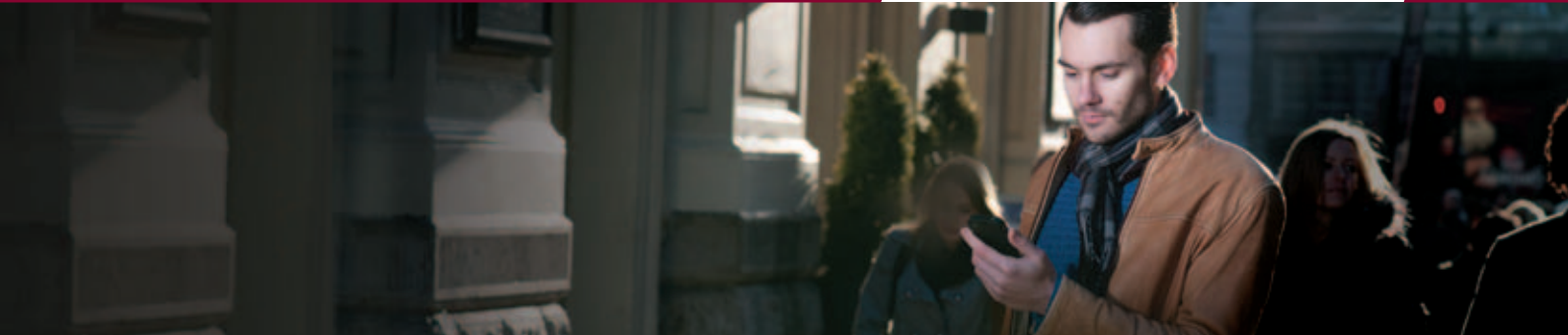
Financial Conduct Authority

Thematic Review TR13/6

# Mobile banking and payments – supporting an innovative and secure market

August 2013



# Contents

# Foreword by Clive Adamson – FCA Director of Supervision

Mobile phones are an invaluable part of everyday life; consumers use their smartphones for much more than phone calls or text messages.

The technology that is now contained in a smartphone is greater than most computers had only a few years ago. The retail banking sector has embraced this technology and innovated, delivering new ways for their customers to transact. This has been a strong driver in shifting consumer behaviour and many now expect access to at least basic banking services through their smartphones. Research published earlier this year showed that one in five adults in the UK has already made a payment using their phone; over a quarter of us use our mobiles to check bank balances, and more than half of us would pay with our phone if it was an option in the local supermarket.[1]

As mobile banking continues to develop and grow in popularity, we have seen greater choice for consumers, as different types of firms launch a variety of mobile banking products. We recognised in the 2012/13 Risk Outlook and 2013/14 Business Plan that mobile banking has the potential to rapidly increase in popularity. Having identified this, we wanted to carry out thematic work to understand the potential risks, as well as the measures being taken by firms to address them.

We approach this review with clear outcomes in mind. We want to support innovation that provides consumers with products that meet their needs and expectations while also ensuring their interests are protected.

Although we haven't concluded our work in this area, we are publishing this interim report and outlining our next steps as part of our ongoing commitment to greater transparency. As well as being open on what we're doing, we are looking forward to engaging with firms, technology providers, trade associations and consumer groups so that we can get a clear view of mobile banking.

1 TNS Survey, May 2013

# 1. Overview

Mobile banking and payments are growing in popularity with consumers. A recent report from Juniper Research suggests that over 1 billion global mobile phone users will have made use of their mobile devices for banking purposes by the end of 2017, compared to just over 590 million this year[2]. The innovation and product development that is taking place provides consumers with greater flexibility to carry out their everyday banking using a new and convenient channel. However, any new technology can also present risks.

This interim report summarises the findings from our initial work on mobile banking and payments, setting out areas of potential risk to consumers and to the market more broadly. We also outline our high-level plans for our future work on mobile banking.

During the next phase of our work we will do a more detailed assessment to test if providers of mobile banking services ensure their offerings are secure, technically robust and straightforward for consumers to use. We will continue to engage with industry, working with firms and trade associations to deliver these objectives.

We will provide a further update in the first half of 2014.

## Who will be interested in this report?

Our work will be of interest to firms that operate in this market, as well as consumer groups and members of the public who are using mobile banking or may wish to do so in the future.

This report does not constitute general guidance or contain detailed findings. It is an interim report to provide information about our work on mobile banking as part of our commitment to be a transparent regulator.

## What do we mean by mobile banking?

Mobile payment services enable consumers to make a payment to an individual or a firm using their mobile phone, tablet computer or other handheld device.

Mobile banking is a broad term, which includes services providing information to consumers, in addition to making payments. This includes features such as allowing consumers to check their account balance, to view statements and to see the latest activity on their account.

In this report we will generally use the broader term of 'mobile banking'.

2 Juniper research January 2013

Our work focuses on the different ways in which consumers may carry out mobile banking on their mobile phones or tablet computers. This includes contactless payments (sometimes called 'NFC' or 'near field communication') made using a mobile device. It does not include payments made using contactless cards, as there is no mobile phone involved.

Our work does not focus on established online or internet banking services, although aspects of the work may be relevant where consumers are using a mobile device to access their regular internet banking.

## Why have we looked at mobile banking and payments?

We aim to tackle potential risks to consumers at an early stage to prevent them from developing. We originally identified innovative banking and payment technologies as an area of interest in 2012 and did some early thematic work to understand any potential risks associated with mobile banking. The high-level findings of this initial work are set out in this report. Our 2013 Risk Outlook identified the growth of usage and broad range of technological developments in this market. We committed to undertake further work on mobile banking in our 2013/14 Business Plan.

## What are we trying to achieve?

We would like to see innovation that provides consumers with products that meet their needs and match their expectations. Our objectives include market integrity and consumer protection, so we wish to ensure that the market works effectively and consumers can have confidence in the services that are being provided. To achieve this it is important that firms providing mobile banking services:

- Have a clear strategy and sustainable business model for mobile banking.
- Consider the requirements of the consumer during each stage of product development from design through to distribution.
- Understand the risks to consumers from mobile banking and take appropriate measures to address these, to provide services aligned with the interests of their consumers.
- Test the robustness of their IT systems, including transactional security, thoroughly stress test their products, and store sensitive data securely.
- Provide information to their customers that is clear, fair and not misleading, and appropriately targeting the intended audience.
- Respond to customer complaints and queries in a fair and reasonable manner, treating customers fairly at every stage.

# 2.
# Our initial findings – potential risks

Our discovery work, carried out during 2012, enabled us to identify the potential key risks presented by mobile banking and payments. We asked firms about their future plans for mobile banking, including plans to launch new products or develop existing services further. We were interested to understand how mobile banking featured in firms' strategies and business models.

We also asked about the risks that firms had considered when developing mobile services and the measures that they had taken to reduce these risks.

In general we found that the firms we spoke to in the course of the discovery work had given some thought to the potential risks associated with mobile banking.

It is important to note that the risks highlighted in this report are not exclusive to mobile banking, with many applicable to other products or services that are in the early stages of development. It is also important to recognise that these risks haven't, in most cases, resulted in problems for consumers, but they do have the potential to do so if not suitably addressed.

## Fraud

Mobile banking may present different challenges around fraud compared with established channels such as internet banking. We believe this is a risk for both firms and their customers. While both risks are important, our main interest is the risk of fraud against consumers, because it could result in consumers being unable to access their money or make payments, resulting in financial loss, inconvenience and stress.

We are interested in how firms are considering and mitigating the risk of fraud in relation to mobile banking and what measures they are taking to protect their customers. Understanding the approaches that firms are taking to detect and prevent the risk and impact of fraud will be an important part of our future work on mobile banking.

## Security

One of the most popular ways for consumers to access mobile banking is by downloading a mobile banking application, or app, for their smartphone. While this provides some consumers with a convenient way of managing their money, it can also lead to the risk of malware, which is malicious software. This can occur if a consumer downloads an application that appears to be from a genuine payment provider but is actually malware designed to capture sensitive financial information. Malware is an important risk for firms to consider, as it can result in financial loss and undermine consumer confidence in mobile banking.

Viruses are an associated risk, especially if consumers are not made aware of sensible precautions to take against them. Many of the firms we have spoken to are aware of these potential issues and we have seen firms take steps to manage them. Examples include firms providing clear security information to consumers, issuing warnings to only download applications from official stores and providing anti-virus software.

We are also taking an active role in contributing towards the regulation of mobile banking at the European level by representing the UK at European negotiations on mobile banking security.

## Use of third parties

For firms to successfully provide mobile banking services to their customers, they will be dependent on IT systems, technical expertise and detailed knowledge of the payments system. Many of the firms entering this market are using the specialised services of outsourcing partners.

This leads to the risk that there may be a chain of companies involved in a customer's transaction, resulting in a greater likelihood of a problem occurring. This may also result in complications if a mistake occurs, as it may be difficult to work out who is ultimately responsible for any problems or financial loss experienced by consumers. We want to understand the measures firms are taking to mitigate the risks around third-party arrangements.

## Consumer awareness and understanding

While many of these services are relatively new, there is a greater chance that consumers may encounter difficulties using mobile banking, compared with more traditional services. This could result in consumers making errors, such as paying the wrong recipient or entering an incorrect amount. Mobile phones, with their smaller screens and limited keypad, may make these errors more likely, therefore it is important for us to understand how firms are mitigating this risk. We also want to understand whether firms have appropriate processes in place to resolve mistakes if they do occur.

## Technology risk/interruption to service

Firms delivering mobile banking need robust systems and technology in place. There is a risk that an IT failure could interrupt services, preventing access to mobile banking, limiting customers' access to their money and undermining consumer confidence in these services. The potential impact of this may grow as consumers increasingly rely on mobile banking. We recognise that firms may be under strong commercial pressure to develop and launch products quickly, which could risk services being released without sufficient testing and protection.

## Anti-money laundering systems and controls

For firms to comply with their legal and regulatory requirements they must have systems and controls in place to identify, assess and mitigate the risk of financial crime. Mobile banking and payments are new services for firms and consumers to access and transfer funds. Therefore we need to ensure that firms have proportionate and risk-sensitive systems and controls in place.

From our research, we believe this is especially relevant for mobile banking services that are not linked to the customer's current account. We will consider the extent to which firms should carry out additional checks to verify the identity of the payee and recipient. Mobile banking may also make it challenging for firms to identify and report suspicious transactions.

We have seen firms take measures to prevent the risk of money laundering through mobile banking and we know that having robust systems and controls can be an effective mitigant against such risks. It is important that these risks are adequately mitigated, especially where firms are moving into more advanced forms of mobile banking, such as facilitating overseas payments.

# 3. Next steps

The next stage of our thematic work is to test a sample of firms providing mobile banking services so we can find out whether firms are meeting our expectations and treating their customers fairly. Our sample of firms includes major high-street banks, as well as firms that haven't traditionally provided banking services, to get a broad picture from across the market.

The work will cover a range of areas, including:

- The strategies firms have in place for mobile banking, including understanding firm's decision-making processes and product governance.
- The way firms go about designing their mobile banking products and how they deal with risks arising, including their use of third-party providers.
- Whether firms are treating their mobile banking customers fairly, for example how firms respond to customer complaints and other situations, such as a customer reporting fraud or making a payment in error.
- Whether the information that firms are providing to their customers is clear, fair and not misleading, and whether the content is appropriately aimed at the target audience.
- Whether firms are complying with the key requirements in the Payment Services Regulations.
- How firms are managing risks around fraud, anti-money laundering and security.
- The contingency arrangements in place in the case of a technical failure of the mobile banking product or service.

We expect firms to consider the points we have highlighted and take sufficient steps to address the risks we have outlined. It is important that firms providing these services have appropriate governance in place to assure themselves that they have considered and mitigated these risks.

We aim to conclude our assessment work in late-2013. We will consider our findings alongside what we have learned through our ongoing monitoring of developments in the market and the way in which consumers are using mobile banking. We will report back to the market in the first half of 2014.

Financial Conduct Authority


**PUB REF: 003302**


25 The North Colonnade Canary Wharf
London E14 5HS
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk