

# Dual-Network Cards and Mobile Wallet Technology

**Consultation Paper**

**December 2016**

---

## **Contents**

1. Introduction	1
Box A: The entities in mobile payments	2
2. Dual-Network Debit Cards	3
Box B: Dual-network cards and mobile wallets: experience in other jurisdictions	4
3. Mobile Wallet Technology	6
4. Some Emerging Issues	8
5. Consultation and Next Steps	10

© Reserve Bank of Australia 2016. All rights reserved. The contents of this publication shall not be reproduced, sold or distributed without the prior consent of the Reserve Bank of Australia.

ISBN 978-0-9805857-8-0 (Online)

# 1. Introduction

---

Mobile card payments are payments that are made using an electronic representation of a payment card in a mobile phone or other device, as opposed to using the traditional ‘plastic’ form factor. The electronic representation of the card is contained in a ‘mobile wallet’ – an ‘app’ provided either by the cardholder’s financial institution or by a third-party mobile wallet provider. Mobile wallets may also contain electronic representations of other cards and credentials that are typically found in traditional physical wallets.

There is currently significant commercial activity in the mobile payments sphere in Australia involving financial institutions, card schemes and third-party mobile wallet providers. Almost all Australian card-issuing financial institutions have mobile banking apps and in many cases these issuer apps or wallets allow cardholders to make mobile payments using the near-field communication (NFC) or quick response (QR) code functionality of mobile devices to communicate with payment terminals.<sup>1</sup> There are also currently three large third-party mobile wallet providers – Apple Pay, Android Pay and Samsung Pay – which allow mobile payments for customers of particular banks and via particular networks. Mobile payments have so far only been possible via the networks of the international schemes (American Express, MasterCard and Visa). However, eftpos Australia, the domestic debit scheme, is working with issuers and mobile wallet providers and has announced that it expects to launch eftpos as a payment option in mobile wallets in 2017.

Many observers expect that mobile payments will grow very rapidly in coming years. Contactless terminals are now ubiquitous, smartphone penetration is very high and banks as well as the global third-party wallet providers are actively promoting mobile payments. In addition, the use of mobile wallets more generally is likely to accelerate due to various related initiatives that are under way. For example, Transport for NSW is looking to allow customers to use their contactless cards or mobile phones as ‘open loop’ alternatives to the Opal card, while various government entities are looking to issue licences and other credentials on mobile phones.

Against the background of intense interest in mobile payments, some stakeholders have recently raised concerns about possible restrictions on competition in this sphere. This consultation paper deals with some issues that have a bearing on competition between payment networks that are enabled on existing dual-network cards issued by Australian financial institutions (see Box A for an outline of the different entities involved in mobile payments). The paper does not cover the current dispute between some card issuers and third-party mobile wallet providers – this is a separate issue that is being addressed by the ACCC.<sup>2</sup>

---

1 A QR code is a two-dimensional barcode consisting of black squares arranged in a square grid on a white background. It contains information that can be recognised by the cameras on smartphones and other devices.

2 On 29 November, the ACCC announced a draft determination proposing to deny authorisation to the applicant financial institutions. See <http://registers.accc.gov.au/content/index.phtml/itemId/1197444/fromItemId/278039>.

## Box A: The entities in mobile payments

There are a number of different types of entities involved in providing mobile payment services to households. The relevant entities for this paper include:

- **Card issuers:** These are typically banks, credit unions and building societies which provide their customers with debit or credit cards that enable payments through different card networks. American Express is also a card issuer.
- **Card schemes or networks:** These include entities such as eftpos Australia, MasterCard, Visa and American Express which provide services such as processing and authorisation of transactions as well as a set of rules that bind participating card issuers and card acquirers (entities which provide card acceptance services to merchants).
- **Third-party mobile wallet providers:** These are entities such as handset manufacturers, mobile carriers or independent developers which provide mobile wallets that enable payments through a wide range of banks and schemes and may hold other credentials. The major providers include Apple Pay, Samsung Pay and Android Pay.
- **Token service providers (TSPs):** These provide services associated with tokenisation (described below) which enhances the security of card transactions in the mobile or on-line context. The four card schemes referred to above have all established their own TSPs and transactions going through the network of each of those schemes will typically use the relevant scheme's TSP.

## 2. Dual-Network Debit Cards

---

Dual-network debit cards are debit/ATM cards that allow transactions to be routed through two different networks. They incorporate the functionality of two networks in one physical card. For example, dual-network debit cards can route domestic point-of-sale transactions either via the eftpos network (if the cardholder pushes the 'cheque' or 'savings' button) or via the networks of MasterCard or Visa (the 'credit' button). These cards typically have logos of both schemes; often one network on the front of the card and an alternate network or networks on the back.

Traditionally, eftpos transactions accounted for the vast majority of debit transactions in Australia. 'Scheme debit' had a relatively small share of the debit transactions until the early to mid 2000s – Visa Debit was traditionally issued primarily by smaller financial institutions and Debit MasterCard was introduced only in 2005. Scheme debit then experienced strong growth as the four major banks added 'scheme' functionality to their debit cards. This involved switching their standard debit card products from 'proprietary' eftpos/ATM cards (which domestically can access only the eftpos point-of-sale network<sup>3</sup>) to dual-network debit cards (which add access to a scheme debit network for domestic point-of-sale and card-not-present transactions). As part of the migration, the issuer (or bank) identification numbers (IINs or BINs – typically the first six digits in a card number) of the eftpos cards were changed from IINs allocated directly to the issuing bank to IINs issued to the relevant international scheme and then assigned by the scheme to the issuing bank. As of mid-2015, of the 32 million debit-only cards on issue in Australia, 20 million were dual-network and 12 million were proprietary eftpos cards.<sup>4</sup>

While the existence of two networks on the one card is convenient for cardholders and merchants, it raises the possibility of issues involving competition between the competing networks. Such issues first arose in 2010 over data-reporting rules, branding rules, and branding and transaction fees imposed by the international schemes with respect to eftpos. This followed the formation of eftpos as a formal payment scheme in 2009 (prior to this, the eftpos system comprised a series of bilateral arrangements between parties). New disputes arose in 2012, when eftpos was seeking to pilot debit cards with an EMV chip and contactless functionality but reported that it was encountering hurdles from the international schemes regarding its plans for this new functionality.

In August 2012, the Bank's Payments System Board considered a range of issues relating to dual-network cards. It noted that the issues that had arisen between networks had the potential to inhibit competition, limit consumer choice and increase costs. The Board noted that authorities in other jurisdictions had taken measures to address similar issues, and authorised a consultation on the case for regulatory action on dual-network cards. However, rather than proceed immediately to a

---

3 When used overseas, proprietary eftpos cards have access to the Plus, Cirrus or Maestro networks of Visa or MasterCard.

4 This excludes prepaid cards. It also excludes the 5 million 'combo' (eftpos debit and international scheme credit) cards on issue.

consultation, the Board encouraged the parties involved to see if voluntary undertakings could be reached that were acceptable to all parties and also in the public interest.

In August 2013, the Bank issued a media release announcing that the three debit card networks (eftpos, MasterCard and Visa) had agreed to address the Board's concerns. The outcome was intended to safeguard the rights of Australian card-issuing banks and institutions to maintain existing dual-network arrangements in the contactless environment. The three networks made voluntary undertakings to the Bank and committed:

- to work constructively to allow issuers to include applications from two networks on the same card and chip, where issuers wished to do this;
- not to prevent merchants from exercising choice in the networks they accept, in both the contact and contactless environments; and
- not to prevent merchants from exercising their own transaction routing priorities when there are two contactless debit applications on one card.

The Board considered that these voluntary agreements on principles relating to dual-network debit cards were a positive development and, as a consequence, a consultation on a possible regulatory intervention appeared to be unnecessary at that time. However, the Board asked the Bank to maintain liaison with the industry on dual-network card issues and to monitor market developments and technological changes in the industry.

Since the 2013 agreements, eftpos has implemented the eHub, a centralised switch for clearing eftpos transactions, which facilitates technology upgrades in the eftpos system (since participants no longer need to manage multiple bilateral connections). It has also developed chip and contactless functionality (the latter being possible as a result of the undertakings referred to above), and a majority of eftpos issuers are now well advanced in their programs of issuing cards – both proprietary and dual-network – with this functionality. eftpos has added contactless transaction capability to parts of its acquiring network and expects to expand this over the coming months, when the last of its major bank members completes the required development work. It is also working on an 'eftpos online' product, as well as the mobile wallet functionality described in this paper, which it hopes to launch in early 2017 for proprietary and then dual-network cards. However, as outlined in Section 4, eftpos and some issuing banks are reporting obstacles in provisioning dual-network cards for use in mobile wallets.

## **Box B: Dual-network cards and mobile wallets: experience in other jurisdictions**

Dual-network (or 'co-badged') cards have attracted the attention of policymakers in a number of other jurisdictions – most notably the United States, Canada and the European Union, with different policy responses. In each case, however, the response has tended to focus on reducing costs to payments system end-users.

In the United States, Section 1075 of the 2010 Dodd-Frank Act, known as the Durbin Amendment, provided for a number of reforms to the debit card market with the intention of providing more competition in the market. One aspect, which came into effect in April 2012, has the effect of requiring that all debit cards be enabled on at least two unaffiliated networks. Networks must also not restrict or limit an issuer's ability to contract with other networks.

In the European Union, the 2015 regulation on interchange fees makes specific reference to co-badged cards and their role in reducing the cost of payments.<sup>5</sup> The regulation prevents card schemes from having rules that prevent issuers from including payments functionality of two or more networks on one card. It also requires that any scheme rules, routing principles or technical or security standards involving co-badged cards should be objectively justified and non-discriminatory. It specifies that the choice of payment application for transactions using co-badged cards should be made by users, not imposed by card schemes, issuers, acquirers or processing entities.

Individual countries within Europe have different structures with respect to card networks and mobile payments. For example:

- In Denmark, the domestic debit card system is Dankort; there are also co-badged 'Visa Dankort' debit cards. On co-badged cards, domestic transactions are routed via Dankort, while transactions made abroad are routed through the Visa network.
- In France, Carte Bancaire is the domestic (credit and debit) scheme, often co-badged with MasterCard or Visa, with the latter networks used typically for cross-border transactions and Carte Bancaire used for domestic purchases.

In Canada, the Code of Conduct for the Credit and Debit Card Industry in Canada ('the Code') explicitly provides for dual-network cards but takes a different approach.<sup>6</sup> It allows for non-competing, complementary domestic applications from different networks to exist on the same debit card but specifies that competing domestic applications from different networks cannot be offered on the same card. In practice, this means that domestic point-of-sale transactions made on co-branded debit cards are processed through one network, in particular the domestic Interac network, while other applications such as on-line payments and payments at foreign point-of-sale terminals may be processed through the other network on the card. Contactless payments are also processed via Interac ('Interac Flash' transactions). The Code also states that payment card networks must ensure that co-badged debit cards are equally branded. All representations of payment applets in a mobile wallet or mobile device, and the payment card network brands associated with them, must be clearly identifiable and equally prominent. Cardholders in Canada are now able to provision non-competing domestic networks on dual-network cards for mobile use.

Although there is no unifying precedent so far regarding how public policy will evolve regarding mobile payments and dual-network cards, many authorities recognise the benefits of competition among different schemes and have sought to avoid artificial restrictions on competition. A press release from the European Commission in June this year indicates its expectation that dual-network card functionality will be available in both physical and mobile forms.<sup>7</sup> In particular, the Commission noted that under its new interchange fee regulation, consumers will be able to require their bank to co-badge a single card (or in the future their mobile phone) with any card brands that they issue to the consumer.

---

5 See <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0751&from=EN>

6 See <http://www.fcac-acfc.gc.ca/Eng/forIndustry/publications/lawsReg/Pages/CodeofCo-Codedeco.aspx>

7 See [http://europa.eu/rapid/press-release\\_IP-16-2161\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2161_en.htm)

### 3. Mobile Wallet Technology

---

When a customer presents their card details in a mobile payments transaction, they do so from either their financial institution's mobile payments/banking application ('app') or via a third-party mobile wallet. Before the digital representation of a 'card' can be used in an app or wallet, it must be 'provisioned' in that app or wallet. There are two broad ways in which a cardholder can initiate this process:

- via a third-party mobile wallet provider. This method typically requires the cardholder to provide their 15 or 16 digit card number – the primary account number (PAN) – and name. This may involve the cardholder entering his/her card details manually or using the phone's camera to scan the card, with the details recognised by optical character recognition (OCR).
- via an issuer-managed process, typically through an issuer's own mobile wallet or mobile banking app (although this process can potentially also be used to provision a card into a third-party wallet).

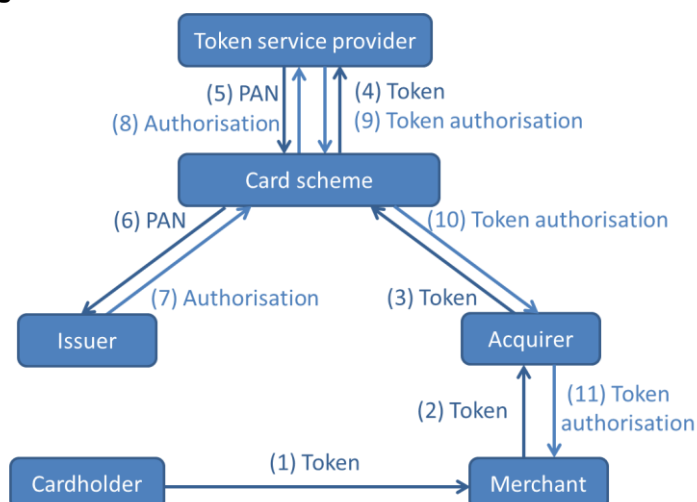
Provisioning a card requires 'tokenisation' of that card, which is a procedure that has been introduced by card networks in recent years to reduce payments fraud. Tokenisation involves de-identifying card details by replacing the PAN with an alternate essentially random number (a 'token'), and storing that number on the cardholder's mobile device. This has two key implications:

- the PAN is no longer part of the message flow in a card transaction. This reduces the risk of it being obtained by fraudsters (especially as there is no longer the risk that a merchant will store a cardholder's PAN)
- the processes of encrypting the card details and decrypting the token information are a required part of the transaction message flow. This involves the use of token service providers (TSPs), with each of the various payment schemes having all set up their TSPs in recent years.

In a tokenised transaction, the token (rather than the PAN) is passed to the merchant's terminal/facility (Figure 1). This token passes with the authorisation request through the acquirer and the scheme to the TSP, which converts the token back to the PAN for the card issuer to authorise the transaction. The authorisation message flows back to the TSP to convert to a 'token authorisation', which is relayed back to the merchant.



**Figure 1: Information Flows in a Tokenised Transaction**



The process of provisioning a token on a mobile device depends on whether the cardholder initiates the process through a third-party wallet provider or an issuer-managed process.

- When a third-party wallet provider is used, the card details are entered into the mobile device and a token request is sent by the mobile wallet provider to the TSP for the relevant network. The TSP then sends a message to the card issuer to seek authorisation for issuing a token. The token is then stored on the user's device.
- When the provisioning of a card is initiated via the issuer's mobile or internet banking app, the cardholder logs in to the app and selects the card (or account) that they would like to provision. The issuer then requests a token to be associated with the card/account. A token is then assigned by the TSP and then linked to the cardholder's mobile device.

The above description of the provisioning process has referred to the process of tokenising a single network. However, equivalent processes can be followed where the card is a dual-network card. In the first case, the mobile wallet provider sends messages to two different TSPs, each contacts the issuer for authorisation, and two tokens are stored on the user's device. In the second case, the issuer can request separate tokens from different TSPs for the two networks that are enabled on the account.

Once tokens for the two networks are issued, the dual-network card can then be shown in the cardholder's mobile device in one of two visual representations:

- As two separate cards in the cardholder's mobile wallet or app, with the cardholder able to choose (possibly on a transaction-by-transaction basis) which will be his/her 'front of wallet' card
- As a single card, with some form of 'button' within the wallet or app that enables the cardholder to set (and reset) his/her default network for that card.

The dual-network card can then enable transactions via either network, with the same effect as occurs when a cardholder dips their physical card in a terminal and uses the terminal buttons ('cheque', 'savings' or 'credit') to choose the network (and in some cases the account).

## 4. Some Emerging Issues

---

With the expected strong growth in mobile payments, it is not surprising that there is strong competition between issuers, schemes and mobile wallet providers in this sphere. However, stakeholders have drawn attention to some specific behaviours that may raise concerns for policy.

In particular, stakeholders report conduct that has sought to prevent or deter Australian issuers of dual-network cards from provisioning those cards to enable eftpos mobile payments. Stakeholders have raised concerns with the Bank about two types of actions:

- Scheme rules or policies of a network that prevent or hinder Australian card issuers from provisioning a competitor network for mobile payments (either expressly or through policies or restrictions that achieve that outcome in practice). In particular, stakeholders have raised concerns that issuers with existing dual-network cards might be prevented from enabling both networks on those cards for mobile payments.
- Contractual terms for tokenisation services that could penalise an Australian issuer for provisioning a competitor network for mobile payments. In particular, stakeholders have raised concerns that contractual terms may allow a scheme to increase the price of tokenisation services for issuers that choose to also enable a network other than that scheme.

Any such actions (and potentially other related conduct) would appear to raise issues relevant for the Payments System Board's mandate under the *Reserve Bank Act 1959* and the *Payment Systems (Regulation) Act 1998* to promote competition and efficiency. They might also raise concerns under competition law.

In considering these matters the Board is guided by its view that competition and efficiency in the payments system are likely to be enhanced where there are a wide range of payment options for consumers and merchants. Mobile wallets represent a technology that allows greater choice by end users. In particular, the physical constraints applied by the size of a traditional wallet or purse – which made the functionality offered by having multiple networks on a single plastic card desirable – no longer apply in the mobile world, where a single device has the potential to store as many cards as the consumer wishes to hold. The Board's longstanding position is that the issuance of physical dual-network cards promotes payments system efficiency and competition between payment methods. Dual-network cards are convenient for consumers and enhance the ability of merchants to encourage the use of lower-cost payment methods. Hence, it would be concerning if, as a new technology is adopted, protocols or rules were put in place that have the effect of reducing competition in the debit card market by making it more difficult for schemes to compete, or impeding the efficient migration of existing competitive arrangements from the physical card to the mobile wallet environments.

Some stakeholders have suggested that it could be in the public interest for the Board to determine a standard that would preclude rules, policies or conduct of any scheme that prevent or make it more difficult and/or costly for issuers to provision a competing network. Before the Board considers the case for such a standard, it wishes to obtain further information and to hear the views of the full range of stakeholders on this issue.

Accordingly, the Board invites stakeholders to make submissions to the Bank that address any or all of the questions below. In addition, it invites stakeholders to provide information on any other matters that are relevant to the issues discussed in this paper.

*Questions for consultation:*

1. What are the views of end-users (cardholders and merchants) regarding dual-network cards, including their use in mobile payments? Are there particular benefits that arise for end-users from having multiple payment networks available on a mobile device? What risks and costs might arise?
2. Are there any impediments or restrictions imposed (or planned or foreshadowed) by card schemes on the mobile wallet provisioning of competing networks on dual-network cards? If so, how significant are these and can they be justified on commercial or other grounds?
3. What are the likely effects – on competition and efficiency in the payments system, as well as more broadly – of the action of any scheme to prevent or discourage the mobile wallet provisioning of a competing network on a dual-network card? Are there benefits for end-users that arise from rules or policies that constrain the provisioning of an additional network on a device?
4. Do cardholders, issuers or others have views as to the feasibility of different possible ways of provisioning dual-network cards?
5. Under the existing voluntary undertakings to the Bank in place since August 2013 (see page 4), schemes have committed to some voluntary principles regarding dual-network cards. Have these principles been an effective response to the competitive issues that arose earlier? Have there been any issues in practice with the operation of these principles? Would an extension of these principles be an appropriate response to the current issues?
6. Are there any foreign precedents that are relevant for the consideration of these issues in Australia?
7. Are the issues raised relevant only to dual-network debit cards or are they also relevant to so-called ‘combo cards’ with credit functionality from one scheme and debit functionality from another?
8. Are there any prospective developments in payment card technology that may be relevant for the Bank as it considers these issues?
9. If the Bank were to contemplate a standard addressing conduct in this area, are there particular compliance costs that would arise for industry?

## 5. Consultation and Next Steps

---

The Board is seeking views from interested parties on this Consultation Paper. Formal written submissions on the questions listed in Chapter 4 or on any related issues, should be provided by no later than 7 February 2017, and should be sent to:

Head of Payments Policy Department  
Reserve Bank of Australia  
GPO Box 3947  
Sydney NSW 2001

or

[pysubmissions@rba.gov.au](mailto:pysubmissions@rba.gov.au).

Submissions provided by email should be in a separate document, in Word or equivalent format. Submissions in PDF format must be accompanied by a version in an accessible format such as .rtf or .doc.

Submissions will be published on the Bank's website, unless the Bank determines that there are reasons not to do so. Where some elements of a submission are considered confidential, respondents are requested to provide two versions of the submission – one for consideration by the Bank and one, with confidential information removed, for publication. In the normal course of events, those making submissions will be provided with an opportunity to discuss their submission with the Bank.

Reserve Bank of Australia  
7 December 2016

### *Privacy*

Unless requested otherwise, published submissions will include contact details and any other personal information contained in those documents. For information about the Bank's collection of personal information and approach to privacy, please refer to the Personal Information Collection Notice for Website Visitors and the Bank's Privacy Policy, which are both available at <http://www.rba.gov.au/privacy>.