Mobile payments

Technological, contractual and regulatory convergence

October 2015

KEMP LITTLE

KEMP LITTLE

Contents

1	**Introduction**	**2**
2	**What is a mobile payment?**	**3**
3	**Regulatory framework**	**5**
3.1	**Payments-related legislation**	**5**
3.2	**Payment Services Regulations 2009**	**6**
3.2.1	What are payment services?	6
3.2.2	Obligations under the payment services regime	8
3.3	**Electronic Money Regulations 2011**	**9**
3.3.1	What is e-money, and how is it different from other payment services?	9
3.3.2	Obligations under the e-money regime	10
3.4	**What do these pieces of regulation mean for mobile payment models?**	**11**
4	**Other forms of regulation: retail meets financial services**	**13**
4.1	**Data protection**	**13**
4.1.1	Security and authentication	13
4.1.2	Marketing	14
4.2	**Payment systems – the new regulator**	**15**
4.3	**Anti-money laundering**	**16**
4.4	**Data roaming charges**	**16**
5	**Conclusion: convergence and adoption – what next**	**18**

1 Introduction

After years of hype, it is only now that mobile payments – long heralded as a growth area in technology, retail and financial services – are starting to gain traction in a way that most consumers really know about. Until very recently there have been a great many "mobile payment" solutions available but very few of them have taken hold in a way that could be described as mass market, despite the best intentions and intervention of the European legislature.

However, things do now seem to be gaining momentum. In 2014 nine of the major banks launched Paym[1], a service which allows anyone with an account at one of those banks to send money to another user of the service via a smartphone app using only the recipient's mobile phone. More recently, Apple Pay's successful launch in the US was followed up by a UK launch in July 2015. As with various other pieces of technology, it may well be that it is Apple's market reach, ease of use and preternatural ability to pitch a product to the public that turns out to be the real tipping point for mobile payments in a broader sense.

However, it would certainly not be right to think that Apple Pay signifies that the game is won and over. Quite to the contrary, the mobile payments area is much bigger than this section of it: it is an area of convergence, of financial services meeting telecommunications, networks, software, consumer hardware and the full range of ways that a smartphone can collect and transmit data. As such, it is open to a whole range of new market entrants and innovative solutions which will broaden and diversify the payments sector, and has the potential to change the way that retailers and marketers interact with their customer base.

This paper examines the key concepts in the area of mobile payments, the principal regulatory risks and pitfalls involved, and how these are likely to affect the partnerships that will need to be struck between different actors along each mobile payments chain. How the law applies to this sector will necessitate detailed consideration as the sector develops.

[1] http://www.paym.co.uk/?gclid=CI7VvLfIqL4CFQzItAodpDUAew.

2 What is a mobile payment?

The term "mobile payment" is widely used and often misunderstood. At its heart, a mobile payment is any form of payment transaction that in some way involves a mobile phone. More specifically, the European Commission has defined 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".[2] The term therefore covers a broad range of concepts, transaction types and technologies, each of which have different legal ramifications and a different place in the regulatory landscape.

The scope for innovation and development in this area is correspondingly broad, but currently the principal "**payment models**" of mobile payments are:

1. **Mobile at the point of sale.** This involves paying for goods in a shop using a mobile phone, or some aspect of it, as the physical means by which the payment transaction is effected. Typically this will involve an NFC chip ("near field communication" – like an Oyster card or a contactless bank card) which is installed in, or attached to, the mobile phone. It may also involve some form of mobile wallet – a form of prepaid account or prepaid card which is stored on the phone (usually in an app) and can be debited using a combination of the app and the NFC chip or some other messaging technology that interacts with the merchant's payment terminal (e.g. BLE, bluetooth etc.). Apple Pay fits squarely into this category – a transaction consent authentication technology that uses NFC and various pieces of tokenisation to trigger a standard underlying card transaction.

2. **Mobile as the point of sale**. Here a merchant uses their mobile phone or tablet as a form of cash register, using technology such as Square, iZettle or "PayPal Here". This usually involves a piece of hardware which can read payment instruments like credit cards, and interacts with the hardware of the phone and an app which credits a form of account which is held by the merchant. In the case of Square, for instance, a small credit card reader is inserted into the phone by the merchant, and when a payment is made by a customer by swiping the card through the reader, the reader interacts with the app in the phone to send the relevant amount to the merchant's bank account.

3. **Direct carrier billing.** This involves charges being added directly to a mobile phone bill. This is the simplest form of mobile payments and can include, for example, charges for ringtones or car park charges initiated by text.

4. **Closed loop mobile payments.** This involves, for instance, a merchant setting up an app onto which funds are loaded, and those funds are linked to the relevant payment device, e.g. a combination of the app and the NFC chip in

[2] See European Commission's Green Paper "Towards an integrated European market for card, internet and mobile payments", para 2.4, http://eur-lex.europa.eu/legal-content/EN/ALL/;jsessionid=qpPTTnXJVHsRswcFLZwT2nL7LCv6QL1RXWRnwpmmqmCylHhpT8Q4!-461598629?uri=CELEX:52011DC0941.

the phone. Once those funds are used up, further funds can be loaded with a further card payment into the app. The most successful version of this to date is the Starbucks app, reported to have over 13 million active mobile users making more than seven million transactions per week.[3] However, few other businesses have managed to emulate the success of this model.

5. **Mobile payment platform.** This encompasses most of the other (relatively) viable forms of mobile payment, and really means any type of mobile-based payment platform, whether linked to a bank or a third party intermediary. It includes PayPal, Serve, Barclays Pingit and Paym. The majority of these platforms are simply mobile versions of the web-based version of the same service. Crucially, however – and this is a point to which we will return later – they use the phone itself as one of the authentication factors for access.

The one thing that unites all of these payment models is that each of them contains four core elements:

- **a handset ("device");**
- **an account containing the user's funds ("account");**
- **a means of communicating the user's desire to transfer funds ("communication");**
- **a connection to the user's funds account enabling the transfer to take place ("connection").**

Each of the above elements can take multiple forms depending on the payment model. For obvious reasons it is likely that the most successful participants in the mobile payments landscape will be those that already have one or more of the elements in place, thereby removing one of the barriers to entry and encouraging adoption.

[3] http://www.fastcompany.com/3041353/fast-feed/starbucks-mobile-app-payments-now-represent-16-of-all-starbucks-transactions.

3 Regulatory framework

There is currently no legislation which is specific to mobile payments or m-commerce, though mobile has been very much in mind in the drafting of the existing legislation, and there are plans within the European Commission to look at this area in more detail.

One of the interesting aspects of the mobile payments area is that it brings together both:

1. legislation that has been designed to allow new participants from areas outside of traditional financial services into the payments space; and

2. other areas of regulation that were previously only tangentially related to financial services, by virtue of the very fact that new entrants do come from other sectors. This applies in particular to areas of regulation relating to consumers, telecoms and certain aspects of personal data (e.g. location data), which will constitute a regulatory overlay to the financial services core.

The interaction and potential conflicts between these areas are likely to require specific legislative attention as the market develops.

3.1 Payments-related legislation

The main pieces of legislation which affect mobile payments most directly at the moment are:

- The **Payment Services Regulations 2009**,[4] ("**PSRs**"), which are the UK implementation of the Payment Services Directive ("PSD") 2007;[5]

- The proposed **Second Payment Services Directive** ("**2PSD**"),[6] which at the time of writing is under discussion between the European Parliament, the Council of Ministers and the European Commission;[7]

- **The Electronic Money Regulations 2011**,[8]("**2EMR**") based on the second E-Money Directive.[9]

Deciding which of these pieces of legislation will apply to a given situation depends entirely on the particular solution or payment model being implemented. Deciding to whom the legislation applies is a matter of working out exactly where each entity sits

[4] SI 2009/209, http://www.legislation.gov.uk/uksi/2009/209/pdfs/uksi_20090209_en.pdf.
[5] Full title: Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF.
[6] Proposal for Directive of the European Parliament and of the Council on Payment Services in the Internal Market, COM (2013) 547 final 2013/0264 (COD) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0547:FIN:EN:PDF.
[7] http://www.europarl.europa.eu/pdfs/news/expert/infopress/20150505IPR50615/20150505IPR50615_en.pdf
[8] SI 2011/99, http://www.legislation.gov.uk/uksi/2011/99/contents/made.
[9] Directive 2009/110/EC of the European Parliament and the Council of 16 September 2009, on the taking up, pursuit and prudential supervision of the business of electronic money institutions, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547.

in the chain of actors involved in bringing each payment model into action, and whether its function in that chain is itself subject to regulation.

Before looking at the effects of these regulations in section 3.4 below, the following is a brief overview of each piece of legislation.

3.2 Payment Services Regulations 2009

The core of the PSRs is that they provide a platform from which entities other than traditional financial services providers can become authorised as "**payment institutions**" which are allowed to provide and execute "**payment services**", provided that those entities meet certain criteria. Payment services can also be provided by other "**payment service providers**", a category which includes those authorised payment institutions but also credit institutions (e.g. banks, but not credit unions[10]), e-money issuers and central banks (which require no further authorisation). The PSRs apply to the payment services provided by all of them.

So, broadly speaking, a bank implementing a mobile payments solution is already permitted to provide payment services by virtue of its being a credit institution, and therefore needs no further authorisation under the PSRs; however, a mobile network operator that wishes to add payments to its roster of services would require authorisation.

3.2.1 What are payment services?

The definition of "payment services" is broad[11] but encompasses:

- money remittance;
- the operation of payment accounts;
- the execution of payment transactions through a payment card or a similar device; and
- the execution of payment transactions where the payer's consent is given using "any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator" in the capacity of an intermediary between buyer and seller.[12]

Even when these definitions have been understood, though, the question of whether or not the PSRs will apply will still depend on the precise function of the relevant party. For instance, the PSRs do not apply to:

[10] PSRs, Reg 3(3).
[11] For the full definition see the Annex to the Directive.
[12] PSRs, Schedule 1, Part 1, paras (a), (b), (d), (f), and (g).

- The activities of technical service providers that do not at any time hold the funds being transferred.[13] This is likely to be a significant exclusion for many of the participants in the transaction chain who provide purely technological support (including those that provide authentication, data processing and storage services).

- Payment transactions executed "by means of any telecommunication, digital or IT device" where the operator of the same is acting as more than an intermediary i.e. is adding value in some way.[14] This is known as the "**value-add**" exemption. This is currently an important exclusion as it potentially allows certain payment models to escape the need for authorisation/registration if they add some value to the transaction.[15] However, the proposed 2PSD redefines and restricts this exemption so as to create a more level playing field between different payment service providers. The application of the exemption is limited to €50 per transaction and €200 per month, meaning that the exemption will be far more difficult to apply to "normal" payment services.

- Services based on instruments that can be used to acquire goods or services:

  - only on the issuer's premises, or

  - under a commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services.[16]

  This is known as the "limited network" exemption. The scope of "limited network" and "limited range" is far from clear, even though the perimeter guidance issued by the FCA seeks to establish some guidelines.[17] The proposed 2PSD seeks to apply a narrower definition of limited network, citing that the exemption under the first Directive had been used beyond its original purpose,[18] but even if enacted and implemented as proposed it is difficult to see how the new text adds much more clarity.[19]

[13] PSRs, Schedule 1, Part 2, para (j).
[14] *Id*. Schedule 1, Part 2, para (l).
[15] The scope of the "value-add" needed is not entirely clear, but the perimeter guidance provided by the FCA does seem to set quite a low threshold, including the addition of search or distribution facilities. From PERG 15.3, Payment Services Q23: "Adding value may take the form of adding intrinsic value to goods or services supplied by a third party, for instance by providing access (including an SMS centre), search or distribution facilities", http://fshandbook.info/FS/html/handbook/PERG/15/3.
[16] PSRs, Schedule 1, Part 2, para (k).
[17] See PERG 15.5, the "negative scope" section of the perimeter guidance issued by the FCA in relation to the PSRs, Q40 and Q41, http://fshandbook.info/FS/html/handbook/PERG/15/5.
[18] See para 5, Art 3(k) of the Explanatory Memorandum to 2PSD at page 10 of http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0547:FIN:EN:PDF.
[19] The operative text added to Article 3(k) the PSD by 2PSD is underlined as follows, but the same lack of boundaries is still an issue (e.g. what is "limited"?): "services based on specific instruments that are designed to address precise needs that can be used only in a limited way, because they allow the specific instrument holder to acquire goods or services only in in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer or because they can be used only to acquire a limited range of goods or services".

3.2.2 Obligations under the payment services regime

If, having waded through the various parameters of what does and does not constitute a payment service, an entity finds that it is providing a payment service and that the PSRs do apply to it, it will have to comply with a number of obligations imposed by the PSRs. These are split as follows:

- **Authorised payment institutions:** In general, payment institutions (i.e. non-traditional financial services and non-e-money issuers) must go through a process of authorisation,[20] and are subject to requirements regarding holding of capital,[21] safeguarding of funds,[22] record keeping,[23] accounting and audit[24] and notification of outsourcings.[25] Once authorised in any EEA jurisdiction, the payment institution has passport rights and is effectively authorised in any other EEA jurisdiction subject to certain notification requirements.[26]

- **Small payment institutions:** Payment institutions which can demonstrate (amongst other things) that, over the previous year, their total monthly average amount of executed payment transactions is under €3 million, do not have to be "authorised" and can instead apply to be "registered" as a "small payment institution".[27] The regulatory burden on small payment institutions is lighter than for authorised payment institutions, not least in that the requirements referred to in the previous paragraph do not apply to small payment institutions.[28]

- **Provisions common to all payment institutions:** There are a few provisions which apply to both authorised payment institutions and small payment institutions, e.g. that funds held with either for a payment account must only be used for payment transactions.[29]

- **Provisions common to all payment service providers:** There are many other provisions which relate to all payment service providers, i.e. both types of payment institution, plus banks, building societies and e-money issuers etc.[30] These include requirements on information to be provided to payment service users (i.e. consumers),[31] the operation of framework contracts for ongoing/repeated use of payment services,[32] charges for payment services,[33]

[20] PSRs, Regs 6 to 9, 11.
[21] *Id*., Reg 18 and Schedule 3.
[22] *Id*., Reg 19.
[23] *Id*., Reg 22.
[24] *Id*., Reg 20.
[25] *Id*., Reg 21.
[26] *Id*., Regs 23 to 26.
[27] *Id*., Reg. 12.
[28] *Id*., Red. 14.
[29] Part 4 of the PSRs, and specifically Reg 28.
[30] For the full definition see Reg 2.
[31] PSRs, Regs 36-39, 47 and 48.
[32] *Id*., Regs 40-46.
[33] *Id*., Reg 54.

consent for payment transactions,[34] liability for unauthorised transactions[35] and (amongst other things) the time at which transactions are deemed to have occurred.[36]

The scope of the regulations is therefore fairly broad, and in some respects intervenes in areas that might normally be viewed as falling within the remit of contract and/or consumer rights. These requirements, plus the fact that to carry on a payment service without the proper authorisation/registration is a criminal offence,[37] means that consideration of the precise function and nature of each entity within a payment model is crucial.

3.3 Electronic Money Regulations 2011

These regulations govern the issue and use of a particular type of payment instrument, namely e-money. E-money has been regulated in the UK since 2002[38] and traditionally has applied to payment instruments such as pre-paid cards. The advancement of technology has, however, broadened the scope of e-money such that it is now found in a range of different technological solutions, including some of the mobile payment models.

3.3.1 What is e-money, and how is it different from other payment services?

E-money is defined in Regulation 2 of 2EMR as follows:

"electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which—

(a) is issued on receipt of funds for the purpose of making payment transactions;

(b) is accepted by a person other than the electronic money issuer; and

(c) is not excluded by regulation 3.[39]

Regulation 3 contains two express exclusions. These are in essence the same as the "limited network" and "value-add" exemptions under the PSD – but, significantly, not the more restrictive versions set out in the proposed 2PSD.[40]

This in itself raises the issue of whether e-money should be brought within the scope of the larger payment services regime. Not only is it becoming increasingly difficult to discern why there is a need to treat e-money as a separate category of payment

[34] *Id*., Reg 55.
[35] *Id*., Regs 61 and 62.
[36] *Id*., Regs 69-73.
[37] *Id*., Regs 110 and 111.
[38] The transposition of the original E-money Directive (2000/46/EC) made the issuing of e-money in the UK a regulated activity under the Financial Services and Markets Act 2000.
[39] 2EMR, Reg. 2.
[40] See under para 3.2.1 above.

instrument, the above example concerning exemptions shows that the current legislative syncopation between the two regimes is apt to cause confusion.

3.3.2 Obligations under the e-money regime

In any case, the e-money regime closely resembles the payment services regime in many respects. It too is designed to open up a branch of financial services to non-traditional financial services providers, imposing:

- Authorisation requirements[41] for entities which wish to participate, i.e. "authorised electronic money institutions" ("AEMIs");
- a lighter registration regime for smaller entities,[42] i.e. "small electronic money institutions" ("SEMIs");
- requirements on AEMIs and SEMIs regarding holding of capital,[43] safeguarding of funds,[44] accounting and audit,[45] record keeping[46] and notification of outsourcings;[47] but
- no requirement for banks/building societies to obtain authorisation or registration, as they are already included under the broader heading of "electronic money issuer";[48]
- a pan-EEA passporting regime;
- rules governing the carrying out of the financial services transactions in question – here the issuance and redeeming of e-money;[49] and
- criminal sanctions for issuing e-money without being permitted to do so under the 2EMRs.[50]

Nonetheless, for all the similarities, the regimes are different, and require separate consideration, but fortunately their co-existence is recognised within the legislation - "electronic money issuers" are included in the broader term of "payment service provider" under the PSRs and therefore do not require separate authorisation to carry out payment services.

[41] *Id*., Reg 5-9, 11.
[42] *Id*., Reg 12-13.
[43] *Id*., Regs 6(3), 13(5), 15 and 19, and Schedule 2.
[44] *Id*., Regs 20 - 22.
[45] *Id*., Reg 25.
[46] *Id*., Reg 27.
[47] *Id*., Reg 26.
[48] *Id*., Reg 2.
[49] *Id*., Regs 38 - 46.
[50] *Id*., Regs 63 and 64.

3.4 What do these pieces of regulation mean for mobile payment models?

There are of course many effects of a set of regulations as extensive as this, but in broad terms the principal effects appear to be these:

1. The regulatory door is open for non-banks to enter the payments market, in some form or other. As stated above, the obvious candidates are those who already fulfil one of the four elements of device, account, communication and connection. For instance:

    a. The banks are already in an excellent position to take advantage of the opportunities in mobile payments. They already have the accounts and, through existing mobile platforms, the connection, and the likes of Paym add the device and communication elements.

    b. Device providers with deep market penetration also have the communication element already set up (because it's a mobile phone), and so can team up with the banks in order to establish the connection. With Apple Pay, Apple have taken their existing elements of device and communication, but have added the connection to the underlying card transaction.

    c. The mobile network operators have the device, connection and communication abilities already in hand, but to create accounts that they could use for payment services purposes they would need authorisation under the relevant regime.

2. The scope of application of the regulations will depend on the precise nature of the payment activity being facilitated. Those facilitating transactions remotely using some aspect of, or data collected by, a smartphone only as a means of authentication may well need to be authorised as payment service providers. However, where the transaction does not happen remotely but rather by virtue of a connection with a local store of funds through e.g., an NFC chip or app, the facilitating entity is more likely to need authorisation as an e-money issuer.[51]

3. There will be a number of important functions in any mobile payment model which are exempt from authorisation, including many of the technology providers who provide services, hardware and/or software which facilitate payments, but never hold funds themselves. However, even these providers should be aware of the parameters of regulation so as to ensure that they do not inadvertently stray into regulated territory. Significantly, the design of Apple Pay means that Apple

[51] To illustrate the point further, even the use of an NFC chip does not in itself signify e-money, as the chip could also be used as the means of communication to facilitate a transaction from a remotely held account – therefore a payment service rather than e-money. In any case it is likely that more mature mobile payment solutions will involve hybrid models that work both with and without a data connection.

never takes possession of any card details – only a tokenised version thereof – and never hold any funds, meaning that they are in a position to earn significant revenue from the payments industry without having to be authorised as a payment service provider.

4. There may be many mobile payment models – or at least forms of m-commerce – which need no authorisation at all. For instance, the Starbucks app cited above may well not fall within the scope of e-money if the funds on the app are not "accepted by a person other than the electronic money issuer" (i.e. Starbucks itself).[52]

[52] *See* 2EMR, Reg 2, definition of "electronic money".

4 Other forms of regulation: retail meets financial services

Given that mobile payments are an area of convergence, it is natural that otherwise distant or only loosely connected areas of regulation will collide. Some of the more obvious areas likely to be relevant here are those attached to retail, including the various pieces of existing legislation that are about to be merged into the Consumer Rights Act.

Some of the more interesting spheres of regulation in this area are those which are set to be most challenged by the widespread usage of mobile payment methods. They include:

- **data protection** (in particular with respect to security and marketing);
- **payment systems** (as opposed to "payment services");
- **anti-money laundering; and**
- **roaming charges.**

We will now take a look at each of these in turn.

4.1 Data protection

One of the great challenges around mobile payments is of course security; one of its greatest opportunities is marketing – both revolve around personal data and can potentially work together.

4.1.1 Security and authentication

There is of course a challenge for any payments business in carrying out secure and reliable authentication of customers in a way that the customers themselves will trust, but without it becoming so involved or cumbersome that it is off-putting to potential users of new services. A further issue in terms of reliability is that false positives increase costs and create the potential for higher customer drop-off rates i.e. where genuine customers are denied access because the authentication system fails to identify them as the correct individual.

From the consumer's perspective, one of the first questions that people normally ask about mobile payments is "aren't payments less secure if made by mobile", and research suggests that security concerns are the primary factor for consumers in slow adoption of mobile payments. In addition, there can be no doubt that smartphone-based authentication provides a new raft of opportunities for fraudsters. SIM Swap fraud has long since been identified as one method of such opportunity whereby the use of the mobile for one time passcodes and identity verification can be

compromised.[53] As telcos and other new entrants begin to move into the payments market, this area – and the liability for getting it wrong – is likely to be a hot topic: put simply, participants in this market are likely to live and die by their security record.[54]

The biggest reassurance on this front is that mobile has the potential to make security of payments better, not worse. This is because of the abilities that a smartphone has – which a payment card alone does not – to record and transmit sound, vision and location, and to receive instructions remotely. The SIM itself can also be used as an authentication factor, and the iPhone (since the 5S model) has a fingerprint scanner which can be used to the same effect. Each of these abilities can be used to aid in proper verification of identity, and to prevent unauthorised usage of payment capabilities on the phone and in other transaction channels, whilst doing away with at least some of the more cumbersome authentication methods used by web-based services (some of us would happily never use a card reader again!). The result – if the move to mobile is done properly – should actually be more security and fewer hurdles.

There are already more advanced multi-factor authentication solutions that use, for instance, voice biometrics or (in one case at least) proximity correlation checks to help validate international transfers. It is certainly not inconceivable that security solutions could emerge that use the phone's camera to carry out facial recognition functions, fingerprint scanners are already being used to great effect with Apple Pay, and voice biometrics are starting to be used in mainstream retail banking.[55] The key principle is that a phone's ability to transmit different types of data means that multi-factor authentication processes can take place largely in the background, providing for layered security in a manner which will enable payment service providers to take risk-based decisions without the user having to give significant amounts of input and time.

4.1.2 Marketing

The corollary of the above is that:

1. in order for any of these factors to be useful for authentication, the relevant information about the consumer must be collected and stored (so that it can then be compared for authentication purposes later on);

2. those stores of data will be very valuable, very sensitive, and will clearly fall within the realm of personal data legislation; and

3. consents from individuals will be needed to store and use this data for authentication purposes.

[53] http://mybroadband.co.za/news/banking/90503-industry-insider-reveals-truth-about-internet-banking-sim-swap-fraud.html.
[54] See for instance http://www.wired.com/2015/01/mobile-payments-adoption/.
[55] http://www.finextra.com/news/fullstory.aspx?newsitemid=27657.

As well as a challenge, the existence of so much personal data therefore creates a plethora of opportunities for marketing services. Whilst marketers are highly unlikely to benefit from knowledge of voice biometrics (for instance), other aspects of payments via smartphones provide incredible opportunities for segmented/targeted marketing. For instance, the location data emitted by a smartphone could potentially be used by payment service providers to market particular offers in nearby stores; knowledge of payments for certain products could trigger marketing for similar products (think Amazon, for instance).

There is therefore significant potential for the following:

1. Loyalty deals can be encapsulated within mobile payments solutions, which can help to drive adoption of mobile payment solutions. This is how, for instance, the Starbucks app operates, but the concept could be extended far more broadly.

2. Advertising revenue can be generated by payment service providers using mobile as a platform. Localised/personalised advertising is worth a great deal to retailers, and payment service providers will be in an excellent position to capitalise on this.

However, again this depends on sophisticated usage of personal data – and lots of it. In turn, adequate data protection consents will have to be collected from the payment service users (this may be easier said than done), and just as significantly the payment service providers will have to tread a fine line between gathering advertising revenue and tracking/prodding users so much that they find it off-putting and switch to a different payment service. Nonetheless, the potential is there and it will be interesting to see how data protection regulators react as the boundaries of current and evolving law are tested.

4.2 Payment systems – the new regulator

One of the key elements to most payments is that at some point they will involve the use of a "payment system". Unlike a "payment service", the payment systems are the mechanisms via which money is transferred between accounts, and include for instance BACS, CHAPS, LINK, and card payment schemes such as Visa, MasterCard and American Express.

In response to concerns about the operation of the payment systems market in the UK, a new Payment Systems Regulator was introduced in 2014[56] to police the openness of the payment systems market, and in particular the strong network effect of the fact that most payment systems are – for historical reasons – owned by overlapping groups of major banks. The role of the regulator is carried out from within

[56] Under the Financial Services (Banking Reform) Act 2013, which came into effect on 1 March 2014, http://www.legislation.gov.uk/ukpga/2013/33/contents/enacted.

the FCA, with competition law powers to take action against anti-competitive behaviour. Amongst the regulator's powers are:

- the power to order the provision of direct and indirect access to payment systems; and
- the power to amend the terms of commercial agreements between operators and users of payment systems governing service levels and pricing.

The potential benefits of these powers to new entrants to the payments market are obvious. One of the primary objectives of the regulator is to encourage innovation - and it will be interesting to monitor how those powers are enforced in practice.

4.3 Anti-money laundering

A new, fourth anti-money laundering directive came into force on 25 June 2015 and must be implemented by Member States by 26 June 2017. There are concerns that it imposes too high a burden on businesses, and that this may act as a significant barrier to new market entrants, and as a complete barrier to certain payment models (e.g. money remittance to developing countries where KYC checks are simply not practical): it is one thing to open the payments market up to new entrants, but on the face of it such an opening is of little use if the AML compliance burden makes it simply too expensive or cumbersome for all but a few big players to comply.

One of the major issues for any emerging service is adoption, and so on the face of it this is an area where the banks have a huge head start over new entrants. Western consumers are culturally used to the idea of visiting a branch with a collection of official documents, but it is not realistic to expect that consumers will be prepared to go through the same processes to sign up to a new digital service unless it offers very significant advantages over the service offered by their existing bank.

However, a number of rapidly growing alternative payment service providers have made use of the reliance principle in existing anti-money laundering legislation (which is preserved in the new directive), using data from alternative sources including financial institutions and credit checking agencies to satisfy the legal identification requirements without incurring significant administrative burden for the user. It is interesting to compare this scenario with other developments in the KYC industry, where certain companies have for some years been providing data collection services to major banks in respect of standard KYC information. Could a similar approach be used for consumers in future?

4.4 Data roaming charges

On 30 June 2015 the European Commission announced with palpable excitement that an agreement had been reached between the Commission, the European Parliament and the Council of Ministers to legislate for the abolition of roaming

charges across the EU, for voice, text and mobile data access.[57] Whilst this will not become binding law until 15 June 2017, the implications for mobile payment services on an international scale are clear: if data access is too expensive abroad, it is unlikely that consumers will choose to use payment methods relying on data access anywhere outside their home country. The move is therefore a significant plus for those with plans in this space.

[57] http://www.europarl.europa.eu/news/en/news-room/content/20140331IPR41232/html/Ensure-open-access-for-internet-service-suppliers-and-ban-roaming-fees-say-MEPs.

5 Conclusion: convergence and adoption – what happens next

Adoption – as with any new technology – will be driven by whether or not the technology provides an incentive to adopt: some new advantage, convenience or reward.

For the banks this is easy – they have the networks, the card details (obviously), the infrastructure, the trusted brand – all they need to do is add the functionality of mobile platforms to their existing armoury of ways to access and use an account.

As noted above, the network operators are also in a very strong position, as they too are already in possession of a number of the elements necessary to complete the package. It is notable that there have been a few tie-ups between banks and mobile network operators, and further tie ups would not be surprising. Equally, some network operators are looking to become banks.[58]

For others to enter the market they have to offer something that the banks and network operators don't have. One obvious area is the international transfer market, where the traditional banks are simply not set up in a way which facilitates international money transfers without the cost of the transaction fee having a significant impact on the value of the transfer itself, and payment service providers such as WorldRemit and TransferWise have made significant inroads in this space. Other obvious market entrants are those who have the card details already in place, thereby removing one of the hurdles for adoption which might otherwise engender a higher drop-off rate.

But there are others too, and it is again notable that probably the most well-known area of mobile payments at the time of writing is Apple Pay, which is not a payment service at all but rather a means of authentication to facilitate a payment service. If anything, this accentuates the fact that there is a wealth of opportunity in this area, not only for emerging payment service providers themselves, but also for two very significant branches of potential participants. The first is the broad spectrum of service providers that provide support for mobile payments, such as software development, security, data collection and manipulation, back-up, marketing and payment systems; the second and by no means any lesser is the retailers and advertisers who can use elements of mobile payments for marketing, loyalty schemes, data analysis and customer value-add services.

Each actor in the mobile payments area will need to be careful of its place in the regulatory landscape. Contracting in this area will be complex, entailing a myriad of partnerships involving financial services, software, hardware, networks, branding, telecoms and data, and with an ever watchful eye on the boundaries and requirements of the various regulatory regimes. As areas of convergence go it is almost unprecedented – and the area is all the more interesting for it.

[58] http://www.reuters.com/article/2015/07/24/orange-bank-idUSL5N10446C20150724.

For more information contact:

Chris Hill
Partner, Commercial Technology
+44 (0) 20 7710 1636
chris.hill@kemplittle.com