to invest in data collection, analysis and enrichment in recognition of this value.

[2] Deloitte (2015). *Navigating the New Digital Divide*
[3] Deloitte. (2015). *Payments disrupted: The emerging challenge for European retail banks*

# Payments data shared today improves consumer outcomes

The payments industry is steadfast in its responsibility to protect all customers and is actively engaged in the use of data to reduce fraud and financial crime.

There is enormous benefit in tackling issues such as these and they are actively supported because the benefit is clear.

Beyond this, there is a large amount of social value in data that is yet to be realised.[4] This is reflected in the European Commission report *'Towards a thriving data-driven economy.'* [5]

> *'A thriving data-driven economy will contribute to the well-being of citizens as well as to socio-economic progress…'*

## Data sharing should be maximised where there are clear opportunities to achieve 'common good'. This should be a focus for future data sharing.

### Data sharing to reduce financial crime

Data sharing and analysis is the basis of 'common good' initiatives such as the Australian Financial Crimes Exchange (AFCX). The AFCX provides a good example of how industry shares data to improve consumer outcomes and ensure the safety and resilience of the payments system.

### The Australian Financial Crimes Exchange (AFCX)

*The Australian Financial Crimes Exchange (AFCX) was established in March 2015. Its purpose is to develop mechanisms to share information and strengthen the response to fraud and financial crimes.*

*The AFCX will be the primary channel through which public and private sector will coordinate intelligence and data sharing activities for the investigation and prevention of financial crimes including fraud and cybercrime.*

*The AFCX is establishing a defined data catalogue of financial crime categories and data elements that will be shared. The result will be an industry standard data and intelligence sharing format.*

[4] SIIA (2013). *Data-Driven Innovation – A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data.*
[5] European Commission. (2014). *Towards a thriving data-driven economy. Brussels.*

### Data sharing to combat fraud

Financial institutions also share data to reduce fraud. This data is published by APCA twice a year and used as the basis for targeted fraud mitigation strategies. These initiatives include: [6]

- Get Smart About Card Fraud Online
- Protect Your PIN
- Safeguard Against Skimming

### Data sharing with third parties

Data sharing has created a vibrant marketplace that benefits consumers through product and service enhancement.

Financial institutions have a number of data sharing arrangements in place with third parties. These commercial arrangements contribute to the large amounts of data financial institutions share every day. [7] For example, financial institutions have partnerships in place with organisations to assess de-identified transaction data to derive insights, trends and shopping habits of different customer groups. The resulting analysis improves consumer outcomes and increases business performance.

The growing market for data sharing encourages competition and innovation and many financial institutions are actively pursuing opportunities for greater data sharing. This has seen financial institutions invest in data sharing start-ups such as Data Republic.[8]

In establishing arrangements with third parties, financial institutions use their significant experience aligning the core requirements of data sharing to assess the suitability of the potential recipient of the data. This includes determining if the recipient can meet the necessary standards required to keep data safe and secure, and ensuring appropriate liability arrangements.

[6] APCA. (2016). *Protect against fraud*
[7] National Australia Bank Group. (2015). *Online Retail Sales Index: In depth report*.
[8] Australian Financial Review. (2016)

### Financial institutions share data to improve financial decisions

Raw payments data is analysed to generate information, create insights and deliver benefits for customers. Some examples include:

Business customers receive analysed payments data to help improve their profitability.[9]

#### *Daily IQ*

*'Daily IQ' provides businesses with insights about their customers. It is designed to help the business make better informed business decisions. The service includes:*

- *Trends on a merchant's card sales*
- *Customer demographic information and spending patterns to help a merchant develop targeting strategies*

Data is used to provide home buyers, home owners, upgraders, investors and renovators with personalised home loans in real-time.[10]

#### Wonder

*Wonder uses the information about customers, such as income, assets, and the estimated value of their existing properties to provide customers with personalised home loan options in real time. This can include how a customer could apply for a loan to purchase a new property, or how they could apply for an increase to existing loans to finance other plans.*

Specific business challenges are addressed and opportunities identified through data driven insights.[11]

#### Insights as a service

*Partnerships with corporate customers and start-up data analytics companies such as Zetaris, provide 'Insights as a Service' using data driven insights to address specific business challenges and identify opportunities based on quantitative analysis.*

[9] Commonwealth Bank of Australia. (2016). *Daily IQ*.
[10] Westpac. (2015). *Westpac launches Wonder*
[11] Eyers, J. (2014). *Westpac's Reinventure buys into big data firm Zetaris*

### A strong platform to build on

The Australian payments industry supports data sharing.

The numerous arrangements in place today deliver consumer benefits and provide a strong platform for using data to generate greater efficiency and innovation, and deliver increased value for consumers. These arrangements should be used as the basis for greater payments data sharing.

### We should further educate the public on how data sharing occurs today

Financial institutions have policies in place on data use and are transparent about how data is shared. Despite this, research suggests the public understand little of the concept of personal data.[12]

As data sharing and use expands, efforts to educate consumers about data sharing should continue. Consumers may benefit from a public awareness campaign to help further their understanding of how data collection and sharing occurs today and the associated benefits and risks.

[12] Digital Catapult. (2015). *Trust in personal data: a UK review.*

**Table 1:** Data sharing can be grouped into three broad categories:

| Data Sharing Category | Objective | Example |
|---|---|---|
| Common good | Protect consumers<br><br>Solve socio-economic problems | • Australian Financial Crimes Exchange<br>• Australian Cyber Security Centre<br>• Financial hardship initiatives<br>• APCA Fraud Data |
| Innovation and performance | Make improvements to help meet consumer and business needs | • Nab/Quantium<br>• Accounting integration software<br>• CBA Daily IQ<br>• MasterCard Analytics<br>• Data Republic Partnerships<br>• Property Exchange Australia (PEXA) |
| Compliance and regulation | Satisfy compliance & regulatory obligations | • Retail Payments Statistics (RPS)<br>• ePayments Code: Reporting data on unauthorised transactions<br>• APRA Monthly Banking Statistics<br>• Payment Card Industry Data Security Standard Reporting<br>• RBA Interchange Studies<br>• Cost of payments studies<br>• Credit Bureau reporting |

# Trust is the cornerstone of data sharing

Trust is critical. A recent report from Telstra Corporation Limited looked at the views of millennials toward personal data. Banks are overwhelmingly seen as the most trusted institutions to store and protect personal data.[13]

> *'When asked about the platforms or organisations they trust with their personal information, 76% of millennials nominated banks'*

Today's data sharing arrangements align the essential requirements of data sharing and have effective governance models to ensure this trust is maintained.

Trust is vital for both public and private sector data sharing and this is recognised in the Public Sector Data Management Framework:[14]

> *'… it is crucial that we* [the public sector] *have the trust of the public. Strong assurances about data privacy and security based on rigorous adherence to protocols, and demonstrated value, are key.'*

Trust in data sharing can quickly perish if the considerations of security and privacy are not aligned.

For example, a recent data breach of Kmart Australia Limited (Kmart) compromised customers' identity, email address, delivery and billing address, telephone number and product purchase details. Kmart received numerous complaints from worried customers.[15]

This breach was small compared to a 2014 JPMorgan breach in which more than 70 million households and seven million small businesses may have had their private data compromised in a cyber-attack. At the time it was called "the single-largest theft of data from a US financial institution."

Dow Jones, which publishes The Wall Street Journal, also recently had hackers enter its networks, seeking contact and payment information for 3,500 customers.[16]

[13] Scopelliti, R. (2016). *Millennials, Mobiles & Money: the forces reinventing financial services.*
[14] Australian Government: Department of the Prime Minister and Cabinet. (2015, July). Public Sector Data Management.
[15] Bogle, A. (2016). *Kmart Australia Hit By Customer Data Breach Including Names and Addresses.*
[16] Crowe, P. (2015, November 10). *JP Morgan fell victim to the largest theft of customer data from a financial institution in US history.*

Because of public concern about privacy and security of data, these data breaches make news headlines and the alarm is amplified via social media. Even though the originator of the data may not have been responsible for a data breach, this is where consumers direct their concern and anger. The reputational and subsequent commercial harm can be substantial.

Trust is the positive outcome when the needs of all participants are addressed and the core requirements of data sharing are aligned.

The ultimate success of future data sharing arrangements depends on how trust is established and maintained as more data is made available.

# Aligning the requirements of data sharing is vital

The importance of maintaining privacy and security is widely accepted. However, to ensure a sustainable model, there are a number of important factors that must be taken into consideration. Today's data sharing arrangements align five (5) core requirements. These include:

1. Consumer interests
2. Privacy
3. Security
4. Compliance and Liability
5. Commercial incentives

The future of data sharing must be explored with the alignment of these requirements as a primary goal.

### 1. Consumer Interests

Consumers want control of their personal data and also want to share it in exchange for benefits.

Deloitte reported that 64% of consumers either did not mind or were happy to share their personal information if it led to direct benefits for them, such as financial savings, product improvements and personalised services.[17]

They also want data to be kept private and secure.

Consumers expect financial institutions to meet their expectations for privacy and security, and for this reason financial institutions have the responsibility to control data appropriately.

Balancing consumer expectations with the responsibility of the financial institution requires shared control.

[17] Competition and Markets Authority. (2015, June). *The commercial use of consumer data. Retrieved from The Competition and Markets Authority*

## 2. Privacy

In a recent article on trust and transparency in consumer data, the Harvard Business Review[18] reported credit card information, government identification and health information as the most highly valued data by consumers.

Privacy is important because consumers attach significant value to payments related information.

For this reason consumers have privacy concerns about sharing their data. De-identification and non-retention of data is often used to manage these concerns and is particularly useful, so long as de-identified data can't be overlayed with other data to make it identifiable. A recent report on Big Data and Privacy to the US President from the Council of Advisors on Science and Technology identified:

> *"In general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially. While anonymization may remain somewhat useful as an added safeguard in some situations, approaches that deem it, by itself, a sufficient safeguard need updating."*

The privacy related issues that could arise from the inappropriate use of payments data present significant challenges to data sharing.

Surveys indicate that many consumers have substantial concerns about the problems that may arise from sharing data. Attitudes vary depending on a range of factors, common concerns include: unintended data sharing and use and fears about exposure to nuisance contacts. [19]

Shared control between consumers and financial institutions must be assured to help manage privacy concerns.

## 3. Security

Maintaining security is critical to ensuring trust in data sharing. Consumers want convenience and security at the same time and financial institutions play an important role in balancing the two.

[18] Morey, T., Forbath, T., & Schoop, A. (2015, May). *Customer Data: Designing for Transparency and Trust. Retrieved from The Harvard Business Review*

[19] Competition and Markets Authority. (2015, June). *The commercial use of consumer data. Retrieved from The Competition and Markets Authority*

The high value of payments data makes it a constant target for criminal activity. A recent study on consumer attitudes to data sharing showed identity theft was the number one concern.[20]

The Australian Federal Police (AFP) also recognises identity crime as a threat to the Australian community. This lucrative crime causes considerable financial losses to the Australian Government, private industry and individuals.

The AFP states:

> *'Recent estimates by the Attorney-General's Department indicate that identity crime costs Australia upwards of $1.6 billion each year, with the majority (around $900m) lost by individuals through credit card fraud, identity theft and scams.'*

Protecting consumers from identity theft is a major consideration for organisations that securely manage their data.

The Australian payments systems has a robust security framework that provides strong protection for consumers. It is essential that this rigorous approach to security is maintained as data is shared.

A significant amount of research exists on consumer attitudes to sharing certain types of data, particularly with regard to security and privacy. Some of this suggests a level of backlash to data sharing. However there is limited research on consumer attitudes toward the privacy implications of sharing payments data. Better understanding these attitudes will help inform future data sharing.

### 4. Compliance and Liability

The e-Payments Code is a voluntary code that regulates consumer electronic payment transactions, including ATM, EFTPOS and credit card transactions, online payments, internet and mobile banking, and BPAY.

The Code may need to be amended to ensure it can maximise the potential of data sharing. While the code is relatively new, a large number of financial products and services have already been created to provide consumer benefit. As the payments system continues to evolve, the code may need to be expanded to cover all parties offering payments services.

The e-Payments Code sets out the rules for determining who pays for unauthorised transactions. Financial institutions are concerned the Code may not sufficiently support their

[20] Morey, T., Forbath, T., & Schoop, A. (2015, May). *Customer Data: Designing for Transparency and Trust. Retrieved from The Harvard Business Review*

terms and conditions which prohibit the disclosure of usernames and passwords to third parties that seek access to customer accounts.

Clarity should be provided to ensure the Code is not seen as shifting liability to the financial institution by virtue of the financial institution not preventing third party access to customer accounts. There is an opportunity to provide certainty for consumers and address these concerns when the Code is reviewed.

As data sharing continues, appropriate governance that effectively manages compliance and ensures the provision of penalties if things go wrong will be important for maintaining confidence in data sharing; it is important to all stakeholders in the payments system.

If the data collected by the third party is compromised and results in loss, third party providers must be able to meet the associated liability. At the same time, liability shifts must be considered to ensure the data originator is not unfairly burdened by risk.

Clarity about liability when breaches occur and what the penalties may be are important considerations for data availability and use.

### 5. Commercial Incentives

The importance of balancing commercial incentives with the wider consumer benefits of data sharing is well made in the Financial System Inquiry.

The Inquiry[21] describes the importance of return on investment in collecting data. It states:

> *'Private returns are necessary to justify investments in developing datasets.'*

The Inquiry also referenced the need to maintain commercial incentives in future data sharing. It states:

> *'Sharing data should not reduce incentives for businesses to collect the data in the future.'*

Collecting, storing, enriching and protecting data requires investment and a return on this investment. As this enrichment process occurs intellectual property is created.

Care must be taken to ensure that all stakeholders are able to balance their significant ongoing investment with their capacity to support continued data availability.

[21] Financial System Inquiry. *Data access and use.*

# International markets

There are lessons that can be learnt from markets where regulation is guiding data sharing arrangements.

Changes in European Union (EU) law concerning the Directive on Payment Services (PSD2) are set to obligate open access to payment services in 2018. Ahead of this timeline, the UK Treasury has moved to lead standards development for the UK payments industry. At the same time, the UK Government is continuing its work to give consumers improved access to data held by banks. This includes allowing consumers to authorise access by third parties.

The Open Banking Working Group (OBWG)[22] was set up in September 2015 at the request of the UK Treasury to explore how data could be used to help people transact, save, borrow, lend and invest their money. In February 2016 the Open Banking Standard (OBS) was set out by the OBWG. Its remit is to:

> *"guide how open banking data should be created, shared and used by its owners and those who access it"*

Work is ongoing and the minimum viable product for the OBS is intended to be launched in late 2016. Appendix 2 looks at how the considerations of data sharing are being managed in this market.

### Implications for Australia

While policies to enhance data sharing are further advanced in the UK, some critical aspects are yet to be addressed. For example, approaches to privacy and liability remain undefined.

It is not clear whether the right balance between consumer interests, commercial incentives, market stability, liability, security and privacy has been struck.

Both PSD2 and the OBS are government, rather than industry led, meaning industry expertise isn't utilised until the implementation phase. This can impact the ultimate success of implementation.

Implementing these policies is potentially very costly for businesses. The development of the technology and standardisation required could have a substantial impact on a business.

APCA is in discussion with Payments UK and will continue to monitor and interpret developments.

[22] Open Banking Working Group. (2015). *The Open Banking Standard.*

# APCA can align the essential requirements for a data sharing future

APCA provides a venue for collaboration to find industry solutions for complex issues while managing the commercial realities that competitors face. This is in addition to its operational role overseeing the major clearing systems and payments infrastructure. For example:

- Jointly with the RBA, APCA recently established the Australian Payments Council[23] (APC). The APC is the strategic coordination body for the payments industry.
- APCA established the Issuers and Acquirers Community (IAC) on 1 July 2015. The IAC provides a forum for discussions, establishes rules, standards and guidelines, and provides a range of specialty services for all card payments in Australia.[24]
- APCA administers the New Payments Platform (NPP). The NPP is the infrastructure that will provide Australian businesses and consumers with a fast, versatile, data-rich payments system.[25]
- APCA's role administering the payments infrastructure was also born out of industry collaboration. The Community of Interest Network (COIN) is a high availability, managed network for multilateral secure transmission of payments files and messages between payments participants. It provides an alternative to point-to-point connectivity between payments participants.[26]

Reflective of our work guiding the strategic direction and regulatory policy for Australia's payments industry, APCA has an ongoing role in examining the opportunities and challenges of payments data sharing.

The essential requirements of data sharing outlined in this submission must be aligned in any future policy framework to increase data availability. APCA is positioned to ensure this occurs via an industry developed framework.

## APCA should be the primary vehicle the government works with on the sharing of payments data.

[23] The Australian Payments Council. (2016). *About Us.*
[24] The Australian Payments Clearing Association. (2016). *Cards and Accepting Devices.*
[25] Australian Payments Clearing Association. (2016). *New Payments Platform*.
[26] Australian Payments Clearing Association. (2016). *The COIN.*

# Conclusion

The payments industry has demonstrated its ability to find solutions to complex industry matters.

As the industry body with a track record of delivering collaborative outcomes, APCA is well positioned to help guide policy on data sharing.

As current industry data sharing arrangements show, the challenges of data sharing are not insurmountable. Despite the sensitivity of payments data, the industry finds ways to share the valuable data it collects, deliver positive consumer outcomes and maintain trust in data sharing. This is achieved by aligning the five core requirements of data sharing.

Despite the data sharing that already occurs, understanding of the wider implications remains relatively low. As policies to increase data availability are explored, immediate attention should be given to increasing public understanding of how data is used and the associated benefits and risks.

In line with this and given its sensitivity, an increased understanding of Australian attitudes towards sharing payments data may also help guide policy development.

The Australian payments industry supports effective use of data to improve consumer outcomes and welcomes future opportunities to contribute to a data sharing future that builds on the proven arrangements that are in place today.

**Appendix 1:**

# About the Australian Payments Clearing Association

The Australian Payments Clearing Association (APCA) is the self-regulatory body for Australia's payments industry.

APCA's role includes providing strategic direction and regulatory policy for the Australian payments system.

APCA is a venue for industry collaboration and works closely with government, regulators, payments stakeholders and individuals to improve the payments system.

APCA was established in 1992 to manage and develop regulations, procedures, policies and standards governing payments clearing and settlement within Australia. It oversees five clearing systems covering cheques, direct debits and direct credits, aspects of eftpos and ATM transactions, high value payments and bulk cash exchanges between financial institutions.

APCA also administers the Community of Interest Network (COIN) infrastructure system which provides network services and connectivity for retail payments. More than 98% of Australia's non-cash payment values are cleared through these various systems.

Jointly with the RBA, APCA recently established the Australian Payments Council[27] (APC). The APC is the strategic coordination body for the payments industry.

APCA also continues its work administering the New Payments Platform: the infrastructure that will provide Australian businesses and consumers with a fast, versatile, data-rich payments system for making their everyday payments.[28]

[27] The Australian Payments Council. (2016). *About Us*.
[28] Australian Payments Clearing Association. (2016). *New Payments Platform*.

**Appendix 2**

# PSD2/OBS approach to data sharing

*Unless otherwise referenced quotes are taken directly from the text of the Revised Directive on Payment Services (PSD2)[29] or the Open Banking Standard (OBS)[30]*

| Data sharing consideration | How it is addressed | | APCA Comment |
|---|---|---|---|
| | PSD2 | OBS | |
| **Consumer Interests** | According to PSD2's Commissioner for competition policy:<br>*"We have already used EU competition rules to ensure that new and innovative players can compete for digital payment services alongside banks and other traditional providers. Today's vote by the Parliament builds on this by providing a legislative framework to facilitate the entry of such new players and ensure they provide secure and efficient payment services. The new Directive will greatly benefit European consumers by making it easier to shop online and enabling new services to enter the market to manage their bank accounts"*[31] | The OBWG expects:<br>*"existing providers and new entrants would compete to dramatically improve existing products by making them more intuitive, personalised, convenient and integrated. In addition, customers would be expected to benefit from a suite of new propositions that are enabled through open APIs."* | Overseas arrangements are resolute in pursuing consumer interests, however some of the factors that ensure consumers are also protected are yet to be finalised. |
| **Commercial incentives** | PSD2 specifies that access to payment services should be completely open to approved third parties. | OBS reflects PSD2. | It is expected that account providers may pursue commercial interests and competitive advantage by supporting additional non-mandatory services. |

[29] The European Parliament and the Council of the European Union. (2015, November 25).
[30] Open Data Institute. (2016). *The Open Banking Standard*.
[31] European Commission. (2015, October 08). *European Parliament adopts European Commission proposal to create safer and more innovative European payments*.

| Data sharing consideration | How it is addressed | | APCA Comment |
|---|---|---|---|
| | PSD2 | OBS | |
| Compliance | PSD2 does not have a defined approach to compliance.<br><br>It does however suggest the creation of a 'competent authority' that would grant third parties authorisation to operate as Payment Service Providers. This 'competent authority' will need to evaluate the privacy standards proposed by third parties in providing authority to operate. | The OBWG recommends an independent authority (IA) to ensure standards and obligations between participants in the OBS are upheld using a risk-based approach. The obligations would cover issues such as "how customer complaints are handled, how data is secured once shared and the security, reliability and scalability of the APIs provided."<br><br>The IA would be responsible for vetting and accrediting third parties that wished to access the payments infrastructure. | There is an implicit assumption that the competent authority (or independent authority under the OBS) would also drive the education and awareness programs needed to support the new initiatives. |
| Privacy | PSD2 does not have a defined approach to privacy.<br><br>The suggested 'competent authority' will need to evaluate the privacy standards proposed by third parties in providing authority to operate. | The OBS has not yet defined their approach to privacy. Their minimum viable product focuses on standardising information that is already publicly available.<br><br>The OBS does however recommend a working group to address privacy risks. | The European General Data Privacy Regulation (GDPR) covers the expected right to privacy for an individual.<br><br>However, it is unclear how privacy considerations will be adhered to. |

| Data sharing consideration | How it is addressed | | APCA Comment |
|---|---|---|---|
| | PSD2 | OBS | |
| **Security** | PSD2 does not have a defined approach to security.<br><br>The suggested 'competent authority' will need to evaluate the security standards proposed by third parties in providing authority to operate. | The OBS specifies that a customer must control which third parties have access to their information. It further outlines an approach to authentication and authorisation. Authorisation focuses on five areas:<br><br>• Permissions – specific permissions to access data and/or functionality<br>• Roles – a set of permissions and roles should be defined to clearly outline what customers are approving and what third parties are permitted to do.<br>• Certification – provides a whitelist of companies<br>• Encryption – a standardised level of encryption<br>• Security Standards – security accreditation based off ISO27001 | Customers will have control over the sharing of their data. It must be clear to the customer what data they agree to share. |

| Data sharing consideration | How it is addressed | | APCA Comment |
|---|---|---|---|
| | PSD2 | OBS | |
| **Liability** | Under PSD2, a customer is entitled to address a refund claim to the account provider:<br><br>*"even where a third party is involved, without prejudice to the allocation of liability. There is a formal obligation on the third party to "immediately compensate" the account provider where the latter is liable for an unauthorised payment transaction or a non-executed or defective payment. In both cases the burden of proof is on the initiator."*<br><br>In summary, while the account provider (i.e. bank) is immediately liable, they have redress in recovering funds from the third party.<br><br>Once the third party receives the information from the data attribute provider, it is assumed that it will be doing so as a data controller and therefore will be responsible for ensuring compliance with the Data Protection Act, even in the case of serious data breaches. Under the PSD2 regulation the PSP would be liable to bear any financial consequences. | The OBS is bound by PSD2 and deals with liability as outlined by PSD2.<br><br>Payment Service Providers (PSP) have a duty under the UK's Data Protection Act to ensure data is kept secure and protected from fraud and misuse of personal data. | It seems likely that the accreditation of a third party would be removed in the event of a breach. |

**Table 2:** How is OBS/PSD2 addressing the considerations of data sharing?

# References


Australian Federal Police. (2016). *Identity Crime: what is identity crime?* Retrieved from https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime

Australian Financial Review. (2016). Retrieved from http://www.afr.com/business/banking-and-finance/financial-services/nab-westpac-and-qantas-invest-in-data-republic

Australian Government: Department of the Prime Minister and Cabinet. (2015, July). *Public Sector Data Management.* Retrieved from https://www.dpmc.gov.au/sites/default/files/publications/public_sector_data_mgt_project.pdf

Australian Payments Clearing Association. (2016). *Protect against fraud*. Retrieved from APCA: http://www.apca.com.au/about-payments/protect-against-fraud

Australian Payments Clearing Association. (2016). *Cards and Accepting Devices*. Retrieved from http://www.apca.com.au/payment-systems/cards-accepting-devices

Australian Payments Clearing Association. (2016). *New Payments Platform*. Retrieved from APCA: http://www.apca.com.au/about-payments/future-of-payments/new-payments-platform-phases-3-4

Australian Payments Clearing Association. (2016). *The COIN*. Retrieved from APCA: http://www.apca.com.au/payment-systems/coin

Australian Securities and Investments Commission. (2016). *ePayments Code*. Retrieved from ASIC: http://asic.gov.au/for-consumers/codes-of-practice/epayments-code/

Bogle, A. (2016). *Kmart Australia Hit By Customer Data Breach Including Names and Addresses*. Retrieved from MashableAustralia: http://mashable.com/2015/10/01/kmart-australia-data-breach/#CcdF0TZWiEqi

Commonwealth Bank of Australia. (2016). *Daily IQ*. Retrieved from Commonwealth Bank: https://www.commbank.com.au/business/online-banking/commbiz/daily-iq.html

Competition and Markets Authority. (2015, June). *The commercial use of consumer data.* Retrieved from The Competition and Markets Authority: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf

Crowe, P. (2015, November 10). *JP Morgan fell victim to the largest thefot of customer data from a financial institution in US history.* Retrieved from Business Insider: http://www.businessinsider.com/jpmorgan-hacked-bank-breach-2015-11

Deloitte. (2015). *Navigating the New Digital Divide.*

Deloitte. (2015). *Payments disrupted: The emerging challenge for European retail banks.*

Digital Catapult. (2015). *Trust in personal data: a UK review.*

European Commission. (2014). *Towards a thriving data-driven economy.* Brussels.

European Commission. (2015, October 08). *European Parliament adopts European Commission proposal to create safer and more innovative European payments*. Retrieved from European Commission Press Release Database: http://europa.eu/rapid/press-release_IP-15-5792_en.htm?locale=en

Eyers, J. (2014). *Westpac's Reinventure buys into big data firm Zetaris.* Retrieved from Australian Financial Review: http://www.afr.com/technology/cloud-computing/westpacs-reinventure-buys-into-big-data-firm-zetaris-20141111-11koyc

Financial System Inquiry. (n.d.). *Data access and use*. Retrieved from Financial System Inquiry: http://fsi.gov.au/publications/final-report/chapter-3/data-access-and-use/

Morey, T., Forbath, T., & Schoop, A. (2015, May). *Customer Data: Designing for Transparency and Trust.* Retrieved from The Harvard Business Review: https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

National Australia Bank Group. (2015). *Online Retail Sales Index: In depth report.*

Open Banking Working Group. (2015). *The Open Banking Standard: unlocking the potention of open banking to improve competition, efficiency, and stimulate innovation.* Retrieved from https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%202%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf

Open Data Institute. (2016). *The Open Banking Standard*. Retrieved from https://theodi.org/open-banking-standard

Scopelliti, R. (2016). *Millennials, Mobiles & Money: the forces reinventing financial services.* Retrieved from Telstra Global: https://www.telstraglobal.com//templates/millennials/assets/gated-content-millennials-mobiles-money.pdf

SIIA White Paper. (2013). *Data-Driven Innovation – A Guide for Policymakers: Understanding and Enabling the Economic and Social Value of Data.*

The Australian Payments Council. (2016). *About Us*. Retrieved from http://australianpaymentscouncil.com.au/about-us/

The European Parliament and the Council of the European Union. (2015, November 25). *Driective (EU) 2015/2016 of the European Parliament and of the Council* . Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2366&from=EN

Westpac. (2015, 10 01). *Westpac launches Wonder - innovative technology to help Australians reach their property dreams*. Retrieved from http://www.westpac.com.au/about-westpac/media/media-releases/2015/1-october