Co-Host of ATPS-APAC 2017
The Regulatory Environment

Interchange, Data Protection and Open Data

Presented by

Lance Blockley
Agenda

Recent focus areas for regulation

Interchange Regulation: Reserve Bank of Australia - Review of Card Payments Regulation

Data Protection: European Union - General Data Protection Regulation (GDPR)

Open Data: Productivity Commission Inquiry - Data Availability and Use

ATPS Asia-Pacific
29th – 31st August 2017
Interchange Regulation

Reserve Bank of Australia’s
Review of Card Payments Regulation
Interchange revenue streams will alter with the revised RBA regulations

1 July 2017: keep 0.5% weighted average on V/MC credit cards, but checked quarterly
- Cap the top interchange rate at 0.8%
- Bring in American Express companion cards of the Big 4 banks
- Merchant surcharging rules tightened

These changes have wide-ranging implications for: Merchants, Issuers, Cardholders and Loyalty Providers

ATPS Asia-Pacific
29th – 31st August 2017
High level impact of new RBA regulations

Merchants

• Lowers acceptance cost for V/MC for most merchants
• Curtails excessive surcharging to the level of the MSF
• Reduces the number of Amex cards in circulation
  >> may reduce merchants accepting Amex
• The differential cost of acceptance between V/MC and Amex is likely to widen
• The new regulations require more detailed MSF reporting by card type
High level impact of new RBA regulations

**Issuers**

- Interchange (or equivalent) revenue reduced for the banks, no change for Amex proprietary or Diners Club
- The Amex companion card programs of the Big 4 become an additional cost for no additional benefit
- Capping interchange at 0.8% reduces revenue on all the premium (and commercial) card portfolios, causing their rewards offers to be devalued
- As holders of reward cards realise the changes to earn rates, they may look around for “better offers”
High level impact of new RBA regulations

*Cardholders*

- Holders of bank issued reward credit cards will have their points earn rates reduced and/or caps lowered
- Amex companion cardholders are most impacted, and premium V/MC less so; no impact on Amex proprietary cards or Diners Club
- High spending points aficionados will notice the change immediately, and attempt to take action / change behaviour to maximise points
- Low spenders and the less engaged may take time to realise the reduction in their reward points earnings (and/or be confused as to what is happening)
- Likely to encounter more surcharging but less minimums at merchants
High level impact of new RBA regulations

Loyalty Providers

- With issuers reducing the points earn rates on their rewards credit cards, less points will be earned into / available to loyalty programs (~$320m reduction)

- The reduction in points earned will impact both Direct and Indirect bank issued credit cards linked to frequent flyer programs

- Amex Membership Rewards will not suffer any changes, and can be expected to communicate this strongly into the market

- Qantas Loyalty has chosen to launch its own credit card (via Citibank) in order to “gain control” - the subsidised economics upsetting its current partners

- The points purchased from all frequent flyer programs by credit card issuers in Australia will reduce by around $250 million per year
Data Protection

European Union –
General Data Protection Regulation (GDPR)
Background

The EU General Data Protection Regulation (GDPR) will go into force on 25 May 2018

Who is impacted?

Every organization — regardless of its location/domicile — doing business with customers within the EU will need to make changes to its oversight, technology, processes, and people to comply with the new rules.

E.g. Non-EU airlines selling tickets to EU citizens

What is the impact?

1. Appointment of data protection officer (DPO)
2. Data breach notifications
3. Privacy-by-design
4. Extraterritorial compliance; and
5. Risk management processes, including a privacy impact assessment (PIA)
# Five Core GDPR Rules

**Establishing the minimum requirements for data protection**

<table>
<thead>
<tr>
<th></th>
<th>Data Protection Officer</th>
<th>Data Breach Notifications</th>
<th>Privacy-by-design</th>
<th>Extraterritorial Compliance</th>
<th>Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The GDPR requires companies to appoint a DPO if they “engage in regular, systematic collection or storage of sensitive customer data.”</td>
<td>The GDPR gives companies 72 hours from the moment they become aware of any data breach for them to report to authorities and affected customers</td>
<td>The GDPR states that firms must consider privacy at the start of any new project and ensure that the right security controls are in place throughout all development phases</td>
<td>The GDPR also requires compliance from non-EU organizations that offer goods or services to EU residents or monitor the behaviour of EU residents, especially online businesses</td>
<td>Organisations must demonstrate that they have implemented appropriate measures to mitigate privacy risks, including a privacy impact assessment (PIA) when appropriate</td>
</tr>
</tbody>
</table>

**ATPS Asia-Pacific**
**29<sup>th</sup> – 31<sup>st</sup> August 2017**
# Moving beyond compliance

## Adopting best practice in data security

1. **Adopt a cost-benefit-based approach to customer data**
   - Organisations need to better assess the costs and benefits of the records they collect. Progressively, this will lead to increased focus on processing, storing, and protecting only the data that offers them the most value.

2. **Using privacy and data security as a source of competitive advantage**
   - Firms are utilising strong privacy policies and data security as a source of competitive advantage, as they realize that customers’ perceptions of privacy strongly affect the quality of customer interactions.

3. **Integrating into internal standards and public commitments**
   - Companies’ security and privacy professionals are designing practices that not only respond to regulatory requirements but are also reflected in their firm’s internal standards, ethics, and public commitments.

Source: Adapted from Forrester Research

ATPS Asia-Pacific
29th – 31st August 2017
Open Data

Productivity Commission Inquiry –
Data Availability and Use
Open Banking Standard and PSD2

Introduction

• The Payment Services Directive 2 (PSD2) was released by the European Commission “to make payments easier, more efficient, and secure to further develop the Single Euro Payments Area (SEPA)”

• This is to be achieved through increased competition by opening the payment markets to new entrants through data sharing and open data for banks (often referred to as simply “open banking”), thus fostering greater efficiency and cost-reduction due to reduced barriers-to-entry

• This resulted in the mandating and creation of standardised APIs enabling access to customer data, for example an individual or business can consent to a third party provider accessing account level data stored with their bank or financial institution

What is an API?

An Application Programming Interface – or API – is a set of functions and protocols that allow access to data or a service. Furthermore, the API can be used to determine what functionality is available, how it must be used and what formats it will accept, whilst maintaining security.

Source: Payments UK
Open Banking Standard and PSD2

Impact on Payments
In the consumer payments space specifically, these changes may have an impact in terms of:

• A shift in payment volumes, away from cards
• An increase in use of 3rd party wallets utilising real-time payments; and
• New approaches to customer security and fraud prevention

• Furthermore, this legislation stipulates that payers have the right to make use of 'Payment Initiation Services', this is where –
  o a third party initiates a payment from a customer's bank account on their behalf; or
  o an 'Account Information Service' can access a customer's account data in order to provide additional tools and services

• Subsequently, Open Banking Working Group in the UK has published the UK Open Banking Standard, which largely mirrors the European directive. The Competition and Markets Authority in the UK has now indicated that banks are required to implement this standard by the end of 2018.
Open Data in Australia

Banks and other FIs resist fintech push for open data regulation

• Productivity Commission's review into ‘data availability and use’ to determine if a system of "open APIs" should occur like the regimes in Europe and Britain

• Driven by Fintech Australia, which initially requested for the commission to recommend that an "open banking API" regime be mandated within 2 years

• However, the calls are being resisted by the nation's banks, which say a compulsory open-data regime would be costly and could raise security issues

• Submissions by CBA, ANZ, Insurance Australia Group and the ASX all urge the government not to mandate open-data sharing >>rather "data-sharing arrangements for private sector datasets should be driven by market forces"
Open Data in Australia

Productivity Commission Recommendations

• Consumers have the right to access & correct their data (a right already conferred by the Privacy Act) and be informed who it has been disclosed to

• Customers have the right to direct one company to give their data to another, e.g. so that an energy provider or insurer can give you a more accurate quote

• However, the recommendations stop far short of recommending the government mandate open data, such as the in the UK and European markets
Summary

Continues to be a focus of Central Bank attention - except USA where V/MC MSF still averaging 2.12%*

Airlines benefit from lower merchant fees, but suffer on lower loyalty point sales

Where surcharging is permitted, Amex can suffer

EU’s GDPR impacts everyone selling to customers in the EU – including non-EU airlines

Data breach notifications within 72hrs, including the impacted customer, may cause brand damage

Security and Data Protection need renewed focus

Regulators want consumers to control the access to their data - providing easier switching to new players

API access to the data you hold on your customers may be mandated

The quality of your offer needs to ensure the customer has no reason to leave

* Nilson Report, May 2017
ATPS Asia-Pacific
29th – 31st August 2017