The changing regulation around mobile payments

28/09/2016

Financial Services analysis: With approximately 93% of adults owning or using a mobile phone in the UK and the introduction of tokenisation services using near-field communication (NFC) technology, the idea of using mobile devices to pay is becoming increasingly common. Ed Bodey, senior associate at Foot Anstey, and Nikki Johnstone, associate at Paul Hastings, explore the regulatory environment for providers of mobile payment solutions and the commercial challenges likely to influence their development.

What constitutes a mobile payment, and what is the current legal framework around mobile payments?

Nikki Johnstone (NJ): The concept of a mobile payment has been defined by the European Commission in its Green Paper, 'Towards an integrated European market for card, internet and mobile payments' as:

'payments for which the payment data and the payment instruction are initiated, transmitted or confirmed via a mobile phone or device. This can apply to online or offline purchases of services, digital or physical goods'.

The sector therefore covers a broad range of solutions, transaction types and technologies.

The impact of regulation on providers of mobile payment solutions will ultimately depend on whether the provider has a direct relationship with the customer. While the customer relationship has historically been the domain of banks and credit card providers, the emergence of new payment technologies (particularly in the mobile space) is beginning to challenge the status quo.

Mobile payments activities are principally governed by the EU Payment Services Directive 2007/64/EC (PSD 1), which introduced—for the first time—a uniform regime for regulation of payment services applicable across the European Economic Area (EEA). PSD 1 introduced:

- an authorisation regime for 'payment institutions' (PIs), which enables PIs to carry on a range of payment services (eg money remittance, the operation of payment accounts, the execution of payment transactions), with the additional advantage of being able to 'passport' a licence obtained in one country to do business in all other EEA countries without needing to seek fresh local licences, and
- a 'conduct of business' regime governing how payment service providers (PSPs) deal with their customers—they include rules on the information to be provided to customers, fee levels, the speed of execution of payments, and liability for any unauthorised or delayed or failed transactions

PSD 1 has created an environment of largely uniform and coherent regulation across the EEA which, together with the passporting regime, makes it relatively cheap, quick and easy to launch a pan-European payments business. Nonetheless, PSD 1 has its wrinkles and a new Payment Services Directive 2015/2366/EC (PSD 2) is to be implemented on 13 January 2018, which will make a range of changes to PSD 1 and indeed replace it.

What impact will PSD 2 have on mobile payments?

NJ: PSD 2 aims to expand customer protection, enhance cybersecurity and level the playing field between regulated PSPs and currently unregulated providers.

Extension to non-EEA transactions and currencies

While PSD 1 is predominantly limited to transactions taking place entirely within the EEA and in an EEA currency (such as euro or sterling), PSD 2 will extend many of these requirements to payments:

- in other currencies (such as dollars) and/or
- sent between a PSP located in the EEA and one outside of the EEA

New regulated payment services

PSD 2 introduces two new payment services:

- 'payment initiation services', whereby the provider will initiate payments at a customer's request from their account at another PSP (eg Sofort, Trustly), and
- 'account information services', whereby the provider will supply a customer online with consolidated information about their accounts with other PSPs (eg MoneyDashboard)

For the first time, firms providing these services—referred to as third party providers or 'TPPs'—will need to become authorised as PIs and comply with certain conduct of business requirements, including having potential liability for unauthorised and improperly executed transactions. As a quid pro quo, PSPs providing online payment accounts will have to enable their customers to have access to TPPs' services.

Narrowing of exemptions

There was a sense among EU legislators that certain exemptions had been relied on more broadly than intended, resulting in a loss of protection for customers. Accordingly:

- the 'limited network exemption' is tightened, and there is a new obligation to notify the authorities of reliance on the exemption in certain circumstances and
- the 'digital download exemption' has been narrowed, so that it will be limited to certain micro-payments charged to mobile phone bills (or equivalent). Providers will again have to notify the authorities and provide them with annual compliance audits.

There has also been a tweak to the 'commercial agent exemption', which is arguably more of a clarificatory than a substantive change in any case, it seems to signal a desire for e-commerce platforms to rely less on the exemption (The exemptions referred to here are in art 3(b), (k) and (l) of PSD 1 and PSD 2).

A new definition for acquiring

PSD 1 introduced a regulated activity of 'acquiring of payment instruments', which PSD 2 renames the 'acquiring of payment transactions' and defines for the first time as:

'a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee'.

This definition—which departs from the English law understanding of acquiring—may result in certain payments processors currently operating on an unregulated basis having to seek authorisation as a PI in future.

Cybersecurity

PSD 2 will introduce requirements for PSPs to:

- implement a robust risk management framework;
- report security incidents to the authorities and (where an incident may impact their financial interests) also to customers and
- implement 'strong customer authentication' when customers access their accounts online or make electronic payments

'[S]trong customer authentication' requires authentication using at least two of the following elements:

- knowledge (something only the user knows, eg a password)
- possession (something only the user possesses, and which may need to be non-replicable, eg a security token generator on a fob or phone) and/or
- inherence (something the user is, eg biometrics)

The need to implement strong customer authentication poses a particular challenge for mobile purchases.

These requirements largely mirror those guidelines introduced by the European Banking Authority in December 2014 on security of internet payments, albeit that those guidelines do not apply to mobile payments.

Are there any other regulatory or legal issues which need to be considered?

NJ: Quite apart from the performance of payment services, providers will need to have regard to some recent developments in the payments sector, which are likely to shape the regulatory and technological landscape.

The new Payment Systems Regulator (PSR)

Inherent to any mobile payments solution is the clearing and settlement of funds through a 'payment system', eg, BACS, CHAPS, Faster Payments Service and card payment schemes such as Visa and MasterCard.

The PSR was launched in 2014 (under the Financial Services (Banking Reform) Act 2013) in response to concerns about the operation of the payment systems market in the UK. The PSR must, so far as is reasonably possible, act in a way that advances one or more of its payment systems objectives, including the service-user objective, which aims at ensuring that payment systems are operated and developed in a way that takes account of, and promotes, the interests of those who use, or are likely to use, services provided by payment systems.

Among the regulator's powers is the ability to order the provision of direct and indirect access to payment systems and/or to amend the terms of commercial agreements between operators and users of payment systems governing service levels and pricing.

It remains to be seen how the PSR will exercise its powers in practice and the extent to which they will be willing to take action against industry participants.

EU Interchange Fee Regulation (IFR)

The Interchange Fee Regulation (EU) 2015/751 sets rules relating to payment card schemes, including caps on certain interchange fees. The PSR is appointed as the main authority responsible for enforcing the IFR in the UK. It has a range of powers, eg giving directions (including for customer redress), imposing penalties and seeking injunctions. It also provides guidance in relation to the IFR, and has the power to intervene in certain interchange fee disputes between payees (merchants, in particular) and their PSPs.

Certain IFR requirements present interesting challenges for the mobile payments providers, which are likely to have an impact on build:

- removal of the 'honour all cards' rule means that merchants may choose which cards to accept where there are differences in interchange fees
- card schemes cannot prohibit merchants from 'steering' customers towards a particular payment instrument
- customers have the right to choose a 'co-badged' card and to be provided with clear and objective information on all brands available

In a virtualised environment, providers are now required to develop systems which are responsive to the flexibility and information needs of both merchants and consumers in a way which does not substantially reduce the speed and convenience of their solution.

How do you think this area will develop over the coming months and years? Do you have any predictions for the future?

Ed Bodey: Away from legal and regulatory requirements, mobile payments represent a highly competitive marketplace where, while the challenges will not prevent mobile payment's continued adoption, how they are addressed will determine how long it takes.

Diversity

Technology battles in the past have often focussed on two competing interests (eg Betamax/VHS, Blu-Ray/HD-DVD). With mobile payments we see competing interests from merchants, consumers, manufacturers, network providers, banks and new entrants.

From a supplier's perspective, this diversity drives and fosters a sense of competition and innovation. Yet, to a consumer, it can represent confusion and hesitancy, particularly if they themselves are required to make personal investment (eg, in the latest handset or wearable).

The myriad of solutions available such as peer-to-peer payments (Paym, Pingit, Facebook Messenger) in-store app based payments (such as Starbucks' app) and e-wallet NFC solutions (such as Android Pay, Samsung Pay and Apple Pay) leads some commentators to voice concerns that this diversity may actually result in slower adoption by the broader potential user base.

Technology

Potentially less of a hurdle than it was a couple of years ago, discussion in this space has often focussed on the significant investment required by merchants to upgrade existing payment terminals.

Given the growth in NFC contactless payments over recent years, this technology is now more commonplace, although some mobile payments solutions do require bespoke hardware, so, depending on the approach, investment may still be required.

The main challenge here is now ensuring that the majority of the potential user base has the capability to make mobile payments through new or upgraded devices or wearables.

Changing behaviour

Here is perhaps mobile payment's biggest challenge. Recent research suggests that, while an increasing number of us have tried mobile payments, the most common reason given for not making them is that we forget. The challenge is therefore to make it habitual.

History shows that changes in behaviour take time and that we need clear reasons and motivation for making the change. A lot of attention has been on the quicker and more convenient commerce experience to the user, but perhaps that is not enough to convince those who see nothing wrong with cash or cards to make the change. So, as mobile payments evolve, they need to offer us more in terms of user experience and convenience over other existing payment methods.

Security

An awful lot of attention goes into security and, as touched on above, regulatory changes are only emphasising further that focus. At a basic level, given the diversity in the marketplace, one bad headline could cause serious problems for a payment solution, as its user base has a wide variety of alternatives if confidence in one solution is lost.

Yet users themselves still need convincing. Against a backdrop of regular headlines around fraud and digital security, the messages about the benefits and safeguards of mobile payments need to be strong to stand out. Further, companies need to make their solution compelling not just from a security perspective, but also from a use perspective. Make the user take the plunge.

Technology can help offer additional solutions here, and increasing interest in location data and biometrics as part of the security mix shows this. Again, regulation has acknowledged this through the introduction in PSD 2 of the 'strong customer authentication' requirements discussed above.

But do not lose sight of increasing focus on data protection. As much as headlines are made from stories around system security, the Information Commissioner takes an interest from the data perspective and loss of, or unlawful access to, personal data. Regulatory and legal change is happening here too through the introduction of the new General Data Protection Directive in 2018. This makes key changes to the regulatory landscape in this area and so it is important that any decisions taken around data collection and security also factor in new obligations and areas of risk arising through these changes. Never has consumer or regulatory focus been greater in this area than it is now, particularly on the issues of transparency around collection and use, and security.

The future

Various potential avenues of exploration and exploitation of mobile payments stand out:

- possible collaboration between PSPs, TPPs, loyalty schemes and merchants to develop more consumer

focussed, cross market and compelling options

- increasing use of merchant centric, proprietary solutions where the merchant facilitates the payment and is able to offer its own loyalty programme and rewards alongside (thereby enabling it to gain ever greater insight into its customers and to hold greater sway over more areas of the value chain)
- the industry has been struck by the utility of the blockchain and other distributed ledger technology, and this could result in new micro payment solutions and alternative payment networks and
- possible development of new customer-centric cyber security solutions (eg biometrics), particularly for retail purchases

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor