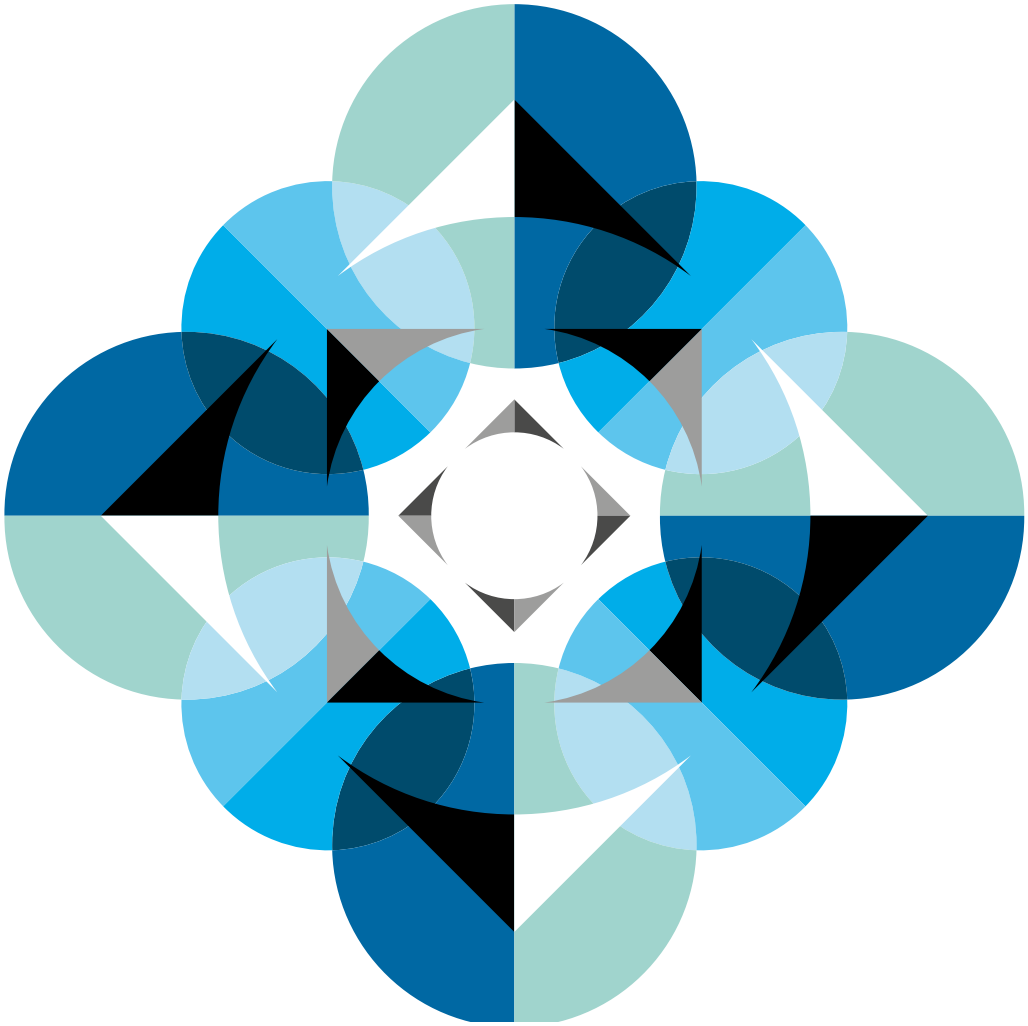
LEWIS SILKIN

The fast growing world of mobile payments - are you on the money?



Inside

Introduction

Your smartphone can already act as your portable office. Now it can replace your wallet too! The world of mobile payments is a fast emerging market that is expected to grow rapidly over the next few years, with some analysts estimating that the global value of transactions over mobile devices will exceed $600 billion by 2016.

The mobile payments market is undergoing rapid and exciting growth that will continue to affect all our lives, both as businesses or consumers. Some recent examples of UK mobile payment initiatives include:

- The launch of the Visa/Samsung "payWave" contactless payment app which was used at the London 2012 Olympics. This allows consumers to make purchases with their Samsung mobile phones and have those purchases charged directly to their Visa accounts;
- Vocalink's imminent "Zapp" payment solution that can be used by consumers through their mobile banking application. This solution will not only allow consumers to purchase items via their mobile phone (using the banks' "faster payments" solution) but also displays the consumer's account balance to the consumer at the checkout;
- The forthcoming launch of "Weve" by EE, O2 and Vodafone, which will offer both mobile wallet and mobile marketing solutions. The mobile wallet solution will enable consumers to transfer their card-based data onto a mobile wallet; and
- The launch of Mastercard's "MasterPass" and Visa's "V.me" both of which offer consumers the opportunity to register payment cards to a 'digital wallet'. Once a consumer has downloaded the respective app and their card numbers have been registered, the consumer is able to pay for items simply by selecting the card to be used and entering their e-mail address and password.

In this inbrief we look at some of the commercial models being used by participants in the mobile payment market and the associated legal and regulatory hurdles that must be considered early in a project lifecycle to ensure adoption of a successful strategy.

Which model is best for you?

The mobile payments market often combines a number of participants.

These normally include the following parties:

- banks issuing credit cards/debit cards and card associations;
- mobile operators;
- retailers;
- device suppliers (including smartphone, point of sale device manufacturers and SIM suppliers); and
- service integrators who can help deliver mobile payment solutions.

These are some of the models that can be adopted:

Bank Model

This model has been adopted by banks issuing credit cards/debit cards (and card associations) who wish to build on their existing networks and deploy mobile payment solutions via bank partners. For example, Barclays' successful "Pingit" solution allows consumers to make payments directly from their mobile phones. NatWest and RBS have also developed the mobile solution "Get Cash" to allow customers to use their mobile phone to withdraw (emergency) money from an ATM.

Collaboration Model

This model has been adopted by banks, card issuers and other credit associations who wish to collaborate with mobile operators and other service providers to provide mobile payment solutions to consumers. For example, "Google Wallet", a digital wallet solution built on NFC technology (currently only available in the US), is a collaboration between a bank (Citi), a card issuer (MasterCard), a mobile operator (Sprint) and a payment processor (First Data).

The model has also been adopted by PayPal and Cardlesspay who have teamed up to develop "mWallet" in the US, which relies on QR codes to enable consumers to make payments to certain merchants, by scanning the QR code. "mWallet" stores credit card and bank account details, as well as PayPal account information.

Closed Loop Model

This model has typically been adopted by retailers and stand alone merchants who wish to create independent, closed-loop payment applications. A good example of this in the UK is Starbucks, which uses a smartphone app to generate a barcode to reload balances, pay for purchases, track spend and award loyalty points. Other retailers such as Pizza Hut, McDonald's and KFC have also launched similar apps in the UK.

Mobile Operator Model

This model has been adopted by mobile operators who wish to act independently, or in collaboration with other mobile operators, to deploy mobile payment applications and value added services. For example, EE, O2 and Vodafone's "Weve" solution or Safaricom's "M-PESA" which allows users to carry out basic banking transactions via their mobile phone. The M-PESA solution has been widely adopted in Kenya and other African countries, as well as Afghanistan and India, where a significant number of the population does not have a local bank.

What are the legal and regulatory hurdles in the UK?

Currently, there is no specific set of regulations that governs mobile payments in the UK. Instead, there are various laws and regulations which market players need to take into account when planning their commercial offering.

Electronic Money Regulations

The Electronic Money Regulations 2011 (EMRs), the Financial Conduct Authority ("FCA") Approach Document and the FCA Perimeter Guidance Manual Chapter 3A (Guidance on the scope of the EMRs) set out a relatively strict authorisation/regulation regime that applies to issuers of e-money in the UK. Non-compliance with the EMRs can result in criminal sanctions.

Credit institutions, credit unions and municipal banks are exempt from the authorisation and registration provisions under the EMRs as they are already subject to authorisation and compliance obligations under other financial services laws. However, they are still subject to various conduct of business requirements in the EMRs.

E-money is defined under the EMRs as monetary value represented by a claim on the issuer that is:

- electronically stored;
- issued on receipt of funds;
- used for the purpose of making payment transactions; and
- accepted as payment by someone other than an issuer.

A person who issues monetary value which can only be accepted by that person is likely to fall outside the scope of the EMRs. Such persons would include retailers who have store loyalty programmes.

The EMRs also set out a number of exemptions. Two key ones are the "limited network" exemption and the "download" exemption. The "limited network" exemption applies where the value is used for purchases on premises of the e-money issuer within a "limited network" of service providers or for a "limited range" of items. The "download exemption" provides an exemption for telco, digital or IT providers who allow goods and services to be paid for with what would otherwise be e-money, delivered and/or used through their respective telecommunication, digital or IT device but who provide services that add value beyond the e-money payment services.

This means, for example, that if a telco, digital or IT provider accepted funds for an item purchased via the device and then transferred those funds to the supplier, the transaction may be caught by the EMRs. However, if the provider provides a value added service, such as allowing the consumer to enjoy the product on their device, it is likely that the transaction would not be considered an e-money transaction for the purpose of the EMRs. For example, if a consumer purchases a cinema ticket using pre-paid credit on a phone and the ticket is then uploaded to the phone, the purchase is likely to fall outside the scope of the EMRs as the ticket can only be accessed via the phone.

Payment Services Regulations

Although issuing e-money is not a payment service itself, a payment service may be required for the issue of e-money. Payment services are broadly defined under the Payment Services 2009 Regulations (PSRs) and include the following activities which carried out as a regular occupation or business activity:

- the execution of payment transactions where the payer's consent (to execute the transaction) is given via any telecommunication, digital or IT device and the payment is made to the telco, IT system or network operator acting only as an intermediary between the payment service user and the supplier of goods/services;
- the operation of payment accounts;
- the execution of payment transactions through a payment card or similar device;
- cash deposits on and withdrawal from a payment account; and
- card issuer, merchant acquiring and money remittance.

The PSRs, the FCA Approach Document and the FCA Perimeter Guidance Manual Chapter 15 (Guidance on the scope of the PSRs) provide the legal framework for the operation of a single market in payment services in the UK and among other things set out an authorisation/regulation regime governing the activities of "Payment Services" providers. Non-compliance with the PSRs can result in criminal sanctions (as with the EMRs).

Similar to the EMRs, credit institutions, credit unions and municipal banks are exempt from the PSRs. Other exemptions also apply. Notably, the PSRs also contain "limited purpose" and "download" exemptions similar to those under the EMRs. There is also a "technical service provider" exemption, which applies to service providers who support the provision of a payment service without acquiring possession of funds, which may include service providers who store and process data, provide security services or provide the communication network.

Consumer Protection

Businesses involved in mobile payments may also need to consider compliance with consumer legislation, including the:

- Consumer Credit Act 1974;
- Unfair Term in Consumer Contracts Regulations 1999;

- E-Commerce Regulations 2002;
- Financial Services (Distance Marketing) Regulations 2004;
- Consumer Protection from Unfair Trading Regulations 2008; and
- Consumer Rights Bill (likely to come into force in 2014).

Data Protection

Privacy issues will be key, as will "ownership" of customers and customer data.

Many existing solutions allow data to be shared among participants involved in providing the solution – whether that is necessary and the purposes for which that data can be used needs careful consideration. One single device may know a consumer's geographic history, social media connections and financial behaviours. This means that consumers may inevitably be more open to identity theft and invasive data collection. It seems likely that as the popularity of mobile payments grows, companies' privacy practices are likely to face increasing scrutiny from the ICO and other regulators.

Businesses involved in mobile payments will therefore need to consider their obligations under privacy legislation, including the Data Protection Act 1998 and the Privacy and Electronic Communications Regulations 2003.

Competition and anti-trust laws

Participants who form collaborations should also have regard to the competition law and anti-trust implications of their proposed model and offering. For example, the EE, O2 and Vodafone joint venture sought advance approval from the European Commission under the EU Merger Regulation in respect of their "Weve" mobile payment solution.

Anti Money Laundering

Mobile payment providers also need to consider whether they need to comply, and how they will comply, with the Money Laundering Regulations 2007. Mobile payment providers will need to ensure that their offerings are not at risk of being used to facilitate money laundering or terrorist financing.

Comment

The mobile payment market is rapidly evolving and has enormous potential. At present, there is no common industry standard or leading solution and so it will be very interesting to see which offerings consumers prefer to adopt. The direction of expansion will undoubtedly be impacted by the regulatory landscape within which these solutions must be offered.

The legal and regulatory framework and requirements are not straightforward, and so it is absolutely vital for businesses to consider these aspects early in the project lifecycle to ensure that the most appropriate model is adopted, especially as some of the relevant laws (such as the Payment Services Directive) are under review and are likely to change.

Some businesses may be able to structure their mobile payment solutions so as to avoid the onerous requirements of the EMRs and PSRs. The scope of the exemptions (especially those in the PSRs) are likely to be revised due to the fact that they have typically been construed too widely in the past, which may present a risk for those businesses that do not factor this risk into account.

Other businesses, such as mobile operators, may seek to avoid the financial implications of the regulations by partnering up with financial institutions. This approach can be a cost efficient way into the market and also help to generate additional consumer confidence in the mobile payment offering.

Businesses who are considering a collaborative venture should be prepared to deal with the contractual and commercial issues that will need to be agreed. These include:

- identifying the contractual framework;
- branding and ownership of the customer facing relationship;
- use of data generated in connection with provision of the mobile payment solution;
- understanding the ownership and use of intellectual property rights involved in creation and provision of the solution;
- apportionment of risk and liability;
- operation of payment flows and indentifying who bears insolvency/bad debt risks; and
- exit principles, including use of customer lists, other data, and intellectual property assets (such as software).

For further information on this subject please contact:

James Gill
Partner
T + 44 (0) 20 7074 8217
james.gill@lewissilkin.com

Owen Watkins
Barrister
T + 44 (0) 20 7074 8222
owen.watkins@lewissilkin.com

Bryony Long
Senior Associate
T + 44 (0) 20 7074 8435
bryony.long@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com