PSR Payment Systems Regulator

Contactless mobile payments

A PSR report

July 2018

Contents

1 Executive summary

1.1 The recent rapid growth in the UK of contactless mobile payments (CMPs) means they are becoming an increasingly important means of payment with the potential to change the way we make everyday purchases. We therefore need to have an up-to-date understanding of this sector – in particular, of any potential issues that could have a detrimental effect on the PSR's statutory objectives of innovation, competition and interests of people and organisations that use payment systems.

Contactless mobile payments

1.2 CMPs are in-store payments that consumers make by using apps installed on their mobile devices. In the UK, the CMP apps that are currently available – Amex Pay, Apple Pay, Barclays Contactless Mobile, Google Pay and Samsung Pay – allow consumers to upload their card details onto the app to make payments from those devices.

1.3 From a technical point of view, when a consumer wants to use a CMP app to make a payment, the app has to communicate with a retailer's point-of-sale (POS) system.[1] In the UK, the large majority of CMPs initiated through mobile devices use near-field communication (NFC) technology.[2] This requires the mobile device to have what is called an 'NFC antenna', enabling contactless services. To the retailer's POS terminal, a transaction with a CMP app is the same as a contactless card transaction. The CMP app communicates with the NFC antenna on the user's device to send the payment information to the retailer's POS terminal.

1.4 A key difference between CMPs and contactless card payments is the information communicated between the consumer and the retailer's POS terminal. In a contactless card payment, the consumer-related information transmitted includes the payment card's Primary Account Number (PAN[3]). In CMPs, the mobile device transmits a replacement number, created through a process known as 'tokenisation'. Tokenisation replaces the PAN with a 'device primary account number' (also called a 'digital primary account number') known as a DPAN or 'token'. This is intended to reduce the risk of the consumer's payment details being stolen electronically during a CMP. It is possible to use a PAN obtained fraudulently but not a DPAN.

1 A POS system is the hardware and software used to record a retail financial transaction. In this case, it could be an electronic cash register (in a shop) or an integrated computer system (in a transport environment), also equipped with a card reader.
2 See also paragraph 3.12.
3 This is the long number usually printed across the middle of a payment card.

Our work

1.5 To better understand the CMP sector in the UK, we undertook a call for information exercise in 2016 and 2017. Over two rounds of requests for information (RFIs), we engaged with a variety of stakeholders involved at different levels in the provision of CMPs.[4] We were particularly interested in understanding:

- whether competition, innovation and the interests of people and organisations that use payment systems could potentially be affected by the way CMPs operate and are being offered in the UK, and if so how
- whether there were any restrictions affecting the provision of tokenisation services

1.6 As mentioned in paragraph 1.3, CMPs in the UK currently rely largely on NFC technology for communication between the mobile device and the retailer's POS terminal. There are many mobile devices that have an NFC antenna embedded, which allow developers of CMP apps unrestricted access to the NFC antenna. However, on Apple devices (which run on Apple's iOS operating system), only the CMP app offered by Apple – Apple Pay – has access to the NFC antenna in a way that can be used to make CMPs. Other mobile devices that use the Android operating system (for example, those made by Google and Samsung) do not restrict access to the NFC antenna by a particular CMP app. Some card issuers[5] contended that the restriction on access to the NFC antenna on Apple devices prevents the use of non-Apple CMPs on these devices, thereby limiting innovation and competition.

Issues we considered

1.7 We sought to understand the nature of Apple's restriction on access to the NFC antenna on Apple devices and its potential impact on our objectives. In particular, we looked at whether any substantial innovations were likely to be hampered by this restriction. We asked stakeholders about the effect of Apple's restriction on access to the NFC antenna, and what they would do if the NFC antenna on Apple devices were made accessible to other CMP apps. Some card issuers argued that, in general, the restriction had a negative impact on competition and innovation, although they did not identify specific examples of how such innovation or competition was being hampered.

1.8 The tokenisation process for CMPs in the UK generally occurs in accordance with the industry standard known as the 'EMV specification'. This is the main global standard for tokenisation services. The EMV specification was developed by EMVCo, a limited liability company owned by six of the major card schemes.[6] We considered how the EMV specification was developed. Specifically, we considered whether card issuers had to use particular token service providers (TSPs), and whether there was any restriction on non-card-scheme TSPs to develop and offer tokenisation services.

4 These included CMP app developers, token service providers, payment card issuers, technology companies, mobile network operators, card scheme operators and a tokenisation standards body.
5 A card issuer is usually a consumer's bank or credit card supplier.
6 American Express, Discover, JCB, Mastercard, UnionPay and Visa, each of which has 1/6 ownership.

1.9 We were told that some CMP app developers require other parties to use tokenisation services compliant with the EMV specification. However, the main providers of tokenisation services (the three major UK card network operators) all offer tokenisation services that are compliant with the EMV specification. According to one card issuer, the existence of the common standard on a global scale has had a positive effect on the development and uptake of CMPs in the UK. We were not made aware of any examples of market entry being prevented for tokenisation services due to the EMV specification. We are aware of a party, not a part-owner of EMVCo, that has developed its own tokenisation service. In general, no major concerns were raised with us relating to tokenisation services.

Concluding remarks

1.10 While CMPs currently represent a relatively small percentage of transactions compared with alternative payment methods, their use is growing rapidly and the development of CMP as an alternative payment method has the potential to benefit both participants and end users in payment systems. Respondents to our RFIs told us that CMP apps can create real benefits for consumers, retailers and card issuers.

1.11 For all end users of CMP apps to be able to take full advantage of the current and future benefits of this payment method, it is important that efficient competition and innovation in the markets concerned be maintained. We have considered a range of issues raised with us. However, we have not been told of any prevented innovation or practices in tokenisation service provision that would require an in-depth assessment of the issues at this point. Nonetheless, we are aware that CMPs, while still a relatively new development, are a fast-developing feature of the payments sector. We will therefore continue to keep the sector under observation, retaining the option to investigate and to act as we believe necessary to address any problems we may identify or that may be brought to our attention in the future.

2 Introduction

Developments in card payments

2.1 In the UK, payment cards have experienced constant and sustained growth since their introduction[7], and debit cards recently overtook cash as the most popular form of payment.

2.2 As the use of payment cards for purchases has grown, so has that of card-based contactless methods of payment.[8] According to UK Finance, contactless accounted for 38% of all in-store card payments in October 2017 (up from 24% in October 2016).[9]

2.3 Technology developments are affecting every aspect of our daily lives, including the way we pay. For example, users are now able to pay for goods and services quickly and easily using mobile devices, such as mobile phones or tablets. Payments using mobile devices have also increased greatly in the past few years.

2.4 Payments through mobile devices can be made through a website (online payments), within an app on the device itself (in-app payments) or, more recently, by using contactless payment technology (in-store payments at a point of sale).[10] All three types of mobile payment are usually based on the consumer's payment card – whether credit or debit – using the relevant card network to complete the transaction.

2.5 Contactless mobile payments (CMPs), as currently available in the UK, are a type of contactless debit or credit card payment, initiated using a mobile device for in-store payments. The latest mobile devices contain an antenna that enables CMPs to be made in-store using near-field communication (NFC) technology, which uses the existing network of contactless terminals that currently serve contactless card payments. CMP solutions have emerged in the UK market to take advantage of NFC functionality. At present, all CMP apps in the UK use consumers' credit or debit cards (i.e. cards issued under the Visa, Mastercard and American Express schemes). When a consumer authorises an in-store transaction, the app releases payment information to the retailer's POS terminal via the NFC antenna, which then travels through the card network system, in the same way as when a consumer pays with a physical card.

7 Credit cards were introduced to the UK in 1966, and debit cards in 1987.
8 Contactless payment cards were introduced to the UK in 2007.
9 www.ukfinance.org.uk/wp-content/uploads/2017/12/Card-Expenditure-Statistics-October-2017.pdf
10 The first contactless mobile phone payment functionality was introduced by Orange and Barclaycard in 2007.

2.6 The recent rapid growth of CMPs in the UK has been driven by their increasing adoption by consumers, by more NFC-enabled POS terminals, and by the move in 2015 from £20 to £30 as an upper limit on contactless payments.[11] Growth in the number of CMPs is likely to continue as more users, handset manufacturers and retailers adopt the technology. Further broadening of CMP functionality is also possible. For example, major CMP apps may also begin to use interbank payment systems[12] in addition to, or instead of, cards.

Why consider CMPs?

2.7 The growth in CMPs means they have the potential to represent a sizeable part of all UK payments in the near future and thereby have an impact on all three of the PSR's statutory objectives.[13] We therefore wished to have an up-to-date understanding of this sector, in particular with a view to identifying any potential issues that could have a detrimental effect on innovation, competition and interests of service-users.

2.8 This report reflects our current understanding of the CMP sector in the UK, following the request for information exercise that was launched in 2016 in pursuit of our objectives.

2.9 There were two areas we were especially interested in:

- Access to the NFC antenna in mobile devices: We sought to understand the nature of Apple's restriction and its potential impact on our objectives. In particular, we looked at whether there were any substantial innovations likely to be hampered by the restriction on access to the NFC antenna on Apple devices.
- The existence of the EMV specification for tokenisation services: We looked at how the EMV specification had been developed. Specifically, we considered whether card issuers had to use particular providers of tokenisation services, and whether there was any restriction on non-card-scheme token service providers (TSPs) to develop and offer such services.

The information-gathering process

2.10 To better understand the CMP sector in the UK, we undertook a request for information (RFI) exercise, engaging with a total of 18 stakeholders from the following groups:

- Card issuers
- Card network operators
- CMP app providers
- Mobile device operating system (OS) developers
- Non-payment service provider market participants (e.g. mobile operators)
- Associated technology companies, including industry standards associations

11 In addition, CMP apps can now be used for payments above £30, if further verified (for example, by code or fingerprint) and accepted by the retailer.
12 Interbank payment systems allow payments to be made between bank accounts – for example, Faster Payments, Bacs and CHAPS. While contactless apps using interbank systems have yet to take off in the UK, we believe they are established in other countries.
13 The PSR's statutory objectives are contained in sections 50 to 52 of the Financial Services (Banking Reform) Act 2013 (FSBRA).

2.11 We issued two rounds of RFIs using our information-gathering powers under the Financial Services (Banking Reform) Act 2013 (FSBRA).[14] The first round, undertaken in autumn 2016, was designed to give us a better understanding of topics such as who the main players are, what services are on offer, what mobile devices are used, usage data, the role of tokenisation services, and the contractual arrangements in place for the provision of CMPs. We wanted to understand the sector, its incentives and the various consumer offerings available, and to consider whether there might be any issues that could have an impact on competition, innovation or the interests of service-users.

2.12 In our second RFI, undertaken in summer 2017, we focused mainly on two areas: access to the NFC contactless antenna on mobile devices and the use of industry standards in tokenisation services. We also held follow-up meetings with several stakeholders.

2.13 We summarise the results of our call for information exercise in this report. The next chapter explains what CMPs are (in particular, how they work from a functional and technical perspective, who the main participants are and what their respective roles are). Chapter 4 outlines our consideration of the particular areas we were interested in. Chapter 5 sets out our concluding remarks and proposals for next steps.

14 Under section 81 FSBRA, we have the power to require a person to provide information and documents that we need to exercise our statutory functions.

3 What are contactless mobile payments?

3.1 In this chapter, we explain what contactless mobile payments (CMPs) are, their technological features, how they work and the parties involved in delivering the service.

3.2 We start by explaining the technological elements of a CMP, then describe the key parties offering the different services that together effect a CMP, as well as how information is exchanged between them. We then focus on CMP apps: how they store and communicate information securely, and how their features vary across different suppliers.

3.3 We then look at a key difference between CMPs and other card payments – the tokenisation of payment details. We describe how tokenisation works, how payment cards are tokenised, and the information flows involved in tokenised transactions. Then we describe the added security to payments that stakeholders consider tokenisation brings about. We also look at how the use of these apps currently fits into the broader landscape of different payment types, and at the incentives for the different parties involved in providing CMP services. We conclude this chapter with the benefits of CMP apps to consumers, retailers and card issuers, and a reference to CMP usage (current and future).

CMP services and how they work

3.4 Mobile payments are those for which the payment data and the payment instruction are initiated, transmitted or confirmed via mobile devices. These payments can be made online, in-app or in-store for purchases of services or goods. There are therefore two broad categories of mobile payments: remote payments at virtual points of sale, which take place through the internet (e.g. online or via apps on devices); and proximity payments, which take place directly at a physical point of sale.

3.5 CMPs are proximity payments requiring specifically equipped mobile devices that interact with a corresponding terminal at the point of sale (e.g. in shops or on public transport). These payments are initiated by consumers using apps that allow their mobile devices to communicate with a retailer's POS system using the device's hardware. In this way, payment data can be exchanged between the parties involved in the transaction (payee and payer, or retailer and consumer). The retailer's point-of-sale (POS) terminal interprets a transaction with a CMP app as a contactless card transaction. The app communicates with the POS terminal via near-field communication (NFC) technology, which is currently the predominant technology for contactless card payments in the UK. The CMP app will need to communicate with the device's NFC antenna in order to transmit the payment information to the retailer's POS terminal.

3.6 Although it is possible that in the future CMPs will use interbank systems, the CMP services currently available in the UK use debit and credit cards only. Therefore, this report focuses on card-based CMPs. Card-based CMP apps in the UK connect with card payment schemes. The transaction is processed through a card scheme and the payment is completed to the retailer through an acquirer (see below). From a processing and settlement point of view, there is no difference between CMP transactions and those conducted through plastic cards. While the payment instruction is initiated from a mobile device, a CMP nonetheless uses the consumer's card information to make the transaction (in the form of a tokenised proxy, discussed in further detail below). The consumer's mobile device sends the tokenised card information to the retailer's card terminal and through the card payment system where it is processed. To understand the systems underpinning CMPs, it is therefore helpful to look first at card payments.

3.7 To offer card-based CMPs, CMP app developers (such as Apple or Google) must secure participation from card schemes (such as Visa or Mastercard) and card issuers. They must also encourage consumers to download the CMP app (if not already pre-installed), add their cards to the app and initiate transactions using the app.

3.8 A plastic card payment transaction involves a number of parties. A card payment scheme has two basic configurations: four-party schemes (such as VISA or Mastercard), which have a consumer (sometimes known as a 'cardholder'), a card issuer, an acquirer and a retailer (also known as a 'merchant'); and three-party schemes (such as American Express), which have a consumer, a card issuer/acquirer (i.e. a single organisation acting as both) and a retailer:

- **Consumers** use cards to make payments.
- **Card issuers** provide consumers with payment cards.
- **Acquirers** are the banks that contract with retailers to accept and process card payments.
- **Retailers** are the trader or service providers that accept card payments from consumers.

3.9 The underlying method of processing and settlement of a payment transaction is the same for CMPs as for transactions initiated with plastic cards. As with transactions made through plastic cards, CMP transactions are subject to the rules of the relevant card scheme as payment messages are transferred from one party to the other using the card scheme's infrastructure.

3.10 The only difference between a plastic card payment (whether contactless or not) and a CMP is in the type of information that is sent from the buyer's payment device to the retailer. More precisely, in contrast to contactless payments made using plastic cards (which release the Primary Account Number (PAN[15]) to the retailer's terminal), the payment information transmitted by CMP apps is a Device Primary Account Number (DPAN), or token. We describe the processes for creating and using this token later in this chapter.

15 The long number usually printed across the middle of a payment card.

3.11 As with contactless cards, when a consumer wishes to initiate a POS transaction using their mobile device (e.g. to pay a restaurant bill), the retailer's POS terminal must be able to communicate with that device. To date, the large majority of CMPs initiated through mobile devices use near-field communication (NFC) technology to transmit the relevant information. Likewise, a large number of retailer terminals in the UK are NFC-enabled.[16]

3.12 As noted in paragraphs 3.24 to 3.37, there are several other technologies currently available that may be used to effect CMPs. These include QR Codes, as used in the apps offered by Tesco and Starbucks. However, as we also point out below, these apps are store-specific and cannot be used at other retailers. The five NFC-based apps are all usable with any retailer with a contactless card terminal, and it is for this reason that we concentrate on these apps in this report.

3.13 In the responses to our requests for information (RFIs), many stakeholders regarded the wide prevalence of NFC in retailer terminals as giving that technology a clear advantage over alternative technologies for CMPs. Other factors in favour of NFC, according to several stakeholders, included the speed and ease of payment for the consumer and what was seen as superior security (e.g. compared with Bluetooth). We discuss the alternative technologies for CMPs in further detail below.

Principal roles in CMPs

Key consumer hardware and software for CMPs based on NFC technology

3.14 To recap, in order to make CMPs, users need a contactless-enabled device which, using contactless technology, communicates payment information from the device to a retailer's POS terminal. In the UK, that contactless technology is generally NFC.

16 According to UK Finance, the number of bank-owned NFC retailer terminals grew by 28% between June 2016 and June 2017. www.ukfinance.org.uk/statistics/cards

3.15 From the responses to our RFIs, the following are the essential hardware and software components that a mobile device needs to perform CMPs:

- **A CMP app:** These apps provide the user interface for CMP services, and facilitate the storage and transmission of payment information.
- **An NFC antenna:** The NFC antenna facilitates communication between the CMP app and the retailer's POS terminal.
- **Secure storage:** It is key to the security of CMPs that payment data can be stored securely, either on the mobile device itself or remotely, within the systems of the app provider, as follows:
  i. **Secure element:** This is a chip used to store sensitive data on a mobile device. The secure element may be embedded in the device (e.g. for Samsung Pay and Apple Pay) or the SIM card (e.g. for the recently closed Vodafone Pay). The secure element stores the tokens representing the consumer's card details registered with the CMP app. It also holds dynamic cryptograms that accompany the tokens to verify them as having come from the consumer's device (see paragraphs 3.56 to 3.61).

  ii. **Host Card Emulation (HCE):** Under this configuration, the CMP app supplier stores the sensitive information (i.e. tokens and cryptograms) remotely on secure servers in host or 'cloud' databases (e.g. for Google Pay). The CMP app uses the mobile device's data connection to the internet to access this information and draw it down onto the device as needed.
- **An operating system (OS):** This enables the mobile device to function, and handles the processing of apps loaded onto it. CMP apps that do not use a secure element for CMP services, such as Google Pay, use the device's OS and cloud-based technology (HCE) to store and send tokens and dynamic cryptograms.

Mobile device manufacturers

3.16 CMPs require a mobile device to contain, or be connected to, a contactless radio antenna capable of communicating with a retailer's POS terminal using NFC or similar technology. Mobile device manufacturers decide whether or not to include such an antenna in their models, and they seem to have the ability to control how apps on the device can access the antenna. Our understanding is that most recent mobile phone devices have an NFC antenna embedded.

Mobile device operating system developers

3.17 Mobile devices come with a pre-installed OS that enables the phone to function. In some cases (e.g. Apple and Google phones) the device manufacturer also develops the OS. In other instances (e.g. Samsung phones), the OS is developed by a third party, although it may be customised by the device manufacturer. The developer may exercise control both over which apps may be used on the device and the extent of the functionality offered to those apps (including the extent to which the apps are able to access and control the device's various hardware elements, including the NFC antenna). The OS pre-installed on the device will usually contain a number of apps including, increasingly, a form of CMP app.

CMP app developers

3.18 CMP apps can be provided by an array of developers, including card issuers (e.g. Barclays), OS developers (e.g. in the case of Google Pay), card scheme operators (e.g. Amex Pay), device manufacturers (e.g. in the case of Samsung Pay), mobile network operators (e.g. in the case of Vodafone Pay[17]) or, potentially, third-party app developers.[18]

Token service providers

3.19 As noted in paragraph 1.4, a key difference between CMPs and payments made by other means (e.g. contactless plastic cards) is the information communicated between the buyer and the retailer's POS terminal. In CMPs, rather than a card's PAN, a mobile device transmits 'tokenised' payment information to the POS terminal (i.e. a DPAN, or payment token). The main role of token service providers (TSPs) is to replace a PAN provided by a buyer's card issuer with a payment token.

3.20 The responses to our RFIs indicated that the three main card schemes operating in the UK – Visa, Mastercard and American Express – are also the principal TSPs to UK card issuers offering CMPs, and that they provide token services in accordance with the EMV tokenisation standard. We were told that one UK card issuer provides tokenisation services for contactless payments made with its own app. Card issuers can also offer TSP services to other parties.

CMP apps

3.21 CMPs are made by consumers through apps that allow their card issuers to send and receive payment information using their devices. As well as being a user interface for consumers, a CMP app facilitates the storage and transmission of the DPAN or payment token provided by the card issuer's TSP (see paragraphs 3.56 to 3.61). In order to do this, a CMP app must be downloadable onto the device, able to communicate with the device's OS and to do so using the same technology by which the device sends the payment information (for almost all CMPs, this is the NFC antenna). Consumers may buy CMP apps – or download them free – and install them on their mobile devices. Some devices may have CMP apps pre-installed before sale.

17 Vodafone was the only mobile network operator offering its own CMP app in the UK after EE ceased support for its 'Cash on Tap' service in 2015. However, Vodafone Pay also closed on 28 June 2018.

18 There could be an expansion of third-party account and payment services offered following the implementation of the revised Payment Services Directive, which is designed to encourage new third-party players in payments markets, such as Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

3.22 CMP apps vary in three basic ways:

- **Acceptance:** This refers to where an app can be used to make payments – whether in almost any shop or in specific shops only. Apple Pay, Google Pay, Samsung Pay and Amex Pay all offer general purpose apps that can be used to pay any retailer accepting contactless payments, whereas retailers such as Tesco and Starbucks offer specific apps that can only be used within their own outlets.
- **Funding:** In the UK, CMP apps have two main funding methods. Some apps, such as Google Pay, Apple Pay and Samsung Pay, can be linked to any payment card (i.e. any card issuer and network). Other apps, such as the Barclays Contactless Mobile App, are limited to cards issued by a specific bank – in Barclays' case, any UK credit or debit card that it has issued.
- **Pass-through or staged wallets:** Some CMP apps are referred to as 'pass-through digital wallets' and others as 'staged digital wallets':

  i. A pass-through digital wallet is an app that enables payment directly from a single payment system, such as a credit or debit card. At the appropriate time, the consumer selects one of the 'stored' payment methods to finalise payment to the retailer. Google Pay, Apple Pay and Samsung Pay are examples of pass-through wallets.

  ii. In a staged digital wallet, payment from a consumer to a retailer has two distinct stages. First, on the funding leg, money is drawn down from the consumer's credit or debit card (or from a line of credit from the staged wallet provider) and used to 'top up' an account (the wallet) so that payments can be made. This is done independently of the retail payment stage. When a payment is to be made (the second leg) the app moves funds from the wallet to the retailer to complete the purchase. The app manages both the drawing down of the top-up money and the dispensing of it to make purchases, allowing users to monitor their spending. bPay (from Barclays) is an example of a staged digital wallet.

3.23 As stated earlier, a CMP app does three things to enable CMPs through a mobile device:

- It communicates the payment information to a retailer's terminal.
- It provides a user interface for the CMP service.
- It facilitates the storage of payment information.

We will discuss each of these in turn.

Technologies used to communicate CMP payment information

3.24 To make a CMP, the consumer's mobile device must communicate with the retailer's POS terminal. We now look at the technologies that respondents to our RFIs identified as allowing mobile devices to exchange information with POS terminals.

3.25 There are several technologies currently available that may be used to effect CMPs. They include NFC, Magnetic Secure Transmission (MST) and Bluetooth Low Energy (BLE). While contactless communication technologies are necessary for CMPs, they are not exclusive to contactless-enabled mobile devices and may also be used for other payment methods such as contactless payment cards.

Near-field communication

3.26 **NFC** is an agreed messaging standard for communication using radio-frequency electromagnetic waves to exchange information (without contact). Apart from mobile devices, NFC technology is also used for contactless plastic cards, wearable fobs and stickers.[19] Some of these external devices (e.g. Barclays' bPay products) have an embedded passive NFC chip, enabling the device to provide the same functionality as a contactless prepaid card.[20] Alternatively, external devices may be fully functioning extensions of an on-device CMP app, with real-time information and tokenised payments (such as Apple Watch or Samsung Gear).

3.27 Devices using NFC may be active or passive. A passive device, such as the NFC chip in a contactless card, contains information that other devices can read but it does not read any information itself. Active devices can both read and send information. An active NFC device, such as a smartphone, can not only collect information from NFC chips but can also exchange information with other compatible phones or devices. Most importantly from a mobile payments viewpoint, a mobile device with active NFC capability can send and receive different information for different transactions – for example, different information per transaction through the process called tokenisation (see paragraphs 3.56 to 3.61), which allows these devices to offer higher levels of security.

3.28 Almost all CMP apps in the UK use NFC technology to transmit payment information between a mobile device and the POS terminal.[21] The network of NFC infrastructure is already widely rolled out in the UK (and retailer acceptance therefore well established)[22] – mainly as a result of the growth of contactless card payments. Any CMP service with NFC technology can use a retailer's existing contactless terminals. This means that there is no need to provide any new equipment for either the consumer or the retailer, or for CMP app developers to invest in promoting the adoption of NFC technology to make CMPs.

3.29 From a retailer's perspective, NFC CMP transactions are treated by the card schemes in the same way as physical card transactions, with the same liability rules applying to retailers. Furthermore, to be able to accept CMPs, retailers only need to have POS terminals capable of effecting contactless payments (e.g. contactless plastic cards) and to receive a software update from their POS terminal provider – there is no need for further hardware changes.

19 NFC has wider applications and can be used for purposes other than payments, such as phone-to-phone connections, local information caching and transmission (e.g. in museums) or tagging areas visited (such as by security guards or cleaners).
20 A bPay device does not interact with the user's device, but is standalone and works as a prepaid card. The device is only used to top up the card.
21 The major non-store-specific CMP apps (such as Apple Pay, Google Pay, Samsung Pay and Amex Pay) all use NFC technology. Some store-specific apps (such as the Starbucks and Tesco apps) use barcode technology.
22 For example, according to the UK Cards Association, around 60% of all acquirer-owned POS terminals in the UK were contactless at the end of 2016. www.theukcardsassociation.org.uk/wm_documents/UK Card Payments 2017 - Summary FINAL.pdf

Bluetooth Low Energy

3.30 Bluetooth Low Energy (BLE) is one alternative to NFC that also uses radio-frequency electromagnetic waves, albeit using a different frequency from that used by NFC.[23] BLE works on most mobile devices and is distinctive in allowing consumers to make CMP transactions over a longer distance; a Bluetooth-enabled device does not need to be held right next to a terminal to make a transaction. However, some card issuers thought that the longer range[24] can pose security concerns, which could be a reason why Bluetooth has yet to be used as a contactless payment technology in the UK.

3.31 A BLE roll-out would also likely require new hardware to be deployed to all supporting retailers, and for those retailers to develop their own systems to integrate BLE. According to stakeholders responding to our RFIs, for these reasons, as well as the existing prevalence of NFC, BLE has yet to be adopted in the UK.[25]

Magnetic Secure Transmission

3.32 Samsung has a proprietary technology called Magnetic Secure Transmission (MST), which also uses radio transmissions to send encrypted data. MST replicates a card swipe by using a Samsung smartphone to send radio transmissions that communicate with standard magnetic credit card readers.

3.33 While card readers may require a software update to read MST messages, MST technology could be accepted at nearly all payment terminals that have a card reader. However, MST has not been made available on Samsung Pay in the UK since its launch in 2017.

QR Codes

3.34 Some mobile payment services have been launched that rely on two-dimensional (or matrix) barcodes, also known as QR codes. For example, Tesco has enabled a payment service called PayQwiq and Starbucks has a mobile payment application, both of which use two-dimensional codes. QR code-based payments work by scanning barcodes between the retailer's POS terminal and the mobile device to communicate payment details. Payments are made over the card networks. However, because these services are usually retailer-specific, they can only be used within the relevant retailer's stores. Furthermore, 2D barcodes have limited adoption and acceptance countrywide, and NFC technology is already well established. Consequently, no other solution, open to card issuers and usable outside specific retailers, is likely to be established in the UK – an opinion shared among the stakeholders who responded to our RFIs.

23 NFC operates on 13.56 MHz, BLE on 2.4 GHz.
24 BLE can work at ranges up to 100m; NFC works at a range of around 4cm.
25 However, BLE can be used to provide location-based services for mobile marketing activities. For example, a BLE beacon can provide an additional communication channel by alerting customers to offers in a shop they are passing by – even enhancing these messages with personalised offers, such as discounts or loyalty schemes, to the customer's mobile device.

Anticipated use of technology

3.35 While some of these alternative CMP technologies have been adopted and used in other countries, the submissions we have received indicate that non-NFC technology currently presents disadvantages in the UK. The primary disadvantage is comparatively limited retailer acceptance. The associated cost of building a new network and the potential need for extra on-counter equipment are likely to deter retailers from adopting alternative technologies. Some respondents to our RFIs also mentioned the security concerns currently associated with non-NFC payment methods (e.g. from BLE's signal range being wider than that of NFC).

3.36 Based on the information gathered in our RFIs, it seems that NFC is currently the main practicable option for providing widespread CMP functionality at POS terminals in the UK. Other alternatives are either proprietary or lack widespread retailer acceptance, and it appears that material investments in POS terminals would be necessary to advance their adoption.

3.37 Given the prevalence of NFC technology in processing proximity payments in the UK, this report will now focus on CMPs based on that technology.

Providing a user interface

3.38 CMP app developers offer consumers apps with which they can manage their funds as well as, in some cases, view transaction details, and use offers and gift cards. For example, users interact with Apple Pay through Apple's Wallet app, and with Samsung Pay through the Samsung Wallet.[26] CMP apps are either downloaded onto a user's mobile device or are pre-loaded onto devices before sale. The apps themselves can be intended for CMP use only or they can offer a more comprehensive set of payment options, such as online or in-app purchases.

3.39 CMP functionality within CMP apps can be part of more comprehensive mobile banking apps supplying broader services (e.g. peer-to-peer payments and banking services). Alternatively, it can be supplied to these payment apps as a 'bolt-on' or 'pass-through' service (e.g. mobile banking apps linking through to Apple Pay for CMPs).

3.40 CMP apps may also be used to engage with or sell users other services (e.g. by providing links to download other apps or by presenting targeted advertising).

Storing payment information

3.41 CMP apps must store card numbers securely, even if tokenised, to reduce fraud risks. For this reason, CMP apps do not store consumers' payment details on a mobile device's operating system (as they would most other data). Instead, CMP app developers design their apps to enable payment information to be stored on one of the following:

- a secure element built into the mobile device
- a secure element built into the mobile device's SIM card
- secure servers in the cloud (HCE)

26 A 'wallet' can be an app on the device within which the CMP app sits. Users can often store other electronic items within them too, such as event tickets, boarding passes, membership cards and coupons.

Secure element approaches

3.42 To recap, a secure element is a separate physical chip installed within a device. CMP apps that use secure elements store sensitive data within the element and communicate with it to obtain the necessary token and cryptogram to make a payment.

3.43 Secure elements on mobile devices are not generally accessible by apps placed on those devices. CMP app developers wishing to make use of a mobile device's secure element must enter into an agreement with the entity that controls it. That is, depending on the type of secure element used, CMP app developers wishing to use it must agree this with either the device manufacturer if the app is to use an in-built secure element (e.g. Apple or Samsung) or the consumer's Mobile Network Operator, if the app is to use a SIM-based secure element (e.g. Vodafone and EE).

3.44 We are unaware of any CMP app developed by a card issuer or third-party provider that uses the secure element within a mobile device or SIM card. The only CMP apps available in the UK that use the secure element embedded in the device or the SIM card are those developed by handset manufacturers and SIM card providers respectively.

Host Card Emulation

3.45 As an alternative to using the secure element built into the device or SIM card, certain CMP apps developed for the Android OS use HCE. With this solution, the CMP app developer does not need to reach an agreement with the device manufacturer or Mobile Network Operator to use the in-built physical chip or SIM card.

3.46 When HCE is used, the sensitive data is stored in the cloud rather than on the mobile device itself. Tokens are transmitted remotely to the consumer's device via the internet and mobile network, and stored there until needed for a payment. However, this data is only in single-use form (i.e. only a few time-limited single-use tokens can be downloaded and stored each time). Once the single-use tokens are used or expire, new tokens must be drawn down. This happens automatically whenever the device connects to the mobile network as part of its normal synchronisation process. This means that if the device is stolen, or its system hacked, the information on it is only usable for a limited amount of time and money.

3.47 The CMP apps based on the HCE alternative are available on all mobile devices with NFC technology enabled, except those made by Apple.

CMP Developers and their CMP apps

3.48 Based on the responses to our RFIs, we list here the main CMP apps currently available in the UK and their functionalities.

3.49 **Amex Pay (American Express):** American Express launched its proprietary CMP app in the UK – Amex Pay – in November 2016. Amex Pay is an added element to the American Express Mobile App that enables cardholders to use 'tap and pay' CMP functionality on Android devices using HCE. The American Express Mobile App does not have CMP capability on Apple devices. Amex cardholders, who have Apple devices and want to make CMP transactions, can register their cards on Apple Pay.

3.50 **Apple Pay (Apple):** Apple Pay was launched in the UK in July 2015. It is the only payment app currently available on Apple devices that can make NFC CMP transactions. Apple Pay can be used by holders of the major credit and debit cards (Visa, Mastercard and American Express) issued by many UK banks, and it uses a secure element built into Apple devices for tokenisation. While other CMP apps require user verification only when the cost of a transaction is over a certain amount (typically £30), Apple Pay requires all CMP payments to be verified, either by Touch ID (Apple's fingerprint identity sensor) or by a passcode. Loyalty cards can also be stored on Apple Pay.

3.51 **Barclays Contactless Mobile (Barclays):** Barclays Contactless Mobile was released in January 2016 and forms part of the Barclays mobile banking app. While the Barclays mobile banking app is available on both Android and Apple devices, the Barclays contactless mobile element is only available on devices using the Android OS. This solution uses HCE to store a consumer's tokenised card details in the cloud. Only Barclays debit cards or Barclaycards (i.e. credit cards) can be used to make payments through this app.

3.52 **Google Pay[27] (Google):** Google Pay was launched in the UK in May 2016. While it is available on both Android and Apple devices, it can only conduct CMP transactions on Android devices. Google Pay uses HCE and works with Visa and Mastercard credit and debit cards issued by many UK banks, as well as American Express. The consumer can add debit or credit cards issued by participating banks to Google Pay, which can be used to make payments in-store (except on Apple devices), online and in-app. Loyalty cards can also be uploaded to the Google Wallet and used automatically in Google Pay transactions, including CMPs. (The Android OS can also be used by third parties, such as banks, to offer their own NFC payment apps on Android, enabled by HCE.)

3.53 **Samsung Pay (Samsung):** Samsung Pay launched in the UK in May 2017 and is available on Samsung devices (these use the Android OS), using a built-in secure element. Samsung Pay supports Visa, Mastercard and Amex-branded cards, and can be used contactlessly in-store as well as for in-app and online payments. Samsung Pay also supports loyalty card integration for certain UK retailers. According to our RFIs, while Google Pay is usable on all Android-based devices, including Samsung ones, Samsung Pay is only available on Samsung devices.

3.54 One example of a CMP app using a SIM-based secure element was Vodafone Pay (Vodafone).[28] Vodafone Pay was launched in the UK in October 2016 and was available on the Android operating system, using a SIM-based secure element. Vodafone Pay was also a staged wallet: it used the consumer's payment card or PayPal account to put money into a 'virtual' prepaid card, details of which were provisioned into the secure element attached to the device's SIM. It was also a part of a wallet app (Vodafone Wallet) that could store loyalty cards. Vodafone Pay and Wallet closed on 28 June 2018.[29]

27 In January 2018, Android Pay and Google Wallet were rebranded as Google Pay.
28 Another example was EE's 'Cash on Tap' service, which closed in 2015.
29 According to Vodafone, 'The uptake of mobile payments has remained low and we know there are a variety of similar services on the market. We have therefore decided to concentrate on our other Vodafone apps and services.' www.vodafone.co.uk/explore/apps/vodafone-wallet

3.55 As well as the CMP apps listed above, we note the existence of Zapp (VocaLink/ Mastercard). Zapp offers a way for consumers to pay retailers directly from their bank accounts, using their mobile devices. This pay-by-bank-app functionality is offered to banking apps and retailers' sites to facilitate payment. For in-app and online purchases, the consumer uses the pay-by-bank-app button on the retailer's app and is then put through to their mobile bank app where there is a request-to-pay message. They then choose which account to pay from and the payment is made. Zapp is currently used by a number of card issuers in their banking apps (and a number of retailers' apps too). Zapp can also offer banks CMP functionality for their mobile apps on Android devices, via the NFC antenna.

Tokenisation

3.56 Tokenisation is currently a key feature of CMPs and the main difference between CMPs and contactless payments using plastic debit and credit cards. It is intended to reduce the risk of the PAN being stolen electronically in the course of a CMP. The PAN of the payment card being used is generally the main payment information susceptible to fraud in card payments. It provides a direct link to a consumer's bank account or credit facility.

3.57 Tokenisation is the process by which a card's PAN is replaced by a DPAN. A PAN can be used if obtained fraudulently but a DPAN cannot. This is because CMPs require DPANs to be supplied alongside other information to validate them, usually in the form of a dynamic cryptogram. These cryptograms are limited-use codes (usually single-use) that relate the token to the consumer's contactless device. Without the cryptogram, the token service provider cannot validate the DPAN and match it to the PAN to permit a purchase to proceed. The cryptograms are also difficult to use fraudulently because (as the name suggests) they are non-static, encrypted and only valid for a limited time and number of purchases. Furthermore, only tokenised information is ever transmitted between a mobile device and a retailer's POS terminal.

3.58 When a card number is tokenised, the PAN is replaced by the card issuer's TSP with a second series of numbers (the token), which is then stored on the mobile device and sent to the retailer's POS terminal (along with device-specific information and payment details) to complete a CMP transaction. Because tokens are not generated using an algorithm, the PANs that they replace cannot be reconstructed from the tokens themselves.

Card provisioning and the tokenisation process

3.59 The act of enrolling a payment card for use with a CMP app on a mobile device is known as 'provisioning'. Tokenisation occurs during the card-provisioning process. Consumers enrol their cards with a CMP app by entering their PAN, security code and other information requested by the app. The CMP app provider then requests a token from the TSP. The TSP forwards the request to the card issuer for approval. If that approval is given, the TSP creates a token to replace the PAN and the token is then used in CMP transactions. The TSP stores a list of the tokens and their corresponding PANs in its 'token vault'.

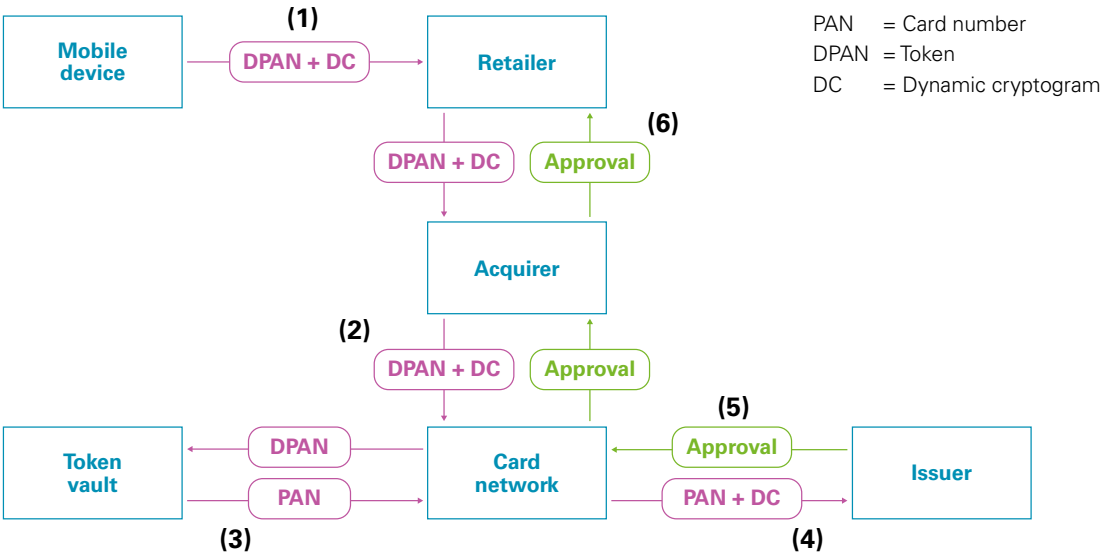
3.60 The token is a device-specific account number that the TSP sends directly to the consumer's device. Tokens are unique to each card and device, and serve as a proxy for the consumer's card account. They are stored on the secure element of the consumer's device, a secure element on the SIM or 'in the cloud' under HCE (as per the different configurations discussed in paragraphs 3.41 to 3.47).

3.61 During tokenisation, the TSP also creates cryptographic keys. As with the token, these cryptographic keys are provisioned (placed) into the secure element, or stored in the cloud, as per the method used. The use of dynamic cryptograms (as created by the cryptographic keys) is one of the principal security features underpinning the EMV tokenisation specification. It means that, even if a fraudster were to obtain a token, the information would be of no use because the token could not be used to make transactions without an associated dynamic cryptogram. The tokens, and the PANs they correspond to, are kept by TSPs on behalf of card issuers as part of the tokenisation service.

The tokenised transaction process

3.62 When a CMP transaction is made, the CMP app takes the token and dynamic cryptogram from the secure element on the device or SIM card, or from the cloud under HCE, and sends these through the NFC antenna to the retailer's POS terminal. From there, the payment information journey is represented in Figure 1.

Figure 1: Information flows in a CMP transaction



3.63 In Figure 1, the pink flows represent the gathering of relevant payment information pre-approval, and the green flows show the transmission of that approval back to the transaction location. The sequence is as follows:

1. The consumer's DPAN (the token replacing their card number) is combined with a dynamic cryptogram (containing information on the device and the transaction itself) and sent via the NFC antenna to the retailer's terminal.
2. The acquirer takes the information from the terminal and passes it to the relevant card network operator.
3. The card network operator sends the DPAN to the TSP's token vault to be verified and exchanged for the card number (PAN).
4. The card network operator then sends the PAN and dynamic cryptogram to the issuer for verification and approval.
5. The issuer now has the card information, payment details and confirmation that the CMP instruction came from the consumer's device. They then send their approval for the transaction back to the card network operator.
6. From the card network operator, the approval is transmitted back to the acquirer and on to the retailer, who sees that the consumer's payment has been accepted and that they will be paid for the goods or services sold.

Security

3.64 By transmitting tokens rather than card details, CMPs could arguably lead to lower fraud risks than contactless payments made using plastic cards. Also, consumers' payment details (even when tokenised) are not stored on the mobile device's OS, but on either a secure element (on the device or SIM) or on secure servers in the cloud (HCE). Several issuers and card scheme operators set out these security points as advantages of CMPs and tokenisation in their responses to our RFIs. However, data supplied by these parties does not yet conclusively show this to be the case. CMPs are still relatively new and reliable fraud data will take time to accumulate.

3.65 Statistics regarding the level and nature of fraudulent CMP transactions will build as CMPs continue to be adopted by consumers as a payment method and industry will be better able to assess the potential for CMPs to reduce the incidence of fraud in the payments sector.

CMP usage

3.66 Payment by card is now more popular in the UK than using cash, and contactless payments accounted for nearly 40% of all in-store payments in October 2017 (up from 24% the year before).[30] While CMPs still constitute a small percentage of all UK contactless payments, they are in the tens of millions each month and increased 2.5 times between mid-2016 and mid-2017. If this growth continues, CMPs could come to represent a significant proportion of daily consumer payments.

30 www.ukfinance.org.uk/wp-content/uploads/2017/12/Card-Expenditure-Statistics-October-2017.pdf

Recent CMP use

3.67 Figure 2 is taken from surveys conducted by Mintel in April 2017 and February 2018.[31] It shows the percentages of the people surveyed who used a number of different payment methods over the six-month periods to the two survey dates.

Figure 2: Use of payment methods, April 2017 and February 2018

Use of payment methods in preceding 6 months

	April 2017		February 2018	
	≤ last 6 months	**Never**	**≤ last 6 months**	**Not in last 6 months**
Cash	95%	2%	97%	3%
Debit card (chip and PIN)	87%	7%	83%	17%
Contactless debit card	53%	42%	63%	37%
Credit card (chip and PIN)	57%	33%	62%	38%
Contactless credit card	49%	47%	43%	57%
CMP (e.g. Apple Pay, Google Pay)	16%	82%	24%	76%
Contactless wearable	11%	87%	15%	85%

Base: 2,000 internet users aged 16 or over
Source: Lightspeed/Mintel

3.68 While 16% of people surveyed had made a CMP transaction in the six months preceding the 2017 survey, 24% had done so in a similar period before the 2018 survey. This shows a fairly strong increase in the use of CMPs in a relatively short time. This is consistent with responses to our RFIs. The survey also shows increased use of debit cards and wearables for contactless payments between the two periods (and a decrease in contactless use of credit cards).

3.69 With regard to the longer term, Mintel's April 2017 survey looked at awareness among the same survey population of different methods of mobile payment by age group (see Figure 3).

31 Mintel: *Consumer Payment Preferences – UK, June 2017 and Consumers and Payment Innovation - UK - May 2018*

Figure 3: Awareness of mobile payment schemes by demographic, April 2017

'Which, if any, of the following payment providers have you heard of?'

Age group	Apple Pay	Google Pay	Samsung Pay
16 to 34	60%	42%	23%
35 to 44	57%	41%	19%
45 to 64	58%	41%	19%
65 and over	42%	20%	9%

Base: 2,000 internet users aged 16 or over
Source: Lightspeed/Mintel

3.70 Figure 3 shows an awareness of CMP-enabled payment apps among a significant percentage of the surveyed population, especially younger people (and a lower awareness among the 65 and over age group). Considering that the apps in question have only been available for a few years, this indicates positive levels of awareness and scope for growth in both knowledge and use.

3.71 Current consumer attitudes towards 'going cashless' could give some indication of future use of contactless payments as a payment method, as seen in Figure 4.

Figure 4: Attitudes towards non-cash payment methods by demographic, April 2017 and February 2018

'I am comfortable with the idea of a cashless society'

	April 2017			February 2018		
Age group	**Yes**	**No**	**Don't know**	**Yes**	**No**	**Don't know**
16 to 24	39%	41%	20%	47%	34%	19%
25 to 34	46%	37%	17%	51%	36%	13%
35 to 44	36%	47%	17%	39%	47%	13%
45 to 54	30%	54%	15%	29%	57%	13%
55 to 64	21%	62%	17%	21%	67%	12%
65 and over	20%	68%	13%	21%	69%	10%

Base: 2,000 internet users aged 16 or over
Source: Lightspeed/Mintel

3.72 There appears to be a significant number of survey respondents in both surveys

who would be comfortable to go cashless. The number is also higher for younger respondents (i.e. aged between 16 and 45). It is also interesting to note increases in the percentages happy to go cashless in the same age groups, between the two surveys. These findings could suggest a growing propensity in the population towards accepting card-based and contactless payments over cash, which could result in increased uptake and use of CMP apps on mobile devices.

Future CMP use

3.73 Based on the views of stakeholders, it seems likely that the use of CMPs will continue to increase in the foreseeable future. There are several factors that are likely to drive this increase:

- There was a general consensus among the respondents to our RFIs that there would be continued growth in CMPs over the next few years, driven by increasing consumer adoption, more NFC-enabled POS terminals[32] and increasing acceptance (and facilitation) of higher-value (>£30) CMPs by retailers.[33]
- There is also potential for increased CMP use through the broader emerging scope for contactless payments – for example, for transport (already adopted in many areas in the UK) and through the growing use of NFC-chipped wearable devices (where these are directly linked to a CMP app).
- CMP apps may also begin to use interbank payment systems in addition to, or instead of, cards, which could increase the scope for innovative services. As we have seen, the functionality for interbank-based CMPs already exists.
- Changes introduced by PSD2 and Open Banking[34] are expected to increase competition in the payments sector by promoting open access to payment systems and accounts. Non-PSPs, corporates (such as Amazon) and FinTech businesses will be able – with consumer consent – to access consumer bank accounts directly to perform payment activities. Thus, for example, non-PSPs could be able to offer contactless pay-by-bank apps or functionality.
- CMP use may increase as other services are now integrated into CMP apps – for example, loyalty cards and discount coupons. CMP app providers told us they see this integration making the use of CMPs more convenient – for example, removing the need to carry loyalty cards, as these can be applied automatically to relevant transactions through the CMP app – and could lead to an increased uptake in CMPs.

32 According to UK Finance, there were 491,084 contactless-enabled bank-owned terminals in the UK in April 2017.
33 Where a CMP is verified by the consumer, for example via the Touch ID fingerprint reader on Apple Pay, retailer POS terminals can (at the retailer's discretion) accept higher value payments.
34 The revised Payment Services Directive (PSD2) was transposed into UK legislation in the Payment Services Regulations 2017 (PSRs 2017). The Competition and Markets Authority issued a ruling (Open Banking) requiring the nine biggest UK banks to allow licensed entities direct access to their customers' account information (if the customers chose to engage the entities).

Incentives

3.74 The different parties involved in providing CMP services to consumers have different incentives for doing so:

- **Card issuers** told us that it is important that their customers have as many secure and convenient ways as possible of making payments with their cards. They also told us that they need to offer their customers the newest innovations in payment methods.
- **Card scheme operators** have an incentive to maintain, or even increase, the number of payments consumers make through their schemes. To achieve this, consumers must choose to use schemes' cards, which are issued by card issuers and must be accepted by as many retailers as possible.
- **Device manufacturers** pointed out that a CMP app developer can provide an additional functionality to a mobile device.
- **CMP app developers** have different incentives when offering their products, depending on the model they follow for monetising them that we now discuss.

CMP app monetisation

3.75 When monetising use of their apps, CMP app developers do one of the following:

- They charge fees to the card issuers that participate in the CMP app.
- They charge nothing for use of the CMP app but monetise the transaction data obtained.

3.76 We explain these in turn, making no judgment about the advantages and disadvantages of the alternative approaches. In this review, we did not consider the regulatory issues around the use of data. We recently published a discussion paper on the future of data in payment systems, indicating that it intends to consider how data is used in this context.[35]

Fees

3.77 To offer card-based CMPs, a CMP app developer needs to interact directly with card schemes, card issuers and consumers. CMP app developers may therefore charge any or several of these parties fees for using their products. This is illustrated by the different approaches of Apple and Google, currently the main players in this sector.

- Apple does not charge consumers fees for making payments through Apple Pay, or card schemes for processing transactions through Apple Pay. However, Apple charges fees to card issuers that participate in Apple Pay.[36]
- Google does not charge card schemes, card issuers or consumers for use of Google Pay.

35 www.psr.org.uk/psr-publications/news-announcements/shaping-future-data-payment-systems
36 See, for example: www.ft.com/content/02287f44-2a3d-11e5-8613-e7aedbb7bdb7

Data

3.78 If it chose to do so, a CMP app developer could, instead of charging a fee, retain data on an individual's purchasing history (regardless of the type of card used). Such data, which can reveal an individual's spending habits, can be monetised, even if the data is not passed to a third party. We have observed different approaches from CMP app developers in respect of their approaches to monetising data. This is illustrated by the different approaches of the two biggest players – Google Pay and Apple Pay.

- Google states in the terms of service for Google Pay that, as permitted by its privacy policies, the user permits Google 'to collect transaction, account, and other personal information from third parties, including retailers and your payment method's issuer'. In its general privacy policy, Google states that 'ads help keep our services free for everyone. We use data to show you these ads, but we do not sell personal information like your name, email address and payment information'.[37]
- In contrast, Apple's website states that 'Apple Pay doesn't collect any transaction information that can be tied back to you'.[38]

The benefits of CMP apps

3.79 CMP apps provide consumers with another way of using their cards to make contactless payments (by 'tapping' their mobile device rather than a plastic card). This extra option could create benefits for both consumers and retailers. In our RFIs, we asked stakeholders what these benefits might be. Stakeholders told us about the following:

- Consumers are able to pay without carrying a physical plastic card with them. This was mentioned by a card scheme operator, several card issuers and a mobile network operator. We note that there is also a potential benefit to a consumer from being able to make CMPs if their plastic card is not contactless.
- Retailers will be able to integrate loyalty schemes with CMP apps, removing the need for consumers to carry and produce a separate card. In turn, this could encourage consumers to use the loyalty scheme for any given transaction, thereby benefiting the loyalty schemes. These were mentioned by a card scheme operator, several card issuers and a mobile network operator.
- According to respondents, CMP apps can, in principle, enhance the security of a contactless payment by requiring biometric authentication before the payment is processed and through the tokenisation process (this may not be available with other payment methods[39] – see paragraphs 3.64 to 3.65). This point was made by card scheme operators, a number of card issuers, a mobile network operator, CMP app providers and a payment system operator. A card scheme operator also pointed out that issuing banks can benefit from the cost savings of not having to issue physical cards or administer and arrange for replacements if they are lost.

37 https://privacy.google.com/intl/en-GB/your-data.html
38 https://support.apple.com/en-gb/HT203027
39 Some card issuers have suggested to us that awareness is low of the security benefits of making a contactless payment using a mobile rather than a plastic card. This is supported by research by Mintel that cites security concerns as a key reason why survey respondents have not used a smartphone to make payments or transfers. (Mintel: Consumer Payment Preferences, UK, June 2017). This is despite CMP app providers' explanations about the security benefits (see, for example, https://support.apple.com/en-gb/HT203027 and www.samsung.com/us/support/answer/ANS00043932).

- The consumer has easy, real-time access to a list of their payments. Consumers with payment cards can see this too, through their mobile banking app, but it would not be in real-time –there would be a delay while the card payment cleared through the system. This was mentioned by two card issuers and a mobile network operator.
- In general, CMPs offer increased speed and simplicity of payments for consumers. This was mentioned by CMP app providers and card and payment scheme operators. It was also pointed out by some card issuers that retailers could benefit from being able to offer a more seamless checkout for consumers, reducing the time needed to serve them.
- One card issuer made the point that retailers may also benefit from consumers having more payment options (possibly making them more likely to make a purchase). Also, to the extent that consumers recognise the security advantages of CMP apps, this could benefit those retailers taking payments, in terms of being able to accept higher-value contactless payments when the CMP app supports this (for example, through fingerprint verification). Another card issuer said that retailers may also be able to provide an electronic receipt through the CMP app, which reduces cost and the environmental impact of paper receipts.
- Several card issuers and a card scheme operator told us that CMPs allow card issuers to add new services to their current account offerings, to provide consumers with a wider choice of payment methods and to provide a new alternative to cash. Card issuers also told us that CMPs allow retailers to deepen customer relationships via consumer messaging opportunities and further value-added services.
- Two card issuers and a card scheme operator pointed out that CMPs (when verified – for example, by a fingerprint scan) could enable consumers to make contactless payments for purchases over £30, whereas cards must be inserted into POS terminals and a PIN used. Retailers could also benefit from somewhat shorter checkout times if consumers chose to make such contactless payments instead of using chip and PIN.

3.80 Most of these benefits are widely available today from CMP apps. Others were raised by stakeholders as potential benefits to both retailers and consumers from using CMP apps.

4 Issues considered in the CMP sector

Access to the NFC antenna[40]

4.1 Near-field communication (NFC) technology is the prevalent technology used to make contactless mobile payments (CMPs) in the UK. As we explained in paragraph 3.36, NFC appears to be the only current feasible option for widespread contactless POS payments.

4.2 The principal concern raised with us was that only Apple has access to the NFC antenna on its devices in a way that can be used to make CMPs. Some card issuers alleged that this restriction on access prevents non-Apple CMPs from operating on these devices, thereby limiting innovation and competition. Comments included:

- card issuers are not able to develop their own branded payment apps to access the NFC capability on Apple devices
- third-party applications are unable to offer host card emulation (HCE) solutions on Apple devices, and cannot innovate with alternative propositions on Apple devices
- as a result of this restriction, Apple-using consumers are not able to access a complete set of alternatives for CMPs on their devices

4.3 However, other card issuers said the restriction on access to the NFC antenna made no difference to their businesses, either because they did not wish to launch their own CMP apps or because they were content with offering their customers CMPs through Apple Pay.

Potential innovation in CMPs

4.4 We sought to understand what the effect of restrictions on access to the NFC antenna on Apple devices could be. In particular, we looked at whether there were any substantial innovations being hampered by the restrictions. CMP solutions that run on platforms that offer access to the NFC antenna (i.e. on Android) offer similar features to Apple Pay.

4.5 There seems to be no great difference – in terms of innovation – between Apple Pay and what is available on the Android platform. Google Pay, Samsung Pay and Amex Pay, for example, all have the same basic functionality as Apple Pay. For example, Apple Pay supports online, in-store and in-app payments.

40 In 2016, following the launch of Apple Pay in Australia, a coalition of Australian banks sought authorisation from the Australian Competition and Consumer Commission (ACCC) to negotiate collectively with Apple over the use of Apple Pay. The ACCC decided not to give clearance to the proposed collaboration, because it did not believe that the likely benefits (in terms of increased competition in CMP apps) would outweigh the likely detriments – harm to Apple's business model, reduced innovation in contactless payments and reduced competition between retail banks. While the ACCC decision is helpful in its examination of some aspects of CMPs, it nonetheless differs from our own work. The ACCC decision looked at the possible effects of granting permission for collective bargaining; we looked at the workings of the CMP sector in general.

4.6 In addition, in the course of our call for information, we did not identify any clearly distinct products that would likely become available if access to the NFC antenna was granted by Apple. None of the issuers suggested that their own apps (had they developed a CMP app) would have offered their customers something significantly more than what was already available through Apple Pay. We asked card issuers about the effect of Apple's restrictions to the NFC antenna, and about what they would do if access to the NFC antenna on Apple devices were open. The issuers identified:

- automatic updating of loyalty card points
- a function to 'auto-provision' customer's cards, and thus eliminate fraud arising at the point of provision.
- a functionality to pay-by-bank (i.e. via Faster Payments) at a physical POS using NFC.[41]
- allowing consumers to use a mobile device to withdraw cash at an ATM.

4.7 'Auto-provisioning' of customer cards, and the adding of loyalty cards are currently available on the two main CMP apps (Apple Pay and Google Pay). Some card issuers already allow their customers to use a mobile device to withdraw cash at an ATM.[42] We also note that the functionality to pay-by-bank is not available on either Apple- or Android-based CMP apps. This may be an opportunity for innovation in the future. In particular, contactless pay-by-bank functionality could be a significant innovation for card issuers.

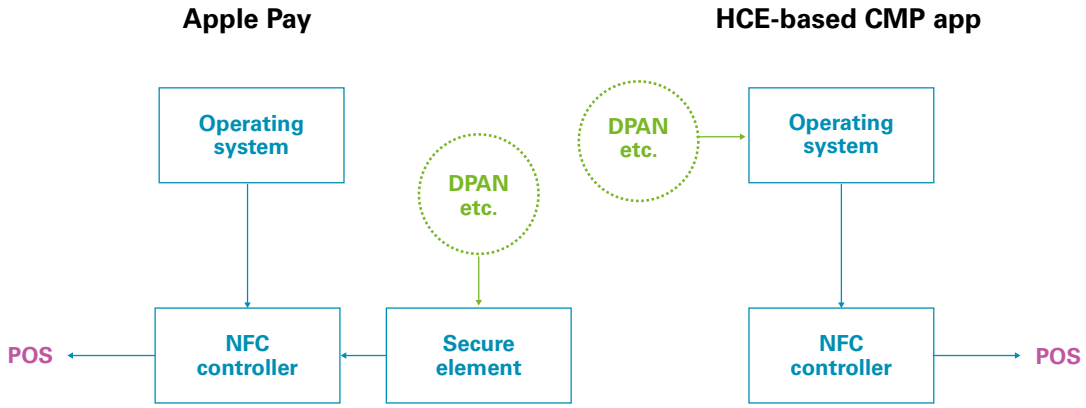
Stakeholder views on potential for consumer benefits arising from restricted access to the NFC antenna

4.8 Apple claimed that there are benefits for consumers arising from its refusal to allow third parties access to the NFC antenna for CMPs on Apple devices.

4.9 Apple told us that it places significant value on privacy[43] and security (for example, through the curation of apps that can be installed on Apple devices) and that Apple devices are designed with security as a main concern (for example, including a device-based secure element). See Figure 5.

41 We understand that, since May this year, PayPal can be used with Google Pay and Samsung Pay in the USA (though not in the UK).
42 For example, RBS and NatWest both offer a service through their mobile banking apps, using a PIN, requested and received via the customer's mobile device and entered into the ATM to retrieve cash. While not NFC-based, this service offers the same functionality and can be used on both Apple- and Android-based devices.
43 www.apple.com/uk/privacy

Figure 5: Apple Pay and HCE payment credentials and storage



4.10 According to Apple[44], the secure element (where the DPAN and dynamic cryptograms are stored) is completely isolated from the device's operating system, and the payment credentials pass only through the NFC controller on their way to a retailer's POS terminal. On devices that allow HCE CMPs, the payment credentials sit within the operating system.

4.11 Apple told us (and have stated publicly[45]) that giving third parties access to the NFC antenna built into Apple devices could lead to concerns affecting the security of CMPs. Apple says that such issues would lessen the security on its devices.

4.12 Apple also told us that opening access to the NFC antenna on its devices would degrade the user experience associated with its devices and brand. According to Apple, there could be friction introduced to this experience if using a third-party app required a change in settings on the device itself before use – for example, to switch between payment apps.[46]

Our current view based on the evidence available

4.13 Although some card issuers argued that Apple's restriction was harmful, the majority of the respondents didn't raise any concerns. Some card issuers complained about negative effects of restricted access, although they were not able to identify specific restrictions on innovation at this stage. We have not identified any innovations in CMP services that are not being developed as a result of the restriction.

4.14 Although we were not told of any specific feature not being offered to Apple users, or of any major development being hindered on the Apple platform, this is still a developing market and we would like to keep a close review of the effects of the restriction, including on fees, product development and user choice of mobile payment solutions.

44 See, for example, www.apple.com/business/docs/iOS_Security_Guide.pdf
45 For example, www.accc.gov.au/system/files/public-registers/documents/D16+149872.pdf, page 5.
46 See also www.accc.gov.au/system/files/public-registers/documents/D17+9804.pdf, page 19.

Tokenisation services

4.15 Tokenisation is a key element in CMPs: it aims to make the card information stored on mobile devices unusable elsewhere, thereby reducing the possibility of fraud through card number theft.

4.16 In our initial request for information (RFI), we wanted first to understand what tokenisation is, how it is provided, whether there are standards and, if so, how these were set up and what is their role in the provision of CMPs. In our second RFI, we asked stakeholders for more detailed information regarding the EMV specification.

The EMV specification

4.17 The tokenisation process for CMPs in the UK generally occurs in accordance with the industry standard known as the EMV specification. This is the main global standard for tokenisation services. It describes the payment tokenisation ecosystem, the types of entities needed to support payment tokens and the main responsibilities of each entity. It also outlines minimum requirements for the creation and use of payment tokens, such as token format, domain specificity, which parties can know what information, etc.

4.18 The EMV specification was developed by EMVCo, which is a limited liability company owned by six of the major card schemes[47], each of which has 1/6 ownership. EMVCo developed its tokenisation specification to allow a registered party to offer tokenisation services and to ensure compatibility across CMP apps. The EMV specification defines a number of roles and concepts relevant to the tokenisation process. These are explained in turn below:

- **Token services:** These can include the generation and storage of payment tokens, placing tokens into a digital wallet on a consumer's device (known as 'provisioning'), keeping the lists of corresponding primary account numbers (PANs) and device primary account numbers (DPANs) for confirmation on request by the card issuer via the card system operator, as well as managing authorisation messages between the various parties. Tokens are usually 'domain-specific' – i.e. specific to the type of payment being made or device on which the transaction is initiated (for example, specifically for CMPs or on a specific mobile device). This means that if someone tried to use a CMP-specific token for an e-commerce payment via a web-browser (or vice versa), or to use a CMP token on a device different from the one on which the token was provisioned, this would not pass the token service's domain controls.
- **Token service provider (TSP):** A TSP generates and provisions tokens to be used on consumers' mobile devices, stores and manages records of those tokens over their working life, and deletes them once they expire.
- **Token vault:** The token vault is where a TSP stores PANs and their linked DPANs. The vault is consulted during a CMP transaction to match the token with its corresponding card number in order to validate the payment request.

47 American Express, Discover, JCB, Mastercard, UnionPay and Visa.

4.19 While these services are generally undertaken by the main card schemes acting as TSPs, they can – together or separately – be provided by card issuers or other parties. However, if a TSP wishes to become EMV specification-compliant from the processes detailed on the EMVCo website relating to becoming an EMV TSP, there are also administrative requirements and costs involved with becoming registered with the organisation.

Possible issues with the EMV specification

4.20 We considered whether the EMV specification might have any effect on the provision of tokenisation services for CMPs. Specifically, we considered whether:

- card issuers had to use particular providers of tokenisation services
- there was any restriction on non-card-scheme TSPs to develop and offer tokenisation services

4.21 We have examined the EMV specification and engaged with relevant stakeholders in relation to how the standard was developed and is set in practice.

4.22 We were told in the responses to our RFIs that some CMP app developers require use of the EMV specification from other parties but that others do not. However, the main suppliers of tokenisation services (the three main UK card network operators) all offer EMV specification-compliant services.

4.23 On the basis of responses to our RFIs, participants appear to prefer using the EMV specification. According to one card issuer, the existence of the common standard on a global scale has had a positive effect on the development and uptake of CMP in the UK. They said this means that card issuers do not need to develop and agree a separate standard for each wallet provider, making the economics of tokenisation more affordable from the perspective of the banks.

4.24 All final decisions relating to the EMV specification are taken by EMVCo members only. However, non-members can become involved in the process of developing and setting the standards, and the standards are freely available.

4.25 We were not made aware of any examples of tokenisation services being prevented market entry because of the introduction and operation of the standard and its associated costs and processes. We were not told of any firm that had been prevented from developing its own tokenisation services due to the existence and operation of the EMV specification. No card issuer has reported that they have been prevented from choosing their own TSP.

5 Concluding remarks

Benefits for end users

5.1 The development of contactless mobile payments (CMPs) as an alternative payment method has the potential to bring significant benefits for participants in payment systems and the people and organisations that use them. Nonetheless, while the use of CMPs is continuing to increase, they currently still represent a relatively small percentage of all payments in the UK.

5.2 Respondents to our requests for information (RFIs) told us that CMP apps can create real benefits for consumers, retailers and card issuers, beyond those currently derived from plastic card contactless payments. For consumers, these benefits are claimed to include:

- generally increased speed and simplicity of payments
- not having to carry a physical card
- being able to link payments to loyalty schemes
- being able to make contactless payments from a non-contactless payment card
- the security brought by tokenisation (and possibly biometric authentication)
- real-time access to payment history

5.3 For retailers, benefits could include:

- consumers having more payment options
- the improved security of CMP apps could allow retailers to accept higher-value contactless payments
- retailers being able to offer electronic receipts through the CMP app
- higher-value payments meaning shorter checkout times if consumers chose CMPs over chip and PIN payments

5.4 For card issuers, benefits could include:

- CMPs allowing them to add new services to their current account offerings in order to retain or compete for customers
- CMPs providing consumers with a wider choice of payment methods
- CMPs providing a new alternative to retailers for taking payment from consumers
- the security brought by tokenisation (and possibly biometric authentication)

5.5 More benefits may arise as the sector continues to evolve. If the benefits just outlined are significant, they may drive and increase take-up of CMP services by consumers and retailers, and card issuers may continue to want to provide these services for their customers.

Our role in protecting competition, innovation and the interests of service-users

5.6 We have considered a range of issues in our call for information exercise. These have included whether the setting of a tokenisation standard and restricting access to key hardware and software elements have a detrimental impact in our objectives.

5.7 Respondents to our RFIs did not identify significant innovation that was being held back by Apple's restriction to give access to its NFC antenna. Any restrictions – including on software or hardware – that have the potential to hinder the development of products or access to payment services will be kept under observation. In order for all end users of CMP apps to be able to take full advantage of current and future benefits of this payment method, it is important that efficient competition and innovation in the markets concerned are maintained.

5.8 CMPs are still a relatively new development and are also a fast-developing part of the payments sector. For these reasons, we will continue to keep the CMP sector under observation as it develops further, retaining the option to investigate in future and to take any action we believe to be necessary to address any problems we may identify or that are brought to our attention. We will therefore continue to monitor developments in this rapidly changing sector.

6 Glossary

Term or abbreviation	Description
Card issuer	A PSP contracting to provide a consumer with a payment instrument to initiate and process the consumer's card-based payment transaction, made by means of any card, telecommunication, digital or IT device or software
Card network	A payment system that enables a holder of a payment card to make a payment
Card scheme	A single set of rules for card-based payment transactions, including any specific decision-making body accountable for the functioning of the scheme
Contactless-enabled mobile devices	Mobile devices that are capable of using contactless technology to initiate CMPs. They may also be capable of implementing security services such as tokenisation
Contactless mobile payment (CMP)	A payment initiated on a consumer's mobile device that uses contactless technology to transmit payment information to a retailer's terminal
CMP app	A computer program, designed to run on a mobile device, that allows that device to make CMPs
Contactless technology	Short-range wireless communication technologies used to transmit payment information from a consumer's device to a retailer's terminal – for example, near-field communication (NFC), Magnetic Secure Transmission (MST) and Bluetooth Low Energy (BLE). These could be available on a contactless-enabled mobile device or on a passive device, such as a contactless payment card
Device primary account number (DPAN)	The token, generated by a card issuer's TSP, linked to a consumer's PAN and used to make CMP transactions (also known as a 'digital' primary account number)
Host Card Emulation (HCE)	Software that enables certain CMP apps to make tokenised contactless payments without relying on a secure element
In-app payment	A payment initiated using a retailer's software application on a consumer's device that transmits payment information to that retailer over the internet
In-store payment	A payment initiated by the transmission of payment information from a consumer's device to a retailer's POS terminal. Payments can be initiated by both passive and 'smart' devices

Term or abbreviation	Description
Mobile device	An electronic device, excluding cards, tags or fobs, that can operate interactively and autonomously, and that connects to other devices or networks via wireless protocols such as Bluetooth, NFC, WiFi or 4G
Near-field communication (NFC)	A standard of wireless communication for enabling a contactless connection between devices. In the case of contactless payments, NFC is the technology that enables them to be made – whether between a contactless card and a POS terminal or between a mobile device and a POS terminal
NFC antenna	A piece of electronic transmitting and receiving equipment, built into a mobile device, that enables CMPs to be made in-store using NFC technology
Online payment	A payment initiated within a browsing application on a consumer's mobile device that transmits payment information to a retailer over the internet
Operating system	The system software that manages computer hardware and software resources, and that provides common services for computer programs
Payment Service Provider (PSP	In relation to a payment system, any person who provides services to people who are not participants in the system for the purposes of enabling the transfer of funds using the payment system (see also s.42(5) FSBRA)
Point-of-sale (POS) system	The hardware and software used to record a retail financial transaction
Primary account number (PAN)	The 12-digit number across the middle of a payment card (credit or debit) that identifies the card account holder's account – also known as a 'funding' primary account number (FPAN)
Secure element	A chip used to store sensitive payment data on a mobile device. The secure element stores the provisioned cards' DPAN tokens and other dynamic information used to verify them as coming from the consumer's device
Tokenisation	The substitution, often to enable secure mobile payments, of sensitive payment data (e.g. a consumer's PAN) with data still capable of initiating a payment, but of more limited potential value if intercepted or stolen
Token service provider (TSP)	A party that provides services that can include generating and provisioning tokens to be used on a card issuer's customer's mobile device; storing and managing records of those tokens over their working life; and deleting them when this is over

12 Endeavour Square
London E20 1JN
Telephone: 0300 456 3677
Website: www.psr.org.uk