KEMP LITTLE

Mobile payments: technological, contractual and regulatory convergence

Annual update
January 2017

If your business depends on technology, you can depend on us _

KEMP LITTLE

Mobile payments: technological, contractual and regulatory convergence

Scope of this note

After many years of promise, mobile payments are finally starting to gain traction in the mass market. In July 2016 it was reported that a study had found that smartphones accounted for a greater proportion of web-shopping traffic than more standard computers. Services such as Apply Pay, Samsung Pay and Paym are widely known, and there are now several mobile-only banks that use mobile technology to full effect in providing financial services that could previously only be provided by retail banks with a vast branch network.

However, the mobile payments sector is much bigger than pure payments. It is an area of convergence, of financial services meeting telecommunications, networks, cybersecurity, biometrics, software, consumer hardware and all the 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 that will broaden and diversify the payments sector, and is changing the way that retailers and marketers interact with their customer base.

This note 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.

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 follows:

"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".

(European Commission: Green Paper: Towards an integrated European market for card, internet and mobile payments.)

The term therefore covers a broad range of concepts, transaction types and technologies, each of which has 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:

- 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 (near field communication – as used in e.g. contactless bank cards) chip which is installed in, or attached to, the mobile phone. It may also involve some form of mobile "wallet", that is, 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 (for example, BLE or bluetooth). Apple Pay fits squarely into this category as a transaction consent authentication technology that uses NFC and various pieces of tokenisation to trigger a standard underlying card transaction.

- Mobile as the point of sale. Here a merchant uses its 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 that can read payment instruments like credit cards, and interacts with the hardware of the phone and an app that 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.
- Direct carrier billing. This involves charges being added directly to a mobile phone bill. This is the simplest form of mobile payment and can include, for example, charges for ringtones or car park charges initiated by text.
- Closed loop mobile payments. This involves, for example, a merchant setting up an app onto which funds are loaded, and those funds are linked to the relevant payment device, for example, a combination of the app and the NFC chip in 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 (by Fast Company) to have over 13 million active mobile users making more than seven million transactions per week. However, few other businesses have managed to emulate the success of this model.
- 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, they use the phone itself, and/or authentication data gathered through the phone, 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.
- An account containing the user's funds.
- A means of communicating the user's desire to transfer funds.
- A connection to the user's funds account enabling the transfer to take place.

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.

Regulatory framework

There is currently no legislation specific to mobile payments or m-commerce. However, 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 the following:

- Legislation that has been designed to allow new participants from areas outside traditional financial services into the payments space.
- Areas of regulation that were previously only tangentially related to financial services, simply because new entrants come from other sectors. This applies in particular to areas of regulation relating to consumers, telecoms and certain aspects of personal data (for example, location data), which constitute a regulatory overlay to the financial services core.

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

Payments-related legislation

The principal pieces of legislation that affect mobile payments most directly are the following:

- The Payment Services Regulations 2009 (SI 2009/209) (PSRs), which are the UK implementation of the Payment Services Directive (2007/64/EC) (PSD). It is anticipated that the PSRs will be amended take into account the second Payment Services Directive (below).
- The second Payment Services Directive (2015/2366) (PSD2), entered into force in the European Union on 12 January 2016, which will repeal the PSD. Member states have two years to implement PSD2 into national law by 13 January 2018..
- The Electronic Money Regulations 2011 (SI 2011/99) (2EMR), based on the second Electronic Money Directive (2009/110/EC) (2EMD).

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 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 (see What does this regulation mean for mobile payment models?), the following is a brief overview of each piece of legislation.

Payment Services Regulations 2009 (subject to amendments, see PSD2 below)

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" that 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". This includes those authorised payment institutions but also credit institutions (for example, banks, but not credit unions (regulation 3(3), PSRs)), e-money issuers and central banks (which require no further authorisation). The PSRs apply to the payment services provided by all of them.

So 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 to implement a mobile payments solution (although it may require an extension of its Prudential Regulation Authority (PRA) permission). However, a mobile network operator that wishes to add payments to its roster of services would require authorisation.

What are payment services?

The definition of "payment services" is broad but encompasses the following:

- Money remittance.
- The operation of payment accounts.
- The execution of payment transactions though a payment card or a similar device.
- 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.

(Paragraph 1(a), (b), (d), (f) and (g), Schedule 1 PSRs.) (For the full definition, see the Annex to the PSD.)

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

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

- The activities of technical service providers that do not at any time hold the funds being transferred (paragraph 1(j), Schedule 1, PSRs). 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, that is, is adding value in some way (paragraph (l), Schedule 1, PSRs). This is commonly known as the "value-add" or the "digital" exemption. This is currently an important exclusion as it potentially allows certain payment models to escape the need for authorisation or registration if they add some value to the transaction. (The scope of the "value-add" needed is not entirely clear, but the perimeter guidance provided by the Financial Conduct Authority (FCA) does seem to set quite a low threshold, including the addition of search or distribution facilities. PERG 15.3, Payment Services Q23 says: "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".) However, the proposed PSD2 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 EUR50 per transaction and EUR200 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.

(Paragraph 1(k), Schedule 1, PSRs.)

This is known as the "limited network" exemption. The scope of "limited network" and "limited range" is far from clear, even though the FCA has issued perimeter guidance (PERG 15.5, Q40 and Q41).

Obligations under the payment services regime

If an entity is providing a payment service and the PSRs apply, it will have to comply with a number of obligations imposed by the PSRs. These are as follows:

- Authorised payment institutions. In general, payment institutions (that is, non-traditional financial services and non-e-money issuers) must go through a process of authorisation (regulations 6 to 9 and 11, PSRs), and are subject to requirements regarding:
  - holding of capital (regulation 18 and Schedule 3, PSRs);
  - safeguarding of funds (regulation 19, PSRs);
  - record keeping (regulation 22, PSRs);
  - accounting and audit (regulation 20, PSRs); and
  - notification of outsourcings (regulation 21, PSRs).

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 (regulations 23 to 26, PSRs).

- Small payment institutions. Payment institutions that can demonstrate (among other things) that, over the previous year, their total monthly average amount of executed payment transactions is under EUR3 million, do not have to be "authorised" and can instead apply to be "registered" as a "small payment institution" (regulation 12, PSRs). 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 (regulation 14, PSRs).
- Provisions common to all payment institutions. There are a few provisions that apply to both authorised payment institutions and small payment institutions, for example, that funds held with either for a payment account must only be used for payment transactions (Part 4, PSRs, specifically regulation 28).
- Provisions common to all payment service providers. There are many other provisions that relate to all payment service providers, that is, both types of payment institution, plus banks, building societies and e-money issuers and so on (for the full definition of "payment service provider", see regulation 2 of the PSRs). These include requirements on:
  - Information to be provided to payment service users, that is, consumers (regulations 36-39, 47 and 48, PSRs).
  - The operation of framework contracts for ongoing or repeated use of payment services (regulations 40-46, PSRs).
  - Charges for payment services (regulation 54, PSRs).
  - Consent for payment transactions (regulation 55, PSRs).
  - Liability for unauthorised transactions (regulations 61 and 62, PSRs).
  - The time at which transactions are deemed to have occurred (regulations 69-73, PSRs).

The scope of the PSRs is therefore fairly broad, and in some respects intervenes in areas that might normally be viewed as falling within the remit of contract or consumer rights. These requirements, plus the fact that to carry on a payment service without the proper authorisation or registration is a criminal offence (regulations 110-111, PSRs), means that consideration of the precise function and nature of each entity within a payment model is crucial.

Second Payment Services Directive (PDS2)

The PDS2 is intended to cover some of the shortcomings of the PSD and importantly, to

enhance consumer protection, promote innovation and improve the overall security of payment services. The policy makers have aspirational aims of levelling the playing field for payment service providers as technology continues to improve and provide new opportunities within the market. Some of the exemptions once available to mobile payment service providers have been tightened with significant ramifications for those impacted.

What's new in the PSD2?

1. Narrowing the scope of the PSD exemptions

The PSD sets out a number of exemptions applicable to payment service providers, which could be applied differently in each member state. Therefore, one of the key aims of the PSD2 is to clarify and limit the scope of the exemptions given in the directive as follows:

- Commercial Agents Exemption. The PSD2 narrows the scope of this exemption to apply to only those commercial agents that act solely for the payer or the payee in a payment transaction. This exemption no longer applies to commercial agents acting on behalf of the payer and the payee in a single payment transaction,
- Limited Network Exemption. The limited network exemption in the PSD did not sufficiently restrict the payment activities carried out within a specific network on the basis that it was being used for significant payment volumes and values, and consumers were being offered a huge number of different products and services. Under the PSD2, the following payment activities fall within the limited network exemption:
  - the purchase of goods or services within a specific retailer or retail chain, whereby the companies involved have established contractual relationships via a commercial agreement governing a single payment brand which is shown at the point of sale;
  - the purchase of a very limited range of goods or services, such as where the such goods or services are limited to a closed number of functionally connected items;
  - a payment instrument for the acquisition of goods or services that is regulated by national or regional public authority for specific social or tax purposes.

The PSD2 provides some examples of the types of payment instruments covered by the limited network exemption, including: store cards, fuel cards, membership cards, public transport cards, parking ticketing, and meal vouchers.

- Electronic Communications Networks (ECNs) or Services (ECSs) Exemption. The "value-add" or "digital" exemption as set out in the PSD and the PSRs lacked legal certainty for operators and consumers. The PSD2 provides clarity by stating that the exemption will apply only in respect of payment transactions by ECNs or ECSs in respect of purchases of digital content, voice-based services, and e-tickets, provided that:
  - the value of any single transaction does not exceed €50; and
  - the cumulative monthly value for an individual subscriber (whether pre-funded or not), does not exceed €300.

2. Introducing two new categories of payment services

The PSD2 broadens the scope of its application by detailing two additional categories of payment services that will now be caught under the directive:

- Account information services. Defined in the PSD2 as "an online service to provide consolidated information on one or more payment accounts held by the payment service

user with either another payment service provider or with more than one payment service provider".

- Payment initiation services. Defined in the PSD2 as "a service to initiate a payment order at the request of the payment service user with respect to a payment account held as another payment service provider".

For a more comprehensive guide to the PSD2, please see here.[1]

EBA's final guidelines on the security of internet payments

The European Banking Authority (EBA) published its final guidelines on the security of internet payments (SIP Guidelines) on 19 December 2014. The SIP Guidelines were later implemented on 1 August 2015, but are not legally binding on member states, competent authorities and financial institutions. The FCA, along with similar authorities in other jurisdictions throughout Europe, has voiced its inability to comply on the basis that it does not have the legal authority to force compliance of all payment service providers in the UK.[2]

The SIP Guidelines have a wide scope of application and apply to any provider of payment services offered via the internet. However, not all types of payments are caught by the SIP Guidelines, and some exceptions apply:

- What types of payments are caught? Card payments (including virtual cards and those used as part of a 'wallet solution'); credit transfers; e-mandates (including the act of issuing and amending direct debits); and e-money (transfers between two e-money accounts).
- What types of payments are excluded? Other internet services provided by a PSP via its payment website (e.g. e-brokerage and online contracts); payments where instructions are given by post, telephone order, voice mail or using SMS; mobile payments other than browser-based payments; credit transfers where a third party accesses the customer's payment account; and payment transactions made by an enterprise via dedicated networks.

There are three categories of guidelines, including:

- General control and security environment:
  - Governance – requiring clear responsibility and reporting lines to be established;
  - Risk assessment – to be carried out before a payment service is launched and later once launched;
  - Incident monitoring and reporting – to management, regulators and law enforcement;
  - Risk control and mitigation – the requirement for layers of defences if one layer does not work; and
  - Traceability – a requirement for all transactions and e-mandates to be traceable.
- Specific control and security measures:
  - Initial customer identification, information – know your client and anti-money laundering checks;
  - Strong customer authentication – to ensure protection, see below for the requirement;
  - Enrolment for, and provision of, authentication tools and/or software delivered to the customer – customer's on-boarded in a secure environment;

1 https://uk.practicallaw.thomsonreuters.com/Document/Id20ed8a25e6311e698dc8b09b4f043e0/View/FullText.

2 https://www.fca.org.uk/firms/security-internet-payments-eba-guidelines

- Log-in attempts, session time out, validity of authentication;
- Transaction monitoring – to detect and block fraud; and
- Protection of sensitive payment data – protecting data when it is stored, processed and transmitted.

- Customer awareness, education and communication:
  - Customer education and communication – a requirement to provide a minimum of one secure channel of communication with customers;
  - Notification, setting of limits – in respect of payments; and
  - Customer access to information on the status of payment initiation and execution – a requirement to provide customers with the necessary confirmation of payments.

EBA consults on the draft the Regulatory Technical Standards in respect of strong customer authentication and common and secure communication

During the three months ending 12 October 2016, the EBA invited comments on its proposed draft Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure communications. The EBA received a large number of responses to the draft text, which it should assess before producing the final RTS by the deadline of 13 January 2017 as set out in PSD2. As a result of the EBA's limited resources to consider such responses, the EBA announced on 29 November 2016 that it expects to publish the final RTS "a month or so later than the deadline of 13 January 2017".

Strong customer authentication The EBA defines SCA as:

"for the purpose of these guidelines, a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence:

(ii) something only the user knows, e.g. static password, code, personal identification number;

(iii) something only the user possesses, e.g. token, smart card, mobile phone;

(iv) something the user is, e.g. biometric characteristic, such as a fingerprint.

In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s).

At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet.

The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data."

(Paragraph 12, Title I – Scope and definitions, emphasis added)

The introduction of a procedure requiring "two or more" elements codifies multi-factor authentication processes which are increasingly implemented by many companies as a security feature in any event. Examples of the factors used that are particularly relevant to the mobile space include:

- geolocation;
- spending pattern and machine learning;
- voice biometrics
- proximity correlation checks to help validate international transfers;
- fingerprint scanners (now standard in many smartphones);

- movement tracking (typing on a keyboard, moving a mouse or touching a mobile phone or tablet screen);
- iris scanning; and
- facial recognition using a 'selfie'.

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. This provides for layered security in a manner that could enable payment service providers to take risk-based decisions without the user having to give significant amounts of input and time.

Electronic Money Regulations 2011 (2EMR)

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 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.

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

E-money is defined 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." (Regulation 2, 2EMR).

What is excluded from 2EMR?

Regulation 3 contains two express exclusions:

- Limited Network Exemption. The 2EMR do not apply to a payment instrument holding a stored monetary value that may only be used to purchase goods or services from the issuer of such payment instrument, or used to purchase a limited range of goods or services from a limited network of providers who have entered into a commercial agreement with the issuer to be part of the limited network.
- Telecoms, Digital or IT Device Exemption. Also exempt under 2EMR is the use of a monetary value to purchase goods or services via any telecommunication, digital or IT device, where such goods or services are delivered to or used through the telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator is not just an intermediary between the payee and supplier of the goods or services (this is very similar to the value-add or digital exemptions under the PSRs),

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

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 the following:

- Authorisation requirements (regulations 5-9 and 11, 2EMR) for entities that wish to participate, that is, "authorised electronic money institutions" (AEMIs).
- A lighter registration regime for smaller entities (regulations 12-13, 2EMR), that is, "small electronic money institutions" (SEMIs).

- Requirements on AEMIs and SEMIs regarding holding of capital (regulations 6(3), 13(5), 15 and 19, and Schedule 2, 2EMR), safeguarding of funds (regulations 20-22, 2EMR), accounting and audit (regulations 25, 2EMR), record keeping (regulation 27, 2EMR) and notification of outsourcings (regulation 26, 2EMR).
- 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) (regulations 38-46, 2EMR).
- Criminal sanctions for issuing e-money without being permitted to do so under the 2EMR (regulations 63-64, 2EMR).

There is no requirement for banks or building societies to obtain authorisation or registration, as they are already included under the broader heading of "electronic money issuer" (regulation 2, 2EMR).

Nonetheless, for all the similarities, the regimes are different, and require separate consideration. 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.

What does this regulation mean for mobile payment models?

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

- 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 services such as Paym add the device and communication elements.
- Device providers with deep market penetration also have the communication element already set up (because the device is a mobile phone), and so can team up with the banks to establish the connection. For instance, with Apple Pay, Apple have taken their existing elements of device and communication and added the connection to the underlying card transaction.
- 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 (unless their activities were to fall within one or more of the exemptions).

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 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, for example, an NFC chip or app, the facilitating entity is more likely to need authorisation as an e-money issuer. 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.

There will be a number of important functions in any mobile payment model that are exempt from authorisation, including many of the technology providers who provide services, hardware or software that facilitate payments, but never hold funds themselves. For example, the design of Apple Pay means that Apple never takes possession of any card details, only a tokenised version of them, and never hold any funds, meaning that it is in a position to earn significant revenue from the payments industry without having to be authorised as a payment service

provider.

As such, yhere may be many mobile payment models, or at least forms of m-commerce, that need no authorisation at all. For instance, the Starbucks app 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" (that is, Starbucks itself) (see the definition of "electronic money" in regulation 2 of 2EMR). However, such "non-payments providers" should be aware of the parameters of regulation so as to ensure that they do not inadvertently stray into regulated territory.

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 have been merged into the Consumer Rights Act 2015.

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 the following:

- Data protection (in particular with respect to security and marketing).
- Payment systems (as opposed to "payment services").
- Anti-money laundering.
- Roaming charges

Data protection

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

Security and authentication

It is a challenge for any payments business to carry 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, that is, where a genuine customer is denied access because the authentication system fails to identify him 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 have been the primary factor for consumers in slow adoption. 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: participants in this market are likely to live and die by their security record. However, mobile actually 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. Each of these abilities can be used to aid and improve verification of identity, and to prevent unauthorised usage of payment capabilities on the phone and in other transaction channels, while doing away with at least some of the more cumbersome authentication methods used by web-based services (such as card readers). The result, if the move to mobile is done properly, should actually be more security and fewer hurdles to access.

Marketing

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). Those stores of data will be very valuable, very sensitive, and will clearly fall within the realm of personal data legislation. Consents from individuals will therefore be needed to store and use this data for authentication purposes.

The existence of so much personal data creates a plethora of opportunities for marketing services. While marketers are unlikely to benefit from knowledge of voice biometrics (for instance), other aspects of payments via smartphones provide incredible opportunities for segmented and 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; and knowledge of payments for certain products could trigger marketing for similar products.

Therefore, there is significant potential for the following:

- Loyalty deals can be encapsulated within mobile payments solutions, which can help to drive their adoption. This is how, for example, the Starbucks app operates, but the concept could be extended far more broadly.
- Advertising revenue can be generated by payment service providers using mobile as a platform. Localised or personalised advertising is worth a great deal to retailers, and payment service providers will be in an excellent position to capitalise on this.

However, this depends on sophisticated usage of personal data. In turn, adequate data protection consents have to be collected from the payment service users (this may be easier said than done). The payment service providers will also have to tread a fine line between gathering advertising revenue, and tracking or 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.

Payment systems 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", a payment system is the mechanism via which money is transferred between accounts, and includes, for example, 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 (under the Financial Services (Banking Reform) Act 2013) to police the openness of the payment systems market, and in particular the strong network effect of the fact that most payment systems are owned by overlapping groups of major banks. The role of the regulator is carried out from within the FCA, with competition law powers to take action against anti-competitive behaviour. Among the regulator's powers are the following:

- The power to order the provision of direct and indirect access to payment systems.
- 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. To date the regulator has focussed on payment infrastructures and indirect access to payments.

Anti-money laundering

The Fourth Money Laundering Directive (2015/849/EU) (4MLD) came into force on 25 June 2015 and under the initial proposal must be implemented by member states by 26 June 2017. The European Commission published the Fifth Money Laundering Directive (5MLD) on 5 July 2016, including within it provisions the European Commission proposed to bring forward the

transposition date of 4MLD to 1 January 2017 to enhance the efficiency of the current regime before 5MLD comes into force. The European Committees on Economic and Monetary Affairs, and Civil Liberties, Justice and Home Affairs are scheduled to vote on the draft 5MLD on 9 February 2017, when it may become clearer if the new transposition date of 1 January 2017 for 4MLD is accepted. Member states have expressed concerns about the proposed change to the transposition date. There are concerns too that 4MLD generally 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 (for example, money remittance to third world countries where KYC ("know your customer") checks are simply not practical).

One of the major issues for any emerging service is adoption. On the face of it this is therefore 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). They use 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. Alternatively, however, better use of existing data sources combined with e.g. facial recognition technology opens up the possibility that even the initial, cumbersome in-branch KYC checks may not be needed, and this is the approach being taken by some of the mobile-only banks such as Atom, Monzo and Monese.

Finally on AML, providers of certain e-money products may find themselves relieved of the customer due diligence burden if member states take advantage of the exemptions that can be granted to particular e-money products, including if:

- the e-money product;
- is not reloadable, or it has a monthly limit of €250 for payment transactions and such transactions are restricted to a specific member state; or
- is used solely and exclusively to purchase goods or services; or
- cannot be funded with anonymous e-money; or
- the maximum amount stored does not exceed €250, or €500 if such amount is limited to use in a specific member state; or
- sufficient monitoring of transactions or business relationships is carried out by the e-money issuer to ensure unusual or suspicious transactions are detected.

The European Commission issued a proposal to bring virtual currency exchanges and wallet providers into the scope of 4MLD, meaning that providers of these payment instruments will have to undertake customer due diligence checks. It is predicted that this is just one of a number of regulations that may affect fintechs and digital currency activities in the future.

Data roaming charges

On 25 November 2015 the European Parliament adopted Regulation (EU) 2015/2120,[3] which seeks to abolish roaming charges across the EU, for voice, text and mobile data access (Roaming Regulations)4. As part of the [Roaming Regulations], the European Commission is tasked with devising a 'fair use policy' to prevent potential abuse by consumers who may look

3 http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015R2120

4 https://uk.practicallaw.thomsonreuters.com/Document/If852173393f811e598dc8b09b4f043e0/View/FullText.html?transitionType=SearchItem&contextData=(sc.Search)

to take out their mobile contract with a provider outside of their home country to benefit from a monthly lower rate. A 'fair use policy' is likely to open up access to affordable mobile data services for users throughout the European Union, but not completely abolish roaming charges altogether. However, it's currently unclear at the time of writing this how Brexit will impact these imminent changes, but one thing for sure is that the Roaming Regulations will come into force before the UK is anticipated to leave the EU, and to subsequently re-impose roaming charges on consumers is likely to prove extremely unpopular. The abolition of such roaming charges is likely to make mobile payments solutions – many of which require some form of data connection - more reliable across a wider geographical area, which increases their chance of more widespread adoption.

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 it, in the form of some new advantage, convenience or reward.

For the banks this is easy. They have the networks, the card details, 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.

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.

For others to enter the market they have to offer something that the banks and network operators do not have. One obvious area is the international transfer market, where the traditional banks are not set up in a way that facilitates international money transfers without the cost of the transaction fee affecting the value of the transfer itself. 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 notable that probably the most well-known area of mobile payments at the time of writing is still 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 opportunities 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 are the retailers and advertisers who can use elements of mobile payments for marketing, loyalty schemes, data analysis and customer value-add services.

Chris Hill
Commercial Technology Partner

+44 (0) 20 7710 1636
chris.hill@kemplittle.com