RESERVE BANK OF AUSTRALIA

65 Martin Place
Sydney NSW 2000

GPO Box 3947
Sydney NSW 2001

21 May 2021

Committee Secretary
Parliamentary Joint Committee on Corporations and Financial Services
PO Box 6100
Parliament House
Canberra ACT 2600

By Email – corporations.joint@aph.gov.au

Dear Sir/Madam

Inquiry into Mobile payment and digital wallet financial services – Submission

The Reserve Bank of Australia (the Bank) welcomes the opportunity to make this submission, which primarily addresses issues related to the Bank's role as the principal regulator of the payments system. The Bank's mandate in relation to payments is to contribute to promoting a safe, efficient and competitive payments system, consistent with the overall stability of the financial system.

This submission provides an overview of the digital wallet market in Australia, discusses the technologies involved in digital wallets and describes some of the features of the business models adopted by different digital wallet providers. It also outlines some of the potential policy issues relevant to the Bank's mandate in this growing area of the payments system. The strong growth in the use of digital wallets in recent years indicates that consumers increasingly value the ability to make convenient and secure payments with a smartphone or other payments-enabled device. Digital wallets can also help to reduce costs associated with fraud in the payments industry, through innovations such as biometric user authentication and tokenisation. However, digital wallet services may introduce new costs into the payments system and raise new and complex issues for policymakers, particularly in relation to competition and the use of customers' data.

Use of mobile payment and digital wallet services in Australia

Mobile payment services can be facilitated by a range of participants in the payments system including banks, technology companies and other third parties. These services are typically accessed by consumers via a mobile application on a smartphone or other consumer device (such as a smart watch). In Australia, the most prominent mobile payment services are the digital wallets launched in recent years by multinational technology companies for use in their respective mobile platforms. Apple Pay, Google Pay and Samsung Pay are the most widely used digital wallets in the Australian market, with all of Australia's major banks and many smaller card

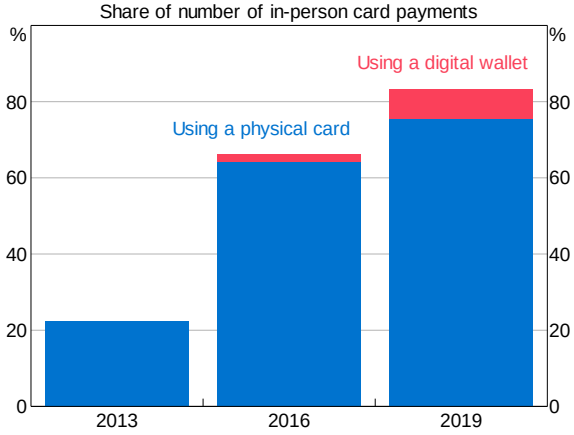
issuers now supporting each of these three wallets.[1] These wallets enable consumers to make contactless (and in some cases online) payments with a smartphone or other consumer device using a digital representation of their debit and/or credit cards.

The available data indicate that the use of digital wallets by consumers to make contactless 'tap and go' payments has increased strongly in recent years. For example, the Bank's 2019 Consumer Payments Survey (CPS) – which was conducted prior to the COVID-19 pandemic – showed that digital wallet transactions accounted for 8 per cent of in-person card transactions in late 2019, compared to 2 per cent when the previous CPS was conducted in late 2016 (Graph 1). The share of contactless payments made via digital wallets is likely to have increased further since the CPS was conducted in late 2019, reflecting the underlying trend towards greater adoption of these services and changes in payment behaviour associated with the COVID-19 pandemic. The pandemic has induced a shift to electronic payments generally and a number of card issuers have indicated that use of digital wallets has continued to grow strongly. More generally, the CPS showed that consumer *awareness* of the ability to make 'tap and go' payments using digital wallets was high (at around 90 per cent of respondents) and around 40 per cent of respondents aged under 40 said they had at least one card stored in a digital wallet.

Graph 1

Contactless Card Payments

Share of number of in-person card payments



Source: RBA calculations, based on data from Colmar Brunton, Ipsos and Roy Morgan Research

Technologies underpinning digital wallets and differences between providers

Mobile payment services can in principle use a range of technologies to facilitate in-person payments but the most commonly used technologies are near-field communication (NFC) and QR codes. In China, QR codes are widely used for consumer payments and involve the consumer or merchant scanning a QR code generated for a particular payment with their device's camera. Most QR-based payments in China are made through the Alipay and WeChat Pay digital wallets, which are associated with technology companies Ant Group and Tencent. Users of these services keep funds in their digital wallet account and payments are made between users in a 'closed

[1] This submission focuses mainly on Apple Pay, Google Pay and Samsung Pay, because they are the most prominent digital wallets in the Australian market. However, a range of other technology companies have also developed digital wallets on their platforms. Consumers can also make contactless payments through the Android applications of some banks (for example CBA and NAB) without the payment being processed by Google Pay or Samsung Pay, though the Bank understands that the vast majority of mobile payments are processed through Apple Pay, Google Pay or Samsung Pay.

loop' on the digital wallet platform, rather than through other payments infrastructure such as card- or account-based payments channels.[2]

In other economies, large technology companies are also the dominant providers of mobile payment and digital wallet services but these services mostly use NFC rather than QR codes. NFC is a wireless technology that allows compatible devices to exchange data over short distances and is based on the same technology standard used for contactless payments using physical (plastic) debit and credit cards, meaning NFC payments can generally be accepted by any card terminal that accepts contactless payments with a plastic card. For this reason, it has been more widely adopted in countries where card payments were already common, such as Australia.

Another key technology that supports the use of NFC for mobile payments is tokenisation. This involves replacing the card number printed on a card, known as the primary account number (PAN), with a randomly generated string of alphanumeric characters. When a customer's request to add a card to their digital wallet is authorised by their card issuer, a token is generated for the customer's card and securely stored on the wallet provider's platform. The token is then used in place of the customer's PAN when a digital wallet transaction is made, with the link between the token and the PAN known only to the token provider (often a card scheme). This can improve the security of digital wallet payments relative to physical cards because digital wallet tokens can be restricted to a particular device or type of transaction, limiting their value if obtained by malicious actors.

Although tokenisation is a common feature across digital wallets, there are technological differences between providers related to how they store customers' tokenised card information on their platforms. These differences may have implications for the security of customer information and the business models adopted by mobile wallet providers.

- Apple stores payment tokens in a hardware *secure element* in Apple Pay-enabled devices, which is analogous to the secure chip in contactless payment cards. During a contactless transaction, the secure element can only be accessed by the device's embedded NFC controller, which is designed to ensure that sensitive payment information cannot be intercepted by other applications. In addition, only Apple's 'Wallet' application can write payment credentials to the secure element. This means that Apple Pay is the only digital wallet that is currently supported on Apple devices such as iPhones.
- In contrast, Google uses a cloud-based technology called *host card emulation* (HCE) to store payment credentials for Google Pay. Google adopted this technology because many Android devices, which are often manufactured by third parties, do not have a hardware secure element. HCE stores payment tokens in a cloud server, periodically downloading them to the device to enable payment without a connection to the internet. As sensitive card information is transferred over the internet and not stored in a hardware secure element, HCE implements additional security features to provide a similar level of security.[3] One difference with Apple's iOS platform is that the Android operating system allows third parties to use its HCE functionality to develop their own NFC-based mobile wallets for Android.
- Samsung Pay uses a third method that involves storing payment credentials in a secure area of the device's main processor, isolated from the mobile operating system, known as a

[2] QR-based technologies have so far not been used on a large scale for consumer payments in Australia. The Bank surveyed Australian consumers about use and awareness of Alipay and WeChat Pay in its 2019 CPS, which showed that a very low share of consumers had used these services. Use of Alipay and WeChat Pay in Australia is likely concentrated among tourist and expat groups.

[3] These features include 'limited use keys' and 'white box cryptography'. Limited use keys are payment tokens downloaded to the device that can only be used for a limited set of transactions. White box cryptography is a technique that obfuscates the location of the payment credentials in the device operating system.

trusted execution environment (TEE). This can be considered a hybrid hardware and software solution.

Another technology often deployed by digital wallet providers is biometric user authentication. This uses the fingerprint or facial recognition technology in mobile devices to verify that the owner of the device is initiating a given transaction. The three major digital wallets differ somewhat in their authentication requirements. Apple Pay and Samsung Pay both require biometric or PIN authentication for every transaction, whereas Google Pay allows a limited number of low-value payments to be made without transaction-based authentication.

Business models of digital wallet providers

Platform rules

Digital wallet providers are generally platform businesses that facilitate interaction between different parts of their networks. For digital wallet services, this network includes card issuers, cardholders that use digital wallets and merchants that accept digital wallet payments. The nature of platform businesses is that they are able to set the rules of participation in their platform or network. In relation to digital wallets, platforms may establish rules related to third-party access, the collection of payments data and fees paid by network participants.

As noted in the previous section, a notable difference between the Android and iOS platforms concerns the ability of third parties to access technology used for contactless payments (such as NFC). On Android devices, third parties are able to directly leverage NFC functionality to develop their own mobile payment applications that compete with Google Pay or Samsung Pay; that is, a user can initiate a payment from their bank's app without the involvement of the technology company's mobile wallet. In contrast, on the iPhone, direct access to NFC technology for payments is restricted to Apple's 'Wallet' application, meaning third parties are unable to develop their own mobile payments applications for iOS without transactions going via Apple Pay. Some stakeholders have argued that this could limit the ability of other wallet providers to compete on these devices and that this could increase costs in the payments system (see below).

Another important distinction between different digital wallets relates to the use and value of information and data. Google Pay and Apple Pay have again taken different approaches in relation to customers' data. Google states that it may collect information on transactions made using Google Pay, which can be used as part of providing or marketing other Google services to users. In contrast, Apple states that it does not collect transaction information that can be tied back to an individual Apple Pay user. The two platforms also take different approaches to charging transaction fees. Apple charges a per-transaction fee to card issuers when an Apple Pay transaction is made but a similar fee is not charged by Google when transactions are made with Google Pay. It is possible that there could be a link between the different approaches that Google and Apple take to the use of data on the one hand and access and fees on the other.

Commercial arrangements

Digital wallet providers may have commercial relationships with a range of different participants in the payments system, including card issuers, merchants and consumers. As discussed below, the size and global reach of digital wallet providers, which include large global technology companies, is likely to result in them being in a strong position when it comes to negotiating terms with other participants in the payments system.

Card issuers enter into commercial agreements with digital wallet providers that enable them to provide digital wallet services to their customers. The Bank is not privy to the details of these agreements but is aware that they can contain clauses that stipulate rules in relation to the use of the provider's platform (for example, relating to transaction fees and data collection).

Merchants seeking to accept digital wallet payments may have commercial obligations to wallet providers in some cases. Brick-and-mortar merchants that accept contactless payments are typically not required to enter into a specific agreement to accept digital wallet payments. However, online merchants that integrate wallet providers' checkout 'buttons' on their websites or in their apps may be required to share some transaction-related data as part of the terms of their agreement with the provider. Consumers also accept various terms of use from their wallet provider or card issuer when they provision a card in a digital wallet. These terms may include clauses related to data sharing between the card issuer and wallet provider, and some digital wallet providers may seek to commercialise customers' data. For example, in some countries, Google uses transaction data to serve targeted offers to customers through Google Pay.

As part of the Bank's current Review of Retail Payments Regulation, stakeholders raised a number of issues in relation to platform rules and terms in commercial agreements between issuers and digital wallet providers. A particular concern for some stakeholders was that certain rules – for example in relation to access to NFC functionality – could limit competition in the provision of mobile payments to consumers. On the other hand, some stakeholders noted that controlling access to NFC functionality could have benefits in terms of security and privacy of consumers' payments.

Policy considerations

The expansion of large technology platforms – sometimes referred to as 'bigtechs' – into payments and other financial services markets is presenting new competition challenges for policymakers and regulators. These platforms have very large user bases and benefit from strong network effects, which is likely to result in them being in a strong negotiation position with payments system participants and can make it difficult for smaller firms to compete. While technology platforms have the potential to improve the efficiency and security of the payments system by providing innovative new services, they can also introduce new direct and indirect costs. Accordingly, it will be important for policymakers to assess whether there is an appropriate balance between the costs and benefits of these services. As digital wallets become more widely used, wallet providers could obtain substantial market power and this could have implications for competition and efficiency in the payments system.

A specific issue attracting growing international regulatory scrutiny is the ability of digital wallet providers to control access to technologies (such as NFC) used for payments on their platforms. The European Commission is currently conducting a formal antitrust investigation into a number of Apple's practices in relation to Apple Pay including its limitation of access to the NFC technology for payments on the iPhone; it is also considering legislation that would ensure third parties could access technologies used for payments on fair and reasonable terms. German, Swiss and Dutch national authorities have also considered, or are considering, access issues related to NFC. Increased attention related to access issues on mobile devices highlights some of the complex competition issues posed by multinational technology companies. While on the one hand, these issues can appear to be limited to particular services (such as contactless payments), global policymakers are also increasingly recognising that specific issues need to be considered within the context of these companies' broader platforms. For example, fees or data from particular services may cross-subsidise or support other services, which could have broader competition implications.

In Australia, the ACCC denied an application by four Australian banks (including three of the major banks) for authorisation to collectively bargain with Apple over access to the iPhone's NFC controller in 2017, on the basis that granting such authorisation to the banks was not likely to result in a net public benefit. One potential detriment was the potential to distort competition in the mobile payments market, which was in its infancy in 2017. However, the market has since matured significantly and Apple Pay provision is now nearly ubiquitous among issuers (including all of the banks party to the ACCC application).

The Bank has considered issues related to third-party access during the ongoing 2020/21 Review of Retail Payments Regulation and does not see a case for regulatory action at present. However, if the recent strong growth in the use of digital wallets continues, a case for further scrutiny could emerge as digital wallets become a more prominent part of the retail payments landscape. Accordingly, the Bank will continue to closely monitor developments in Australia and overseas.

Another issue that may warrant further consideration is that there is a lack of transparency in relation to the fees and other arrangements associated with digital wallets. As part of the current Review of Retail Payments Regulation, the Bank is consulting on a number of initiatives to improve transparency in the payments system – for example, a requirement that card schemes provide the Bank with access to their fee schedules and scheme rules. One of the aims of these initiatives would be to discourage any changes to fees and rules that may be anti-competitive. It is possible that improving transparency related to fees and rules in the digital wallet market could similarly allow policymakers to identify potential competition issues, and generally provide better information about the functioning of the market. However, the Bank recognises that some elements of these fees and rules may be commercially sensitive (as is also the case for card schemes). Accordingly, any effort to improve transparency would need to adopt a consistent approach and be balanced against commercial considerations.

As Australian policymakers and regulators consider policy issues involving digital wallets and other newer participants in the payments system, it will be important that they have appropriate powers and that regulatory frameworks remain 'fit for purpose'. In the case of the payments system, the Bank's submission to the Treasury Payments System Review noted the significant technological changes that have occurred since the current regulatory framework was introduced two decades ago. The Bank noted that there may be scope to clarify how newer participants in the payments ecosystem (including digital wallet providers) should be treated under the *Payment Systems (Regulation) Act 1998* (PSRA). The Bank believes there is merit in establishing arrangements that would allow all entities that play a material role in facilitating payments to be regulated where doing so would promote competition and efficiency and control risk. One option here would be to consider amendments to the PSRA that would confer appropriate powers to ensure that these entities can be the subject of regulation under the PSRA where that is in the public interest.

The Bank would be happy to discuss any of the issues raised in this submission further with the Inquiry.

Yours sincerely

Tony Richards
Head of Payments Policy
Payments Policy Department