International Telecommunication Union

GSR 2013 Discussion Paper

DIGITAL TRANSACTIONS IN TODAY'S SMART SOCIETY

Work in progress, for discussion purposes

Comments are welcome!

Please send your comments on this paper at: gsr@itu.int by 19 July 2013.

TABLE OF CONTENTS

1 DIGITAL TRANSACTIONS IN TODAY'S SMART SOCIETY

Author: William Delylle, Nick Seeley and Igor Plahi, Greenwich Consulting

Introduction

There remains considerable enthusiasm for the mobile payments industry with a rarely challenged view amongst industry commentators that there will be rapid growth in mobile payments around the world, and there are compelling reasons to agree.

The number of service launches is accelerating, breadth and sophistication of services offered widening, and volume of transactions have indeed grown at a rapid pace. And in the majority of cases there are clear and real benefits to users – services are meeting a real customer need, not one dreamt up in R&D labs or marketing meetings. However a reality sinking in is that success is far from a given. Not all launches have taken off and in fact a large number have struggled to meet their albeit high expectations.

There remain barriers to adoption on the user side in spite of clear benefits. On the supply side there are challenges characteristic of an emerging industry – the market is fragmented, there are a lack of industry standards, and providers are still experimenting with the best business model to adopt.

Also, crucially, providers can find themselves in a tangle of regulation. Regulatory frameworks may offer an enabling and safe environment for services to grow, but can also stifle innovation and the commercial viability of services, or be conspicuous in their absence creating uncertainty for users and providers. While many of the issues facing the industry will be met by the market, the role of regulators will also be a defining factor in the industry's success.

Directed at telecoms regulators, this paper also covers issues that more traditionally would fall under the remit of banking regulators such as payment security. This is a necessary inclusion with many services around mobile payments falling out with existing regulatory frameworks and the roles of regulators, in some though not all countries, yet to crystallise – telecoms regulators need to be aware of these issues to advise operators, but also be ready to act on them as required. References to 'regulators' in this paper effectively refers to *telecoms and banking regulators* recognising that how this is ultimately organised will vary by market.

The key challenges for regulators are:

- Having a clear understanding on the current state of services and challenges faced, and likely developments based on experiences in their own and other markets
- Clarifying their own roles and that of other regulatory bodies, and being able to communicate this to providers
- Developing or supporting the development of regulatory frameworks that ensure services take place in a secure and safe environment
- Also, ensuring regulation creates an enabling environment for services and adoption to grow

The rest of this paper is organised around how regulators can meet these challenges: Section 2 sets the context for policy making and regulation, Section 3 provides an overview of current services and how they are delivered as well as likely developments in future, Section 4 outlines the key challenges faced and Section 5 sets up a discussion on the regulation of services.

1 Context for Policy Making and Regulation

1.1 Market and Regulatory Environment

For telecoms regulators it is important to have a clear understanding of markets they are overseeing, to be clear on their role and where it sits in overall regulation of the market, and to develop a regulatory framework as required that balances security with creating an enabling environment. There are a number of important considerations about both the nature of the market and existing regulatory environment for digital transactions that should be recognised and taken into account:

Markets at early stage of development: Mobile payments are still at a relatively early stage of development in most regions. It is difficult to anticipate how these services will develop as part of current regulation, and equally there is a risk that being too prescriptive could hinder innovation.

Differences between regional markets: Markets vary in the nature and needs of users, existing financial services, level of unbanked populations, security risks, and openness to innovation. Though elements of regulatory frameworks are universal, they also need to be tailored to the local market.

Proliferation of non-financial institutions: A range of MNOs, technology companies, retailers and new companies are entering the payments market and this is likely to increase. It is not always clear if and how these providers fall under existing regulation risking confusion and regulatory gaps.

Wide variety of models being applied: Models of service delivery vary quite significantly across the different providers involved, the technology used and the service itself. This creates an extra degree of complexity in terms of understanding the market and the risks and issues involved.

Many services provide a basis for financial inclusion: Particularly in emerging markets, but in all regions, mobile payment and banking services are addressing the needs of unbanked and under-banked populations. Policy makers need to consider making this a priority and encourage adoption.

Consumers assume same protection as for existing financial services: While regulation may not treat mobile payments and banking services in the same way as traditional financial services, consumers typically assume they receive the same level of protection – this needs to be addressed.

Intersection of regulatory oversight: Mobile payment and banking services touch on four key areas of existing regulation including financial services, telecoms, technology, and retail/consumer protection. This can create confusion for providers, especially those new to the industry.

Roles of regulators not always clear: The roles of different regulators, for instance between financial services regulatory bodies and telecoms regulators in the case of an MNO providing payment services. There is a risk both of doubling up regulation, and of gaps.

Cost of compliance with regulation can be high: Existing regulations can create a high burden in terms of compliance particularly for relatively small providers who are new to the industry.

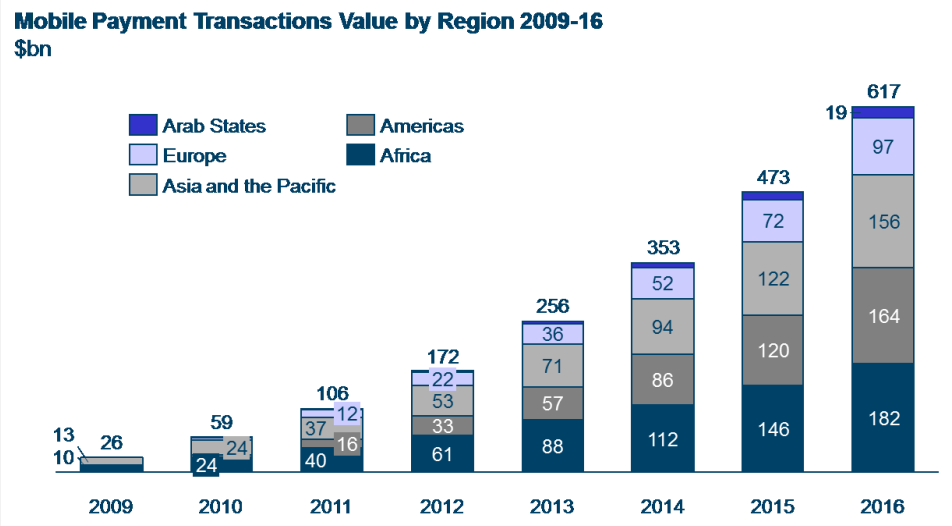
Services are safer than alternatives: Particularly in emerging markets mobile payments are replacing cash transactions this allows for tracking of payments previously not possible[1]. This calls for a degree of moderation when weighing up security against encouraging adoption (see section 4.3.2 for further discussion on tailoring regulation relative to the risks involved).

1.2 Outlook for Mobile Payments and Related Services

The mobile payments market has seen rapid growth with the total value of transactions close to doubling every year from 2009-12. Market commentators and forecasters expect the market to continue apace for the foreseeable

future. Broadly this has been, and will be a global phenomenon – Africa is expected to maintain its place as having the largest value of mobile transactions, Asia and the Pacific, North America and Europe in turn see high activity and growth. Latin America and the Arab States by comparison are expected to develop more slowly.

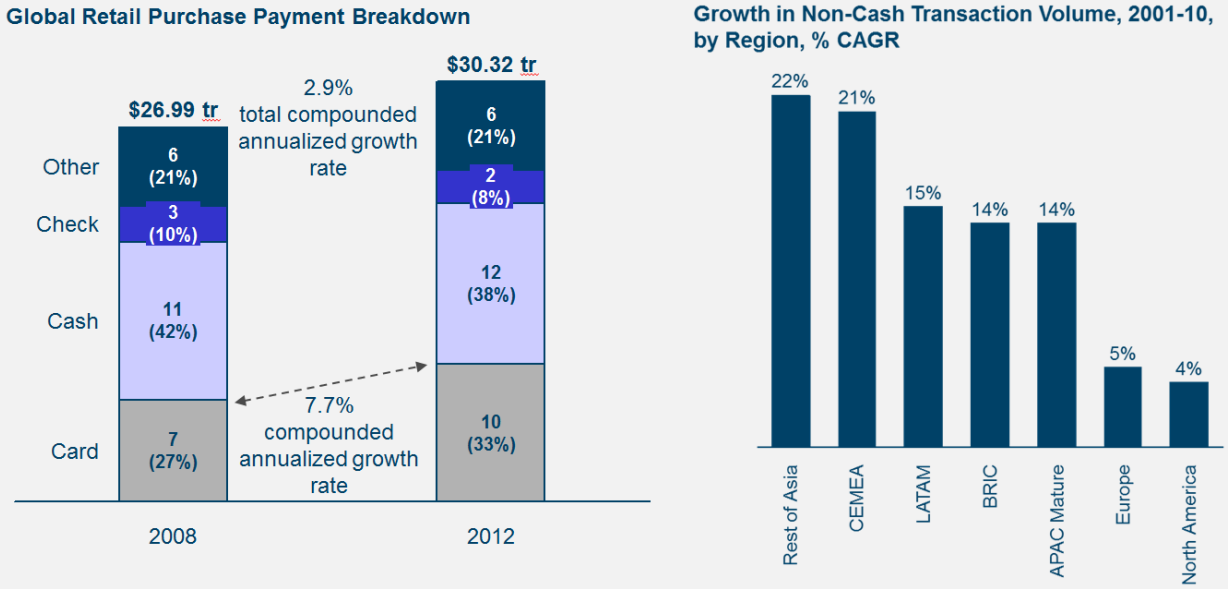
Figure 1.1: Mobile Payment transactions Value by Region 2009-16 ($bn)



Source: Gartner

The growth in mobile payments is consistent with a long running global trend that sees a move away from cash and cheque transactions to card based payments. This can be seen on the left hand side of Figure 1.2 with card payments increasing as a percentage of total purchases. The right hand side of Figure 1.2 shows particularly strong growth on non-cash transactions in emerging markets.

Figure: 1.2: Global Retail Purchase Payment Breakdown and Growth in Non-Cash transaction Volume[2]



Source: Euromonitor International Merchant segment Study 2012, Moodys analytics

Although relative growth of services is expected to be high, mobile payments still only account for around 1% of total transaction volumes globally, and by 2016 this would still only be 2-3%. On the hand this represents significant growth potential, but on the other it demonstrates that mobile payments are still far from a common habit for a mass market of global consumers.

The number of mobile payments and banking launches has gathered significant pace. Back in 2006 there were ten mobile money schemes in emerging markets. By 2010 this was 38. As of May 2013 there were over 160 schemes with a further 100 planned.[3] Most countries have at least one service, and are moving towards increasing levels of competition – Kenya has five providers, Uganda six and Nigeria ten.

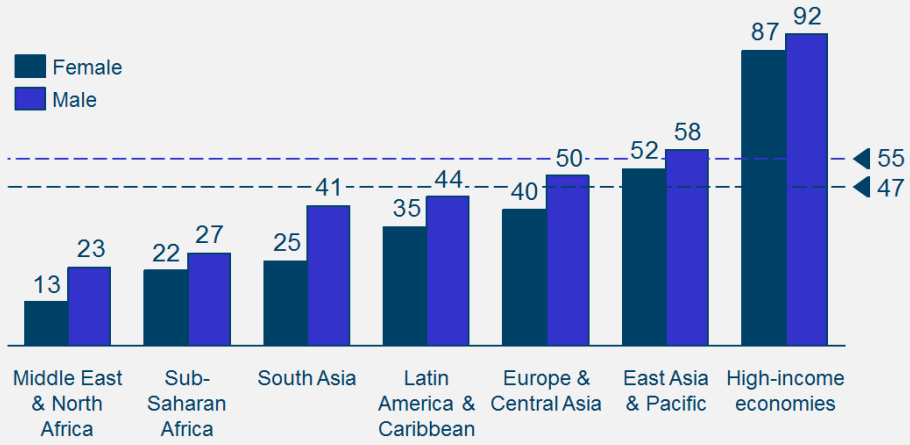
Developed markets appear to be showing an equal enthusiasm for mobile payments both from established companies like mobile operators and technology companies like Apple and Google, and from start-ups. From 2010 to mid-2012 over 300 companies attracted funding for mobile and online payment initiatives.[4]

Beyond simply being an attractive new market interest in offering mobile payment services is driven by a desire of established companies to diversify into new services. Mobile operators across the world are facing slowing growth or real decline in core voice and messaging services and financial institutions see slow growth in consumer businesses. Technology companies have a history of moving into new service lines leveraging good relationships with customers. Mobile payments are a logical next step for companies like Google and Apple.

1.3 Benefits and Latent Demand for Services

Many services are providing the basis for financial inclusion for unbanked and under-banked customers. Particularly in emerging markets but also in developed markets such as the United States there is often a significant proportion of the population which are unbanked or under-banked. Figure 1.3 demonstrates this showing the proportion of adults with bank accounts.[5]

Figure 1.3: Global Retail Purchase Payment Breakdown
Adults with an account at a formal financial institution (%)



Source: Demirguc-Kunt and Klapper 2012

This implies significant latent demand for a range of banking and payment services often taken for granted such as safe storage and easy access to money, the ability to make transfers to friends, family or business in remote locations, and alternatives to carrying cash to pay for goods and services.

In many cases these needs are unlikely to be met by an extension of current services. This is a particular issue in some emerging markets where it is not commercially attractive and viable to extend the necessary infrastructure of branches and ATMs and market services in many areas where unbanked populations reside. However, these same groups often do have access to mobile phones which as an alternative model for delivering financial services offer much greater reach at much lower cost.

For these unbanked and under-banked customers mobile payments and banking services can be genuinely transformational. Some of the key benefits are as follows:

- **Facilitates payments that would previously have been impossible or prohibitively expensive,** particularly remote payments.

- **Lowers the real cost of transacting,** especially for remote payments, where alternatives electronic transfers can involve high processing fees, and cash transfers can involve mailing, courier or travel expenses.
- **Lower cost of international remittance via mobile compared to existing services will boost flow of money.** The GSMA indicate that even a modest drop from a current average of 15% fees for international remittance will see a significant increase in demand – '*reducing charges by 2-5% could increase the flow of formal remittances by 50-70% boosting local economies*'[6].
- **Is safer than alternatives**, for instance reducing the need to carry cash to make payments, or send cash e.g. by mail or courier to make transfers over long distances. The mobile also provides a channel to send alerts in case of suspicious behaviour on an account.
- **Offers a better service than alternatives financial services** such as instantaneous transfers and the ability to access 24 hours a day.
- **Helps budgeting** by providing access in real time to balance and transaction history, as well as having facility to send alerts if limits are reached.
- **Greater accessibility and education possible** for instance through bilingual services, and ability to provide additional information through familiar and convenient services such as SMS and applications.

As an example of collective action on this the European Union in May 2013 announced measures to make bank accounts available for all EU citizens (there are currently c.58m unbanked consumers in Europe) on the basis that '*bank accounts have become an essential part of our everyday life … [and that] citizens cannot fully participate in society without a basic bank account*'[7].

There are benefits for consumers who already have access to financial services, but they are not as compelling. Services can mean greater convenience in making payments remotely and in person, and having access to accounts at any time place, as well as new services e.g. carrying loyalty card info or location based features.

Mobile point of sale solutions are also transformational for some merchants. Historically many small and 'micro' merchants have not been able to access conventional point of sale (POS) terminals to accept card payments because the economics do make sense for acquiring the banks, or in the case of mobile workforces it is not practical. This is common in both emerging and developed markets.

Figure 1.4: Mobile Point of Sale Terminals

- The smartphone is loaded with a payment application
- At sale the merchant keys in the relevant transaction amount into the app
- To make payment customers swipe their card through an mPOS dongle (or insert for chip and PIN) connected to the phone
- The transaction data is encrypted and sent via the phone's internet connection
- Once payment has been confirmed an SMS, email or physical receipt is provided

Source: Greenwich-Consulting Research

Developments in POS technology however such as mobile point of sale solutions (covered in Section 3.2.3), which allow merchants to accept payments via a mobile device and hardware accessory have lowered the barriers for merchants in the following ways:

- mPOS solutions are significantly cheaper than a conventional POS terminal (c.15-40% of conventional terminals)
- Distribution of dongles can be supported by suppliers of mobile devices generating cost efficiencies
- High penetration of smart phones, where applicable, enhances the reach for mPOS solutions

The ability to accept card payments can help merchants generate more sales, and also reduces their cash-handling requirements.

There are a number of underling trends that imply demand for mobile payments will continue to grow. These encompass a combination of consumer habits and access to technology, as well as broader economic and social trends. Table 1.5identifies these trends and their relevance for emerging and developed markets.

Table 1.5: Trends affecting the mobile payments

Trend	Relevance		Description & Rationale
	Emerging	Developed	
Access to mobile devices capable of mobile payments	High	Medium/ High	• Building on very high mobile penetration, high and rising penetration of smartphones in developed markets gives more people access to devices that will run a wide range of payment-related services • Mobile penetration is high in most emerging markets and still rising, and smartphone and feature-phone adoption is increasing at a rapid pace in many markets
Use of mobile devices for non-communication purposes	Medium	High	• There is an ongoing trend in mobile usage beyond basic calling and texting from consuming content, internet browsing, gaming etc • Particularly relevant is consumers using mobiles while shopping e.g. to browse items and compare prices at other stores • Familiarity supports an extension to using mobiles to make payments • Particularly relevant in developed markets, but also emerging markets
Trust in making online payments	Medium	High	• E-Commerce continues to rise with more and more customers making online payments • This represents an increase in trust around a channel which originally was associated with significant security concerns • This trust is likely to increase comfort with making mobile payments
Growth in economic activity	High	Low	• Economic growth can mean more transactions, greater value of transactions, greater reach of transactions as trade increases between regions and overseas, and greater stored wealth – all of which will support demand for payment (and banking) services • More relevant in emerging markets which are seeing high growth
Migration within regions and overseas	High	Medium	• Coupled with economic growth is migration of people – from rural to urban areas, across regions, and overseas • A greater physical distance for instance between family and friends, increases the need for services such as money transfers

Source: Greenwich-Consulting Research

2 *Overview of Services and Delivery*

2.1 Overview of Services Offered

2.1.1 Review of Service Types

There are a myriad of mobile payment and banking services offered both in terms of the function provided and the way it is delivered. Providers either already offer these services or are likely to want to in future – in either case it is important for regulators to build and understanding of each service.

2.1.1.1 Classification of Service Types

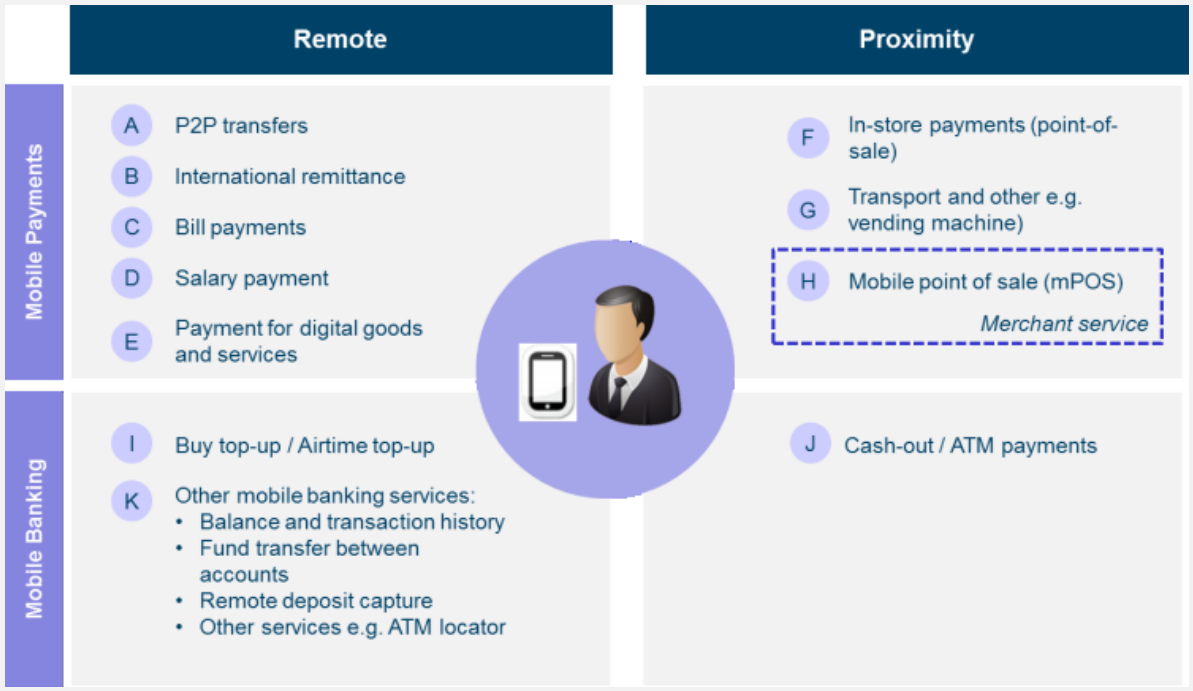
A useful categorisation is to split payments into those which are made remotely from the recipient, and those made when both the sender and recipient are both present, referred to as 'remote' and 'proximity' respectively.

On top of some obvious differences in the user experience, there are also differences in the technology used with remote payments (discussed in Section 2.2.3). This leads to differences in the risks involved, and also relative adoption in emerging versus developed markets. Regarding the later proximity payments including via Near Field Communication (NFC) and Quick Response (QR) code tend to be much more prominent in developed markets where smartphone penetration is higher.

2.1.1.2 Catalogue of Services Offered

There are a wide range of services offered between mobile payment and mobile banking services. Figure 2.1 captures the key types of services offered which are described below.

Figure 2.1: Key mobile payment service categorisation



Source: Greenwich-Consulting Research

A. P2P Transfers

Customers can make e-money transfers to other users such as family and friends. Particularly for unbanked customers, this is a safer, less costly and more convenient means of transferring funds than some existing alternatives e.g. sending cash via post or courier. A proximity version where users touch phones and make a contactless transfer has also arrived in some markets like the United States.

B. International Remittance

An extension of P2P transfers is making payments overseas, for instance a migrant worker sending money back home. By removing the need for physical points of presence mobile based international remittance can be lower cost than existing services. The user experience is similar to P2P transfers, but risks and regulations differ.

C. Bill Payments

Consumers can pay for bills e.g. for utilities via their mobiles. Especially with unbanked customers this is a safer and more convenient way of making or receiving relatively large payments. For banked customers it is more convenient than paying by cheque or bank draft

D. Salary Payments

Employers can make salary payments to employees directly to their mobile accounts in a similar process to bill payments. As with bill payments this benefits unbanked customers who would previously have been paid in cash.

E. Payment for digital goods and services

This covers the purchase of digital content such as music, video, games and ringtones. Examples include the likes of Apple's iTunes and App Store where users register a debit/credit card and make purchases through their smartphones.

F. In-store payments (point of sale)

In store payments differ depending on the technology being used. In emerging markets, where the spread of smartphones and contactless payment is more limited, the process can act more like P2P transfers described above but where the merchant takes the place as the recipient. In markets where there is mass adoption of smartphones, payments can be made through contactless payment technologies such as NFC or cloud-based services where payment information is transmitted via touching the mobile against the POS terminal or over-the-air respectively.

G. Transport and other e.g. vending machines

Mobile payments are also being used in a variety of other settings such as on public transport systems, in taxis, for parking meters, payments at vending machines, and at quick service cafes and restaurants (e.g. Starbucks and McDonalds).

H. Mobile Point of Sale (mPOS) solutions

mPOS solutions use mobile devices including smartphones and tablets already owned by merchants, in combination with a payment application and a hardware accessory (card reader) to allow merchants to accept card payments. In a typical process the merchant opens the payment app and enters the payment amount. The customer enters their card into the card reader accessory and enters their PIN/makes a signature. Payment data is sent for authorisation after which a receipt can be printed or sent by SMS or email.

I. Buy top-up / Airtime top-up

The integration of the mobile payment in the MNO ecosystem allows for customers to top-up their airtime accounts. They may also be able to send airtime for instance to friends or family that are on the same MNO network as per P2P transfers. Typically the phone account and mobile money account are held separately; hence top-up should be purchased by transferring the funds from the mobile money account into the airtime account.

J. Cash-out / ATM payments

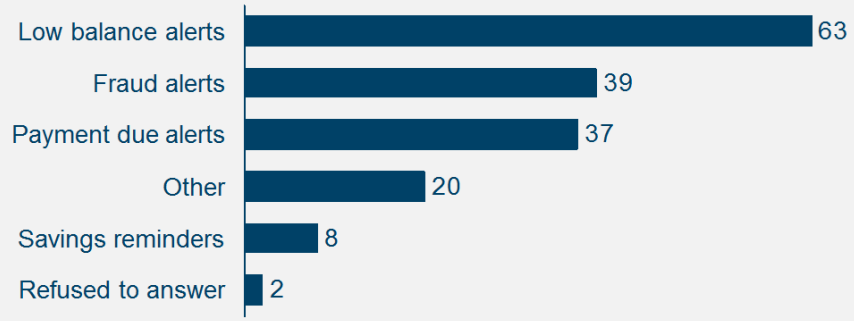
Customers may have the option to take cash off their mobile money accounts either at a cash-out retail agent (or in some cases a bank branch), or through an ATM or both. Ideally the electronic money held on accounts should be easily interchangeable with a cash equivalent – this functionality can significantly affect consumer willingness to join the mobile payment account.

K. Other mobile banking services

Mobile banking services can include a wide range of features. This can include providing information on the account activity, such as balance and transaction history checks, as well as SMS alerts for instance when spending limits are close to being reached, and about other services the bank provides e.g. an ATM locator. It also includes taking action on account such as fund transfers between different accounts.

Figure 2.2 gives an example from the US on the types of alerts customers receive from their providers[8].

Figure 2.2: Text alerts



Source: Board of Governors of the US Federal Reserve System

In addition there have been developments into more advanced services such as remote deposit capture. Here the service allows customers to scan cheques using a camera phone and transmit the scanned images to their bank for posting and clearing. This is an example of how the powerful features of smartphones can be used to provide enhanced mobile payment and banking services.

2.1.1.3 Payment Mechanism

The way the user funds mobile payments typically falls into one of three methods: Pre-paid accounts, mobile billing or credit/debit card linked accounts. Each method has different implications for the customer experience and also the risks involved both for the user and service provider.

Pre-paid accounts

Here a pre-paid account is linked to the customer's mobile – typically the mobile money account and phone account are separate with the later only used for voice and messaging. This is a common solution in emerging markets where card use is limited and the number of existing mobile billing accounts is lower. This creates a perceived and actual risk for the user in that their deposits need to be protected. For the provider the risk is lowered as funds are provided in advance.

Customers add funds to their accounts typically at retail agents or terminals. Qiwi's service in Russia is a successful example of this in a market where there is limited trust in e-payment security, setting up a large number of terminals for customers to top-up accounts. Another example is PayPal's MoneyPak offer where customers pick up a MoneyPak card at a selection of retailers and load cash at the checkout. This is transferred to a PayPal account which can be used to make online and mobile payments.

Direct Mobile Billing

This method is based on operators having an existing billing arrangement with customers i.e. applying to post-paid accounts. Mobile based purchases are added to monthly bills. From the operator point of view this introduces a credit risk, with operator's relying on customers settling their monthly bills. From the consumer point of view it may be preferable to a pre-paid account if they are averse, either from a convenience or perceived-risk point of view, to depositing their funds to a mobile account.

Credit/debit card linked accounts

In this case customers link an existing credit and/or debit card account to their mobile. Any purchases are added directly to the credit card bill or deducted from the customer's debit account. Mobile wallet services such as Google

Wallet work on this basis with customers loading details for one or more cards to their wallet. In some cases such as with SMART in the Philippines cards are issued as part of the mobile payments account.

From the provider point of view[9] this reduces credit risk and negates the need to deal with storing customer deposits. From the customer point of view it may be more convenient, however there is likely to be a higher perceived risk of giving access to their credit or debit accounts.

2.1.2 Breadth and sophistication of service offerings is increasing

The breadth and sophistication of service offerings is increasing and regulators should expect that providers will want to extend services further.

The often cited M-PESA is an example of how the range of services offered by providers has expanded. As one of the early leaders in 2007 their offering focused on P2P transfers. Today, while the P2P business remains popular many services have been added including bill payments, salary payments, merchant payments, Government to Peer (G2P) transfers as well as savings, insurance and micro-loans.

This extension and bundling of services is a common theme across many providers. Figure 2.3 gives four examples across different regions – Wizzit, SMART, MTN Uganda and Easypaisa. For new providers with a narrow range of services, those described here represent a likely product roadmap that they will be looking to offer over time.

Figure 2.3: Mobile payment service provider comparison

Service	WIZZIT *South Africa*	SMART *Philippines*	MTN *Uganda*	Easypaisa *Pakistan*
Transfers (domestic)	Yes	Yes	Yes	Yes
Transfers (international)	Yes	Yes	Yes	Yes
Pay in shops	Yes	Yes	-	-
Pay bills/salary	Yes	Yes	Yes	Yes
Cash in	Yes	Yes	Yes	Yes
Cash out (Agent)	Yes	Yes	Yes	Yes
Cash out (ATM)	Yes	Yes	-	-
Buy top-up/ send airtime	Yes	Yes	Yes	Yes
Airtime loyalty	-	Yes	Yes	Yes
Mobile wallet	Yes	Yes	-	-
Internet banking	Yes	-	-	-

Source: Company Websites, Greenwich-Consulting Research

Markets such as the US have seen the emergence of mobile wallet services offering a range of features and that can, in theory at least, replace a customer's real wallet. They work by storing account information for debit and credit cards which can then be used to make a range of payments. The wallets can also store loyalty card schemes, coupons, offers and gift cards that can be used and updated when purchases are made.

Google Wallet, as described in Box 2.1, as well as PayPal, ISIS, Visa, Mastercard and Turkcell are examples of mobile wallets. Advanced mobile wallet services tend to rely on smartphone functionality meaning these services are less likely to be seen in developing markets but will almost certainly move over as smartphone adoption grows.

Box 2.1: Google Wallet Case Study

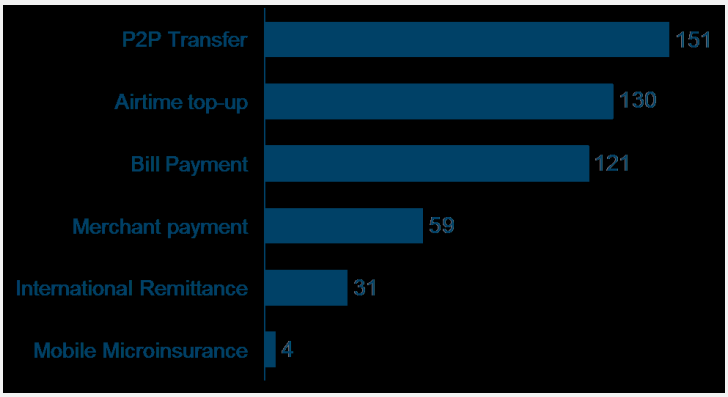
Google Wallet is one of a number of mobile wallet services and offers a range of functionality for both consumers and merchants. Consumers can load multiple credit and debit cards to their Wallet. They can also add details for loyalty programs, gift cards and promotional offers, all of which can be redeemed at point of sale. Additional features include location-based offers using a smartphones GPS function, and 'single-tap payment' via NFC technology (although this relies on both the users smartphone and merchant's point of sale terminal being set up for NFC).

Source: Greenwich-Consulting Research

2.1.3 Service Deployment and Usage

For emerging markets the most commonly deployed services are P2P transfers, one of the first services to emerge, along with air-time top-ups and bill payments – as shown in Figure 24.

Figure 2.4: Mobile payment usage by category (number of deployments)



Source: GSMA MMU Deployment Tracker

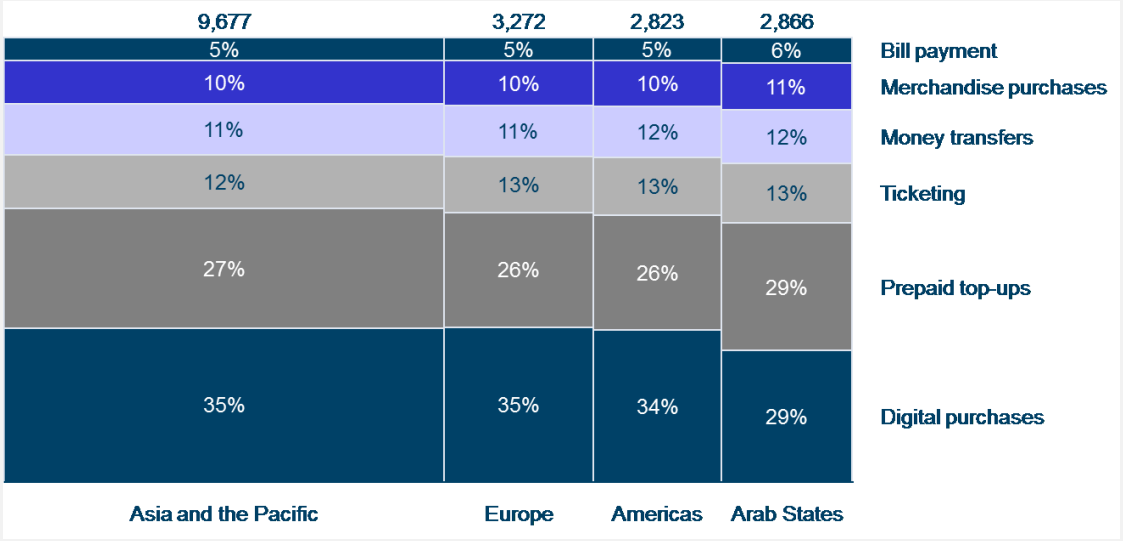
Merchant payments are emerging services which are likely to grow in future, along with more advanced mobile banking services such as micro-insurance.

International remittance is less commonly deployed, than the similar P2P transfers. This may be because there is less demand for the service, but it also may be due to a more complicated regulatory environment. The later comes from heightened concern over money laundering and terrorist financing risks, as well as rules on capital flows, and the need for providers to establish regulations both in their own country and the countries payments are sent to or received from.

This can be a difficult and time-consuming subject for providers to navigate, especially when national regulators (both telecom and banking) are not clear on international rules, and risks stalling the spread of what can be highly valued services. There is clearly a role for local regulators to support providers in understanding.

Although levels of overall adoption differ by region, relative usage of different types of service are remarkably similar across regions as shown in Figure 2.5. Digital purchases and pre-paid top-ups (see top-up/airtime top-up above for example of these kinds of services) are most common, money transfers and merchandise (in-store) purchases are both around 10% of overall volumes, and bill payments commonly around 5% of total volumes.

Figure 2.5: 2012 Mobile payment transactions volume by user case (mm)[10]



Source: IE Market Research, Greenwich Consulting Analysis

2.1.4 Virtual Currencies

The services described above are based on electronic exchanges of 'real-world' currencies. Another important area of digital transactions seeing rapid adoption, and with it increasing attention from regulatory bodies and legal systems, is virtual currencies. Examples of these currencies include Bitcoin, Facebook Credits, World of Warcraft Gold, and Second Life Linden Dollars.

Credits can be earned by taking part in some sort of activity or can be bought with 'real-world' currencies. More conventionally these currencies can be traded in to purchase electronic goods and services, but can also be used to buy physical goods and services, make P2P payments, or exchange back for real currency. Regulatory concerns around virtual currencies are covered in section 4.2.3.

2.2 How Services are being Delivered

A key part to understanding the mobile payments landscape is recognising the breadth of models being adopted to deliver services each varying by the nature of the service offering, the process for payments to take place and the entities involved. While of course there is common ground in terms of the risks involved, regulators need to be aware of the differences in these models and their implications. Formulating regulations as a blunt tool that applies the same strict measures to all services risks overburdening some providers and stifling innovation when not necessary.

A range of entities are taking a lead in the provision of services, owning the relationship with customers and looking to capture a significant proportion of the revenues generated. These leading actors include financial institutions, mobile operators, technology companies and large merchants.

In the cases of non-financial institutions providing services, which are very common, there can be uncertainty around how they are covered by existing regulations. Particularly as these services become more mainstream and their offerings expand in sophistication[11] it will be important for regulators to identify any gaps in existing coverage and ensure all parties, including customers, know and are accountable to their responsibilities.

2.2.1 Variety of models adopted for delivery with non-bank led models being less straightforward for regulation

The following provides an overview of some of the key delivery models. As discussed above the implications for regulation vary by model. Bank-led models and bank and MNO partnerships are typically the most straightforward with banks already falling under clear regulations. MNO, technology player and merchant led models are likely to be less well covered from a regulatory stand-point.

Bank-led Models

The bank-led model is based on an extension of existing payment services to cover mobile and includes an issuer role providing the payment application/account to consumers and an acquirer role to set up merchants to accept mobile payments.

Example process for merchant payment:

i. Customer initiatives payment
ii. Acquiring bank sends payment request to issuing bank via payment network
iii. Issuing bank sends payment to merchants account
iv. Funds deducted from customers account

Figure 2.6: Simplified value chain for bank-led service: merchant payment

Source: Greenwich-Consulting Research

Many key elements for banks to deliver mobile payment services are already in place with them able for instance to draw on existing consumer/merchant relationships and experience in payment processing and risks management.

Banks are not as strong in regions with large unbanked populations and limited existing banking infrastructure. Here they may look to partners to support in distribution of services. Another area where banks typically have less experience is in developing mobile applications. In the bank-led model the role of the MNO is limited with one exception – in the case of NFC payments operators have a strong bargaining chip in the shape of control over the customers SIM.

MNO-led Models

Here the MNO acts more or less independently to offer mobile payment services. They market the service to customers, develop a payment application that is installed on handsets, carry out transactions and manage the billing of customers.

Example process for merchant payment:

i. Customer initiates transaction on mobile payment application
ii. Transaction data is carried through operator network
iii. MNO provides funds to merchant
iv. MNO charges the customer e.g. takes credit from pre-paid account, or adds to mobile bill

Figure 2.7: Simplified value chain for MNO-led service: merchant payment

Source: Greenwich-Consulting Research

MNOs can typically draw on a number of assets to provide services including a large base on installed customers, an existing billing arrangement with those customers either pre-paid or post-paid, and control over the distribution of handsets.

Limitations and challenges to the model described above are that MNOs do not have a link to the existing payment network and also lack experience in processing financial transactions. A way to remedy this is through some degree of collaboration with a financial institution.

In line with this MNO-led models are typically more prevalent in regions with large unbanked and under-banked populations where the benefit of simple services is high. More sophisticated solutions e.g. mobile wallet solutions in developed markets typically require collaboration. That said the like of ISIS in US is a good example of operators being the leading actors in providing services.

MNO and Financial Institution Collaborations

Here MNOs partner with banks and/or credit card companies to offer services. The benefit of this approach is to allow each party to focus on their relative strengths, and to draw on a potentially combined customer base covering consumers and merchants.

The MNO for instance brings its communication infrastructure and control of distribution channels for mobile devices. Financial institutions bring experience in processing financial transactions and risk management, as well as an installed base of credit card users and merchants who are set up to accept card payments. Particularly in the case of credit card companies like Visa and Mastercard they offer strong brands attracting consumer trust.

The process for transactions would be similar to that described for the bank-led model above, however from a commercial point of view MNOs would take a cut of revenues.

This is something of a natural progression from MNO-led provision as services become more complex. Some regulators prefer (and some insist) financial institution involvement in service delivery given their experience and also stronger regulatory oversight. Due to greater complexity of delivery, and the need to share revenues, these types of model while offering benefits can be difficult to manage and set up.

Technology Player-led Models

This covers technology companies who combine their own assets with the existing mobile and payment ecosystem to offer mobile payment services. This includes the likes of Google, Facebook and Apple looking to extend the ways they interact with customers and potentially generate new revenue streams.

These technology players have a number of assets to draw on as they seek to establish their place including customer familiarity with existing mobile and internet based services; existing registered payment accounts (Apple), ability to offer complementary services e.g. Google offering location based services via Google Maps, Facebook combining social networking features with payments.

While currently services like Google Wallet are limited to smartphone users, the reach of these brands is global offering a large potential market as more customers are able to access services.

For mobile operators there is a risk that these services are provided 'over-the-top' meaning that even though the operators networks may be used in providing payment services, they could still be cut out of the loop.

Merchant-led Closed Loop Models

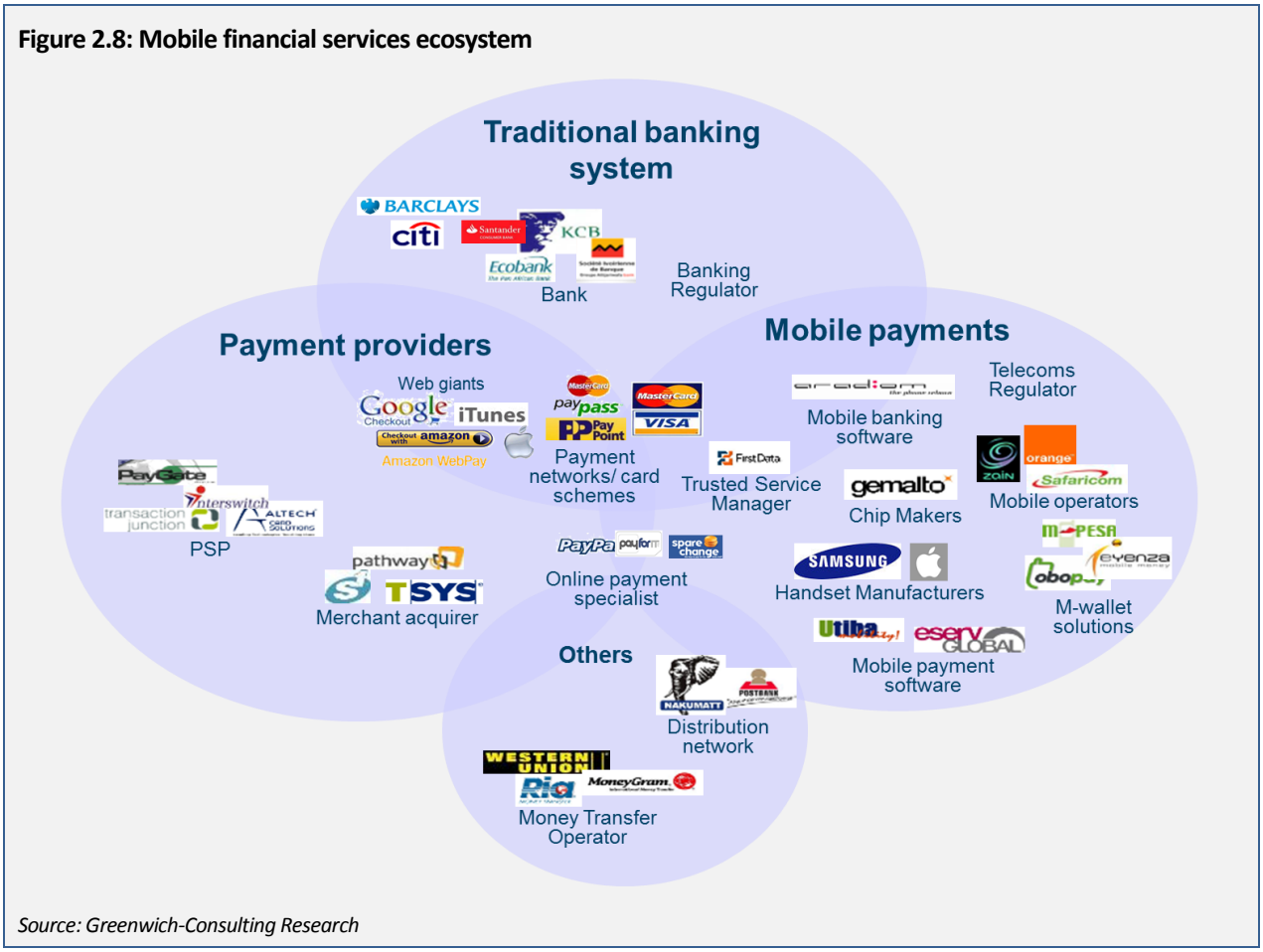
A merchant acts independently, or in collaboration with other merchants, to launch a closed-loop payment system for mobile payments. A key example is the Starbucks coffee chain who set up a closed loop payment system for use in their cafes. Customers download an app with a pre-paid account. They top-up the account online or in store, and then use the payment app to make purchases. Acceptance terminals are based on reading Quick Response (QR) codes displayed on the app. Another example is MCX, a merchant-owned mobile platform set up by US merchants including Wal-Mart, Gap and Lowe's.

2.2.2 Large number of entities in the mobile payments ecosystem

The leading providers of services, as described above, can be financial institutions, MNOs, digital players and large retailers. There are also a wide set of supporting actors in the payments ecosystem who come into play depending on the model being deployed. Figure 2.8 gives an overview of the mobile payments and banking ecosystem.

From a regulatory perspective it is important that the responsibilities and potential liabilities of each entity in the payment process is clear, ensuring there are no gaps or uncertainties on where each one stands. This requires collaboration amongst both industry and regulatory stakeholders.

Figure 2.8: Mobile financial services ecosystem



Source: Greenwich-Consulting Research

Key supporting actors in mobile payments and banking services include:

- **Payment service providers (PSPs):** Offer merchant services for accepting electronic payments managing connections and relationships with multiple banks and payment networks.

- **Online payment specialists:** A variation on PSPs who specialise in allowing merchants to accept online payments
- **Chip Makers:** Produce chips for mobile phones including secure element that will be crucial for NFC payments
- **Trusted Service Manager:** For NFC-based payments the trusted service manager controls access to customer information stored in the secure element of NFC-enable devices
- **Handset manufacturers:** Manufacture the mobile devices, with increasingly sophisticated technology, that mobile payments run on – the role of these manufacturers can be key as they have the potential to significantly scale mobile payment initiatives
- **Mobile Payment and Banking Software/App Providers:** Develop the mobile applications used as an interface on mobile devices for customers to make payments
- **M-Wallet Solutions:** Providers specialising in mobile wallet solutions such as Eyenza who provide a wallet service not specifically tied to any one bank or operator; may operate as a white label solutions for other brands to use
- **Money Transfer Operator:** 'Traditional' money transfer providers who are also looking to expand in the mobile channel

2.2.3 Key Technologies

Each mobile payment solution relies on a combination of technologies to deliver its service to customers. These technologies can vary significantly in terms of customer experience, cost to provide and security, as well as current level of adoption.

Providers must weigh up these points and be pragmatic about delivering to the market today, while keeping an eye to the future and how technologies, and adoption, will evolve over time. Regulators also need to have an understanding of the different technologies and implications for security.

Technologies are categorized into the following groups based on the role that they play:

- Transmission of payment data: SMS, WAP, NFC, QR Codes
- User interface: Browser, Applications
- Storage of payment information: Secure element, Cloud service

Figure 2.9 provides a summary of the key technologies, and associated benefits and challenges.

Figure 2.9: Key Technologies

	Type	Description	Payment Type	Benefits	Challenges
Transmission of Payment Data	SMS	• Payment information sent by SMS • Very common in emerging markets	• Remote • (Proximity)	• Customers familiar with technology, easy to use • Available across mobiles / carriers	• Payments can be slow, lost messages • SMS encryption not as strong as alternatives • Low merchant rates
	USSD	• Based on Unstructured Supplementary Service Data (USSD) standard. Similar to SMS (182 character messages) but able to create real-time connection during a USSD session to more responsive	• Remote • (Proximity)	• Faster than SMS	• As per SMS encryption not as strong as alternatives
	WAP	• Data sent via WAP, in browser or app context • More common in developed markets	• Remote • Proximity	• Does not require new technology for customers • Limited setup for merchants already taking web payments	• Does require smartphone and reliable data connection • Customers suspicion over web payments
	NFC	• Allows devices in close proximity to connect and transmit data • Low adoption	• Proximity	• Heightened security when combined with Secure Element • Smooth payment experience	• Lack of NFC enabled handsets • Merchants reluctant to invest in POS
	QR Code	• Transfer of info via quick-response (QR) barcode • Read by camera phones and specific POS	• Proximity	• Low cost • Functionality to read on most smartphones	• Does require smartphone and specific POS to read • Less smooth an experience vs NFC

		devices			
User Interface	Browser	• Payments made via mobile based browser • Replicates online experience, data sent via WAP	• Remote	• Familiar experience for customers used to online payments	• Relies on connectivity and smartphones • Adaption of websites to mobile screen can be an issue
	App	• Application acts as interface to support payments • Can use WAP, NFC, QR codes	• Remote • Proximity	• Apps can be created for a tailored user experience	• Relies on connectivity • Apps need to be installed by user on device which may slow adoption
Payment Info Storage	Secure Element	• Stores payment credentials on mobile device • Encrypted and tamper-proof chip	• Proximity	• Very secure technology	• Data tied to device that can be lost/stolen • Adoption in devices currently low
	Cloud Service	• Payment credentials stored in cloud and accessed via internet when required	• Proximity • Remote	• Easier to implement and scale than NFC • Data not tied to mobile device - can wipe data remotely	• Takes more time to complete than NFC payments • Relies on connectivity

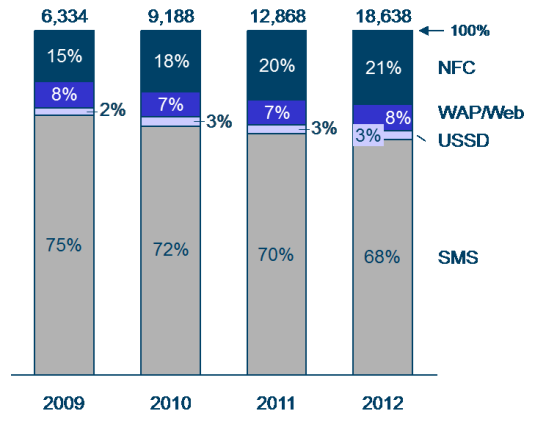
Source: Greenwich-Consulting Research

In emerging markets there is a tendency towards SMS-based payments due to wide adoption of 2G (but currently lower 3G and 4G) mobile services. Applications are simple for mobile devices with limited functionality, and as accounts are very often pre-paid there is not the issue of how to store card data. Figure 2.10 shows SMS is the most common technology globally.

However smartphone adoption, card use and data connectivity are all on the rise and will impact which technologies are used for mobile payments. In line with these trends it would be expected to see the adoption of WAP-based and/or NFC based payments, of more sophisticated user applications, and for card details to be linked to mobile accounts raising the question of how to store card data. Exactly which of these or these technologies, or alternatives, will become dominant remains to be seen, but may depend on their relative success in more developed markets.

Based on the United States as an example, SMS and WAP are the common technologies used for mobile payments with a large quantity of payments through both mobile browsers and mobile applications. Globally NFC payments are increasing faster than other technologies and this is driven by adoption in developed markets. Use of QR codes (or other use of barcodes for mobile payments) is low with adoption limited outside of headline-grabbing example such as Starbucks.

Figure 2.10: Global Mobile Payment Transactions by Technology, Volume (Millions)



Source: Source: IE Market Research

Going forward the number of mobile wallet launches and their increasing sophistication is likely to attractive more and more users. From a technology point of view the battleground for mobile payments is likely to be based around two models:

- *Cloud-based payments:* where payment information is stored in a cloud service, where the user interface is a dedicated mobile wallet application, and the transmission of payment data is through WAP
- *NFC-based payments:* where payment information is stored in a secure element in the mobile device, the user interface is also a mobile wallet application, and the transmission of payment data is via NFC

While NFC is arguably both more secure based on the 'Secure Element' and offers a smoother customer experience, it also relies on more factors falling into place based on wide consumer and merchant adoption of NFC enabled devices (handsets and POS terminals respectively).

As discussed above it is important for regulators to understand the kind of technologies that will be used in their markets, and to build regulations around the associated risks.

3 Challenges Facing the Industry

There have been a number of very successful mobile payment services launched with examples in emerging markets such as EcoCash in Zimbabwe, MTN Uganda, SMART Money in the Phillipines and M-PESA in Kenya. In these cases significant percentages of the population have adopted services in a very short space of time, and this has created high expectations for launches in other markets.

The reality sinking in across the industry however is that success is far from a given. Many launches have struggled to meet albeit high expectations, with the commercial viability of models which require scale being questioned, and adoption of mobile payments services in many countries remains low.

Regulators need to understand the challenges facing the industry and where they can help, and particularly where regulation itself is creating barriers by being over-bearing, or confusing, or creating uncertainty simply by its absence.

3.1 Demand Side Barriers

While the use of mobile payment and banking services is increasing, there remain a number of barriers to further adoption by consumers. One set of barriers is around a lack of awareness or consumers not seeing significant benefits associated with services:

- **Awareness**: Most services are still relatively new and it is not surprising that some customer groups are not aware of the services on offer. It may be that advertising has not reach them, or that their peers do not use the services. A variation of this is that consumers, especially the unbanked and under-banked may be aware of services, but not aware that they are eligible for them
- **Value proposition**: Another commonly cited reason for not using mobile payment services is that consumers do not see the value compared to other means of making payments including cash and card transactions. This is more relevant when consumers already have access to alternative financial services, but in all cases where mobile payments are not yet habitual there needs to be a strong case for use
- **Limited places to use service**: When adoption by consumers and merchants is at an early stage consumers cite the lack of places to use services (either peers to transfer money to, or merchants to purchase at) as a reason for not adopting services

In these cases telecoms regulators may be able to support the industry by raising awareness, but broadly speaking these are problems that will need to be fixed by the market.

There are a further set of customer barriers which are stall adoption of services from customers that would otherwise be interested:

- **Security concerns:** One of the most cited reasons for not using services is concerns about security of payments. Exhibit 3.1 identifies security as a key reason for consumers in the US not using mobile payments. This includes fears about identity theft, loss of personal information and ultimately being subject to fraud.
- **Lack of ID**: Particularly relevant for unbanked and under-banked customers are that they may lack the required ID to sign up to services required on the basis of know-your-customer (KYC) rules.
- **Ability to compare services**: With services being provided by a range of different industry participants including banks, MNOs and digital players it can be hard for consumers to compare services for instance on the level of protection offered.
- **Mobile device requirements**: Some willing consumers cannot access services because their mobile devices do not have the right features (or at least they believe this to be the case). This is more associated with mobile wallet solutions appearing in developed markets that require smartphone capabilities.
- **Lack of mobile internet/prohibitive cost**: As with mobile device requirements this varies depending on the service, but requiring mobile internet to make payments will exclude those who do not have it or find it too expensive. A variation on this is that consumers may *assume* they need access to a data plan to make payments where in fact they do not.

In these cases regulators can have a positive role in promoting adoption – by ensuring greater security around payments, by lowering ID requirements under certain circumstance, and by pushing for easy comparability of services. Barriers around mobile device and internet requirements are more difficult for regulators to influence, but they could for instance set requirements and/or provide incentives (e.g. around spectrum allocation) to providers to increase accessibility of service.

Figure 3.1: Main reasons affecting the decision to use mobile payments

Source: Federal Reserve Board Mobile Financial Services Survey (2012)

Merchant barriersThere are several barriers for merchants which can explain low mobile payment acceptance by merchants. This can include uncertainty over which services to adopt, and difficulty in justifying the investment based on expected sales:

- **Awareness of services and consumer usage:** Merchants may not be aware of all the types of mobile payment services offered and which to consider accepting. Or they may be aware, but not of how popular services are with consumers, making investment decisions difficult.
- **Uncertainty over which services to adopt**: Assuming merchants are aware of the services offered, a secondary challenge is often being faced with a wide and potentially confusing range of provider solutions. With most markets still at an early stage, lacking an obvious leader and without interoperability of services, there is not an easy or obvious choice for merchants. This uncertainty can lead to merchants stalling.
- **Lack of consumers using any one service**: Related to the points made above, there may simply not be enough consumers currently using payment services to justify merchant investment, for instance in new point-of-sale terminals.
- **Low sales volumes**: Even in a scenario where consumers are regularly using mobile payment services, sales volumes at some merchants may simply not be enough to justify the investment for instance in (new) POS terminals, training staff etc.

For these barriers the role of regulators will probably be limited.

There is a network effect associated with mobile payments and acceptance. The more consumers there are willing to use the service the more attractive it is for merchants to accept mobile payments, and the more merchants that accept mobile payments, the more attractive it is for consumers to have access to the service. As adoption rises the reinforcing network effect is likely to lead to even further adoption. Starting from a very small network however means it can be difficult to get the service off the ground. This is exacerbated where a lack of interoperability means networks are fragmented. Regulators need to weigh up the pros and cons of intervening to encourage or even force interoperability to support the spread of services (discussed in more detail in Section 5.3.3.)

3.2 Supply Side Barriers

The market for mobile payments is still at a relatively early stage and is facing a number of the challenges common to emerging technology industries including[12]:

- **Fragmented market for services that are only viable at scale:** With what can be significant upfront investments services may only be viable when a relatively large scale is reached. However markets are mostly still fragmented putting into doubt the viability of services. **Lack of dominant technology standards**: Lack of recognised standards lowers the addressable market for providers and makes investments more risky (in the scenario where they pick the *wrong* technology). Providers can mitigate this by investing in multiple solutions, or may delay investment – in either case investment is diluted.
- **Best commercial model unclear**: Similarly to the point around standards, the best commercial model to adopt is still unclear with what remains a limited number of very clear success stories, and differences between regional markets.
- **Debate over revenue-sharing and customer ownership**: While collaborative models, e.g. an MNO partnering with a bank, can create synergies there are also difficult questions to tackle including revenue-sharing and customer ownership which can make it difficult to get these projects going.
- **Lack of focus on customers**: Industry commentators such as Ovum suggest that providers are not paying enough attention to what customers actually want – "*the merchant and consumer perspectives are being overlooked in the excitement caused by new enabling technologies, the latest device, or yet another mobile payments launch"*[13].

As with some of the consumer challenges discussed above these problems are likely to be solved by the market. One area where regulators could intervene, as discussed elsewhere in the paper, is in encouraging interoperability (see section 4.3.3).

Regulatory Barriers

There are cases where regulation halts or slows the progress of the industry, including:

- **Lack of clarity on regulation**: The regulatory implications of mobile payments for banking and telecoms regulators in particular are still being worked through in some markets. While a lack of regulation can actually allow more innovation, it also holds up providers who need to know where they stand in terms of their responsibilities and liabilities, before launching or expanding services[14].
- **High cost of compliance**: For new and small providers the costs of compliance with regulation can be relatively high to the point of being prohibitive. This can be particularly relevant where new providers offering a limited set of services are subject to the same kind of regulations as well established financial institutions
- **Innovation blocked by regulation**: Prescriptive regulations, particularly where set by banking regulators setting the same kind of requirements as for more complex/risky financial services, that prohibit certain kinds of activity/types of provider can block innovative in payment services. Either by directly prohibiting services or creating compliance requirements that cannot feasibly be met.

Strong regulation may be justified on the basis of risks involved in (new) financial services, but regulators also need to recognise where it slows progress. In this cases where uncertainty over regulation is barrier it is imperative for regulators to act.

4 Regulation of Mobile Payments and Related Services

It is assumed that policy makers and regulatory bodies are balancing two broad aims when it comes to mobile payments and related services. The first is ensuring that any new financial services are regulated to protect consumers and prevent misuse. The second is encouraging the development of services which will potentially bring significant economic and social benefits.

With respect to these aims, and considering the market context set out earlier in the paper, this section addresses the following points:

- The need for regulators to clarify their roles and collaborate with other regulatory bodies
- Developing a regulatory framework to ensure safe and secure payments

- Adapting the regulatory approach to fit the market context, and creating an enabling environment for services to grow

4.1 Clarification of Roles and Collaboration between Regulatory Bodies

Due to the nature of mobile payments and banking provision they involve the intersection of key areas of existing regulation – financial services, telecoms, technology and retail/consumer protection.

- **Financial services regulation** covering account issuance and payments, carried out by one or more financial regulators such as a central bank, dedicated regulatory body and in some cases a separate financial services focused consumer protection agency. In some cases for instance in the European Union providers may also have to refer to EU rules and regulations around the provision of financial services.
- **Telecoms regulation** covering the activities of mobile operators who are playing varying degrees of roles from pure connectivity through to issuing mobile payment and banking services
- **Technology certifications** which apply to technologies used in financial services transactions. These are set by industry bodies, and example being Payment Card Industry Data Security Standard (PCI DSS)[15], and financial regulators will typically require that any technologies used in payments meet certain industry standards.
- **Retail/consumer protection agencies** ensuring consumer interests are protected including tackling specific issues such as consumer privacy and data protection

For each area of existing regulation mobile payments and banking services sees a break from the past:

- Financial services regulators who are used to predominantly if not exclusively dealing with financial institutions are faced with non-banks providing services
- Telecoms regulators are faced with operators moving into the provision of albeit usually basic financial services, an area regulators typically have little experience in
- New types of technology are emerging which will need to be certified against standards as described above, assuming that financial regulators for instance insist that technologies for mobile payments should be held to the same standards as for other financial services
- There are a new range of challenges for consumer protection for instance around the multitude of new customer data being captured

As described above new services and service models do not always fit neatly under existing regulatory frameworks, and in many cases regulatory bodies are still catching up. In the case for instance of mobile operators offering payment services the roles of financial services and telecoms regulators are not always clear[16]. The responsibility, and power, of regulators can gets more complicated still when providers offer services across borders for instance if Google, a US based company, provides mobile wallet services in Europe.

This creates uncertainty both for regulators in fulfilling their roles and for providers who may struggle to understand or even discover their full set of responsibilities. There is also a risk of gaps in regulation when certain parts of the payment process, or the entities involved are not covered. Figure 4.1 gives an example of the regulatory ecosystem in the UK to show the wide range of bodies and sets of law that may (or may not) be relevant for a particular kind of service.

Figure 4.1: UK Regulatory Ecosystem

Type of Regulator	*Regulator*	*UK*
Financial Services Regulation	*Central Banks*	Bank of England
	Dedicated Financial Services Regulator	Financial Services Authority
	Supra-National Bodies	European Commission
Technology Certifications	*Industry Groups*	e.g. Europay/Visa/Mastercard Technology Standards
Telecommunications Regulators	*Mobile Telecoms Regulators*	Ofcom
Consumer Protection	*Consumer Protection Agencies*	The Office of Fair Trade
	Data protection	The Information Commissioner's Office
Competition Regulation	*Competition Commission*	Competition commission
	Supra-National Bodies	European Commission
Commercial Law	*National Legal System*	UK Legal System
	Supra-National Bodies	EU Law
	Intellectual Property	UK Intellectual Property Office

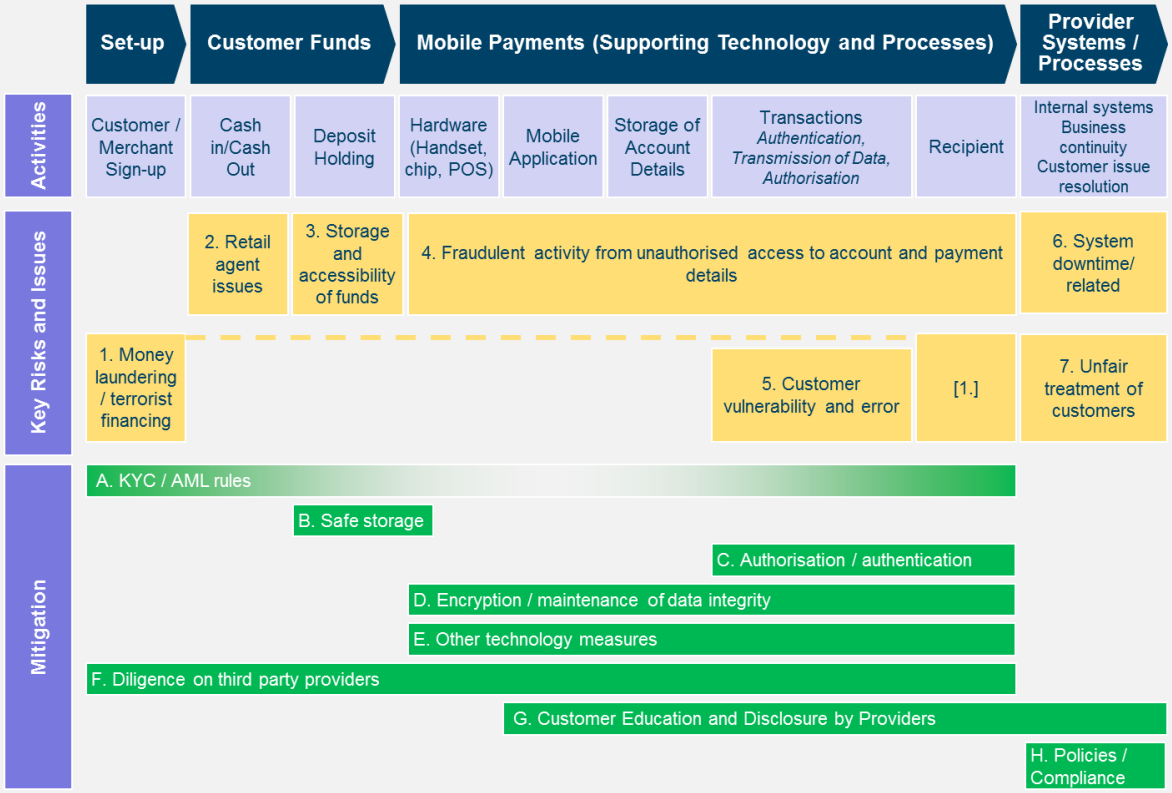
The implication is a need for regulatory bodies to work closely together to understand the full payments landscape and assign roles and responsibilities where appropriate. This should cover developing a joint understanding of the landscape of mobile based services in their markets and the need to adapt current regulations, developing clear objectives for regulation, and deciding on the roles and responsibilities of different bodies and how they will interact.

There is also a place for regulators for a given markets working with international counterparts. This can be to understand specific regulations for services such as international remittance, but also to share experience and best practices. Though a more ambitious idea, there is a case for regulators developing regional or international frameworks from mobile payments and banking regulation. This already takes place for the technology certifications described above.

4.2 Regulatory Framework to Ensure Safe and Secure Payments

This section provides a review of the risks and issues that arise across the various stages involved in providing mobile payments. Telecoms regulators are unlikely to be responsible for tackling all the regulatory issues highlighted here, however an appreciation of the issues that arise and ways to mitigate against them will support in interacting with financial regulators, and supporting operator and the development of the sector.

Figure 4.2: Regulatory Framework to Ensure Safe and Secure Payments



Source: Greenwich-Consulting Research

Figure 4.2 covers the major stages involved from signing up customers and merchants, customers adding funds to their account (relevant for pre-paid accounts), to the carrying out of transactions, along with a set of provider systems and processes that sit behind and support these activities. It highlights the key risks and issues areas where arrived, covered in detail in Section 5.2.1 and means to mitigate them, covered in detail in Section 5.2.2.

For those well versed in financial regulation this will cover some familiar ground, as many of the issues raised here are common across different types of financial services, but in this case directed to a mobile payments environment. The variety of models being adopted, as described in Section 3.2.1, and services offered may entail some variations on what is described here, but this should provide a good high level coverage of the areas that need to be addressed.[17]

4.2.1 Review of risks and issues associated with providing mobile payments

This section highlights the risks and issues that can arise in providing mobile payment services, with reference to those highlighted in Figure4.3**.** Against these, examples of mitigating actions that will be taken are provided – a more detailed view of these mitigating actions will be covered in the next section.

Figure 4.3: Review of risks and issues associated with providing mobile payments

Area	Risk / Issue	Description	Example Mitigation Actions
1. Money laundering / terrorist financing	Money laundering/terrorist financing within borders	Risk of accounts being set up and used to launder money or to support terrorist financing	• Adequate customer due diligence (Know Your Customer measures) on new accounts
	Across borders	Increased risk of ML/TF in some cases of cross-border transactions (where same regulations do not necessarily apply)	• Specific rules for international remittance including KYC measures on recipient
2. Retail agent issues	Liquidity, physical security	Where retail agents are used to deposit and later access funds, risk of them not being liquid, and being vulnerable to theft	• Due-diligence on agents • Onboarding and training of staff • Increase physical security (e.g. vault / guard) • Monitor performance
	Staff awareness / prevention of risks	Staff at retail agents being vulnerable to mistakes/scams due to lack of awareness, or not taking necessary precautions	
3. Storage and accessibility of customer funds	Safe storage of customer funds	Ensuring safe storage of customer funds, particularly relevant when provider is not a bank	• Require non-banks to store funds in regulated banks in low risk financial instruments
	Accessibility of funds	Ensuring sufficient liquidity of provider that funds will always be accessible	• Capital adequacy requirements of non-bank players
4. Fraudulent activity from unauthorized access to account and payment details	Tampered device	POS terminal unsecure e.g. through tampering with device	• Due diligence on POS providers • Due diligence on merchants • Strong authorization controls
	Virus / bad application	Customer accidently downloads a virus or related malware, or a faulty/bad application	• Install anti-virus software on smartphones • Test and certify applications
	Security of SIM/secure element	Sensitive data held on SIM / secure element compromised	• Encryption of data stored on device • Tamper proof SIM / secure element
	Security of data stored in cloud	Sensitive data held in cloud compromised, with multiple account details stored together likely to be a target for cyber attacks	• Encryption of data in cloud • Measures to prevent cyber-attacks and related threats
	Managing access to (multiple) accounts in the mobile wallet	Multiple accounts may be stored in mobile wallet, need to ensure only relevant applications and parties can access the relevant data	• Use of Trusted Service Manager to administer account info, and control which apps / parties can receive data; and to manage lifecycle of de-
		Deactivation of account when	

		device is no longer in use	vice including deactivation at appropriate time
	Lost or stolen device / stolen PIN/password	Device is lost or stolen and attempted to be used PIN/password is stolen or hacked	• Multi-factor authentication • Mobile device password • Auto service logout • Ability to remotely wipe payment details and other private data
	Impersonation for PIN/password renewal	Someone attempts to impersonate user to reset PIN / password	• Strict rules around password renewal
	Interception of data during transmission	Interception of data as it is transmitted between consumer and POS, or across payment network	• Encryption
5. Customer vulnerability and error	Customer vulnerability	Customer does not understand risks and their responsibilities, liable not to take proper precautions and fall victim to scams	• Customer education of risks and responsibilities • Specific measures e.g. prevent vulnerable PINs/passwords e.g. '1234'
	Communication challenge	Small screen on mobile makes disclosure more difficult	• Experiment / identify best practice
	Customer error	Incorrect transactions made due to customer error	• Monitoring • Rules e.g. limiting repeat transactions of same value to same account
6. System downtime	Internal system issue	Technical errors or other issues cause system downtime	• Business continuity plan • Safeguards against external attacks
	External attack	External attacks for instance denial of service attacks blocking over-the-air payment info being sent	
	Lack of connectivity	Connectivity lost stopping, for instance, cloud-based payments	• Back-up in case of lost connectivity
7. Unfair treatment of customers	Managing customer issues fairly and effectively	Customers not made aware of their rights; customers not being treated fairly in resolution of issues; issues not being resolved in timely manner	• Regulations to protect customers (what rights should be, disclosure, timely resolution)
	Customer privacy	Customer privacy not being effectively maintained e.g. information on usage shared with third parties	• Customer privacy measures

Source: Greenwich-Consulting Research

4.2.2 Mitigation of risks and issues associated with mobile payments

Providers need to have effective policies and processes in place to assess, control and monitor against the kinds of risks and issues described above. Below there is a review of the key measures that regulators and providers should

consider. How these measures are, and should be translated into regulatory requirements will depend on the aims of the regulator and the particular nature of the national market environment.

For what is an extensive and complex topic some elements of regulatory concern have been necessarily reduced or excluded.

A. KYC / AML rules

Measures should be taken to prevent money laundering and terrorist financing both within and across borders. Clear rules and guidance already exist for other financial services and these should be extended to mobile payments. Key measures include:

- Application of 'know your customer' (KYC) rules when originating new accounts, for instance requiring certain types of identification e.g. passport, national identification card, driver's license, utility bills.
- Screening payments against government / economic sanctions
- Transaction limits, or specific customer verification (e.g. interviews) for transactions above set limits

Further measures relating to international remittance include:

- Registration and licensing of provider according to local requirements
- Verification of recipient for transactions
- Other measures in accordance with national rules e.g. sender/receiver transaction limits

B. Safe storage of customer funds

Where providers are financial institutions customer deposits will already fall under existing financial regulation and any mobile payment related accounts should fall under the same banner.

However, when providers are not banks (e.g. for MNO-led services) measures should be introduced to ensure safe storage and easy accessibility of customer funds. Various measures have been introduced across countries including:

- Limiting what providers can do with funds including ring-fencing money against commercially risky activities, requiring high liquidity of investments (potentially much higher than regulated banks)
- Requiring that funds are held in regulated bank accounts and in low risk investments (e.g. Kenyan regulator applied this rule to M-Pesa funds
- Stipulations set in place for what will happen to customer funds in case of provider bankruptcy

It is worth noting that some countries have gone further and insisted only regulated financial institutions can accept customer deposits.

C. Authentication and Authorisation

Providers must authenticate that transaction requests are legitimate and prevent unauthorised individuals gaining access to mobile accounts. For instance this should cover a mobile phone being stolen and the mobile payments being attempted. Measures to support this include:

- Various authentication means including PINs, passwords, signature, and biometrics (e.g. finger print scans, voice scans)
- Use of multi-factor authentication to provide a backup if one measure e.g. PIN is compromise
- Mobile device and application features such as additional passwords and automatic log-outs
- PIN and passwords etc may need to be renewed at support point, but strict measures around customer identification should be enforced to avoid impersonation.

Further, a feature of smartphones and emerging mobile wallet solutions is that multiple accounts (e.g. credit and debit cards) and application may be stored on the same device. There is a role to ensure only the authorised applications and parties can access relevant account information. In some cases this has fallen to a Trusted Service Manager, a third party not connected with the MNO/Financial Institution or other parties involved, with responsibility for:

- Manage and administer account information
- Control which apps / parties can receive data
- Manager the lifecycle of the device including deactivation at appropriate time

Finally, a fall back in case account details are compromised is the ability to remotely deactivate an account and wipe all sensitive data from a device.

D. Encryption / maintenance of data integrity

Any data either held on systems or mobile devices, or transferred between parties should be protected both from being read and being altered by unauthorised parties. Measures to support this include:

- End-to-end encryption of data covering 'static' data held on SIMs/secure elements or in the cloud, and data sent and received by parties in the transaction process
- In the case of data being held in the cloud measures to prevent cyber-attacks and related threats
- Internal systems and controls within providers to ensure account and transaction information are kept safe

E. Other technology measures

All technologies involved in mobile payments should be subject to a set of standards and controls. As discussed in Section 5.1 industry certifications based around a set of specifications and standards have been established, and providers should only use certified technologies.

The following, in addition to encryption of data discussed above, are some measures to combat specific technology related risks:

- Due diligence on POS terminal providers, and merchants, to ensure against device tampering
- Testing and certification of mobile payment applications to protect against bad applications
- Installing of anti-virus software to protect against downloading viruses and related malware

F. Diligence on third parties

Transactions are more exposed to risk when multiple parties are involved in providing services and when one or more parties do not fall under clear regulatory jurisdiction or guidelines. Providers should ensure effective due diligence and management oversight of all outsourcing relationships and other third party dependencies.

Measures will vary depending on the third party involved. The following is an example relating to retail agents used for customers to deposit and later access funds:

- Due diligence on agents including KYC measures
- Ensuring effective on-boarding and training of staff
- Ensuring physical security of premises e.g. having a vault / guard
- Monitoring of performance and acting on issues that arise

G. Customer education and disclosure by providers

For all financial services it is important for customers to be informed of the risks involved and their rights. This is particularly relevant for mobile payments that are relatively new services – unbanked customers more likely to have low financial literacy, banked customers may expect mobile services to act in similar ways to existing financial services but, particularly when provided by non-banks, this may not be the case. Measures to mitigate against this include:

- Communication on risks involved in mobile payment services and means to mitigate against them e.g. safeguarding on PIN/password
- Communication of customer responsibilities and rights if something goes wrong (covering customer error, provider error, or other issues like fraudulent activity)

- Experimentation and applying best practice for effective disclosure through mobile channel given small screen

While obligations should fall on providers to educate customers, it will also likely be a role of regulators to support this as a broader push to improve financial literacy in the country.

H. Policies, Internal Systems and Controls, and Compliance

Treatment of Customers and Customer Privacy

Customer rights should be specified in a range of circumstances including customer error, provider error, and incidences of fraudulent activity. As well as being communicated effectively these policies should treat customers will an acceptable level of 'fairness'. A definition of fairness will vary between markets and be subject to governmental and regulatory preferences.

As an example of this the UK's Financial Services Authority (FSA) puts the principle of 'Treating Customers Fairly … [as] central to the delivery of [the] retail regulatory agenda, which aims to ensure an efficient and effective market and thereby help consumers achieve a fair deal'. Elements of this include financial institutions presenting information openly and having 'no unreasonable post-sale barriers'.[18]

In addition to having acceptable customer policies in place providers should also resolve issues in a timely manner. Again the definition of 'timely' will vary by market, but regulators can take a lead from adjacent examples such as time limits for disputes to be solved in 'conventional' financial services or a retail environment.

Appropriate measures should be put in place to protect customer privacy. A starting point will be accommodating privacy regulation and laws of the region. Customers should be made aware of the provider's privacy policies, and have the option to opt-out of certain uses of data e.g. sharing with third parties.

Monitoring and Audit Trail

Providers should have appropriate means in place to monitor transactions and other account activity for suspicious behaviour. Key measures could include:

- Identification of what constitutes 'suspicious activity' and/or customer errors
    - For example frequent small payments made between accounts may be evidence of fraud as an intruder seeking to empty an account without hitting transaction limits
    - Equally repeat transactions of the same value to the same account could be evidence or a customer error who only intended to make the payment once
- Measures to flag behaviour both internally and to the customer, the later for instance being via text message alerts
- Limits and automatic blocks on accounts when suspicious activity is detected

Providers should also ensure that clear audit trails for all transactions and other account activity as a fall-back in case issues arise and need to be rectified.

Security of networks and operating systems

In addition to the security of data transmitted through the payment network, the security of the provider's internal systems is of paramount importance, particularly when stored account information is an attractive target for cyber-attacks. Another related risk is denial-of-service attacks on provider networks. Protective measures should include:

- Effective security controls over provider networks and operating systems
- Secure housing of computers and network equipment

Business Continuity Planning

Providers should have effective business continuity and contingency planning processes in place to ensure the ongoing availability of services. For non-bank providers requirements are likely to be more stringent than other services they may provide. Continuity and contingency planning is another big topic, but some key elements are:

- Ensuring systems and processes are able to cope with level of demand
- Appropriate business continuity plans including processes to restoring/replacing transaction processing capabilities, and disaster recovery
- Existence of contingency back-up systems in case of business disruption for instance through denial of service attacks

Management Oversight and Compliance

A final element to ensure mitigation of risks is effective management oversight of the kinds of policies and processes described above, and effective compliance to regulatory rules. The former should include executive level risk management oversight, and the later regular and accurate compliance reporting to relevant bodies. Regulators also have a role to play in enforcing regulations effectively and ensuring compliance.

4.2.3 Regulatory Concerns around Virtual Currencies

In a similar way to some mobile payments services, regulation around virtual currencies remains unclear and in some cases non-existence. For example virtual currencies sit outside the EU's definition of electronic money set out in the eMoney Directive[19]. As adoption rises and potential uses (and misuses) of virtual currencies expands though they are seeing increasing regulatory attention.

Concerns include a destabilising effect on economies of currencies that are not managed by any monetary authority. In 2009 China introduced rules to prevent virtual currencies being exchanged back for real currencies[20]. Bitcoin recently gained significant attention as its exchange rate for 'real currencies' fluctuated dramatically at the start of 2013 from USD 20 in February to a high of USD 250 before falling to USD 150 in April[21].

There are also significant concerns around money laundering. In May 2013 a criminal indictment was brought against Liberty Reserve in the US charging the company with running a money laundering operation that authorities estimate involved 55m transactions and laundered money of USD 6 billion dollars making it the largest case ever in cross-border money laundering[22].

These and related issues remain unresolved in many cases and will be an important focus particularly for financial services regulation, but also other bodies with a stake in overseeing digital payments.

4.3 Adaptation of Regulatory Approach to Fit Market Context

Regulators who want to promote the spread of services face a balancing act of allowing providers enough freedom for innovation, whilst giving consumers and businesses confidence that they are protected and their legal positions are clear.

Strong regulatory frameworks will protect consumers but at an early stage of development in most markets may limit innovation and stop the development of improved services. At the same time overly light or unclear regulation risks customers facing issues and losing trust in services, and providers not being willing to invest when their liabilities are unclear – both of which will severely impact the spread of services.

4.3.1 'Test and Learn' approach to developing regulation[23]

With many markets still at a relatively early stage it is hard to predict how services will develop. Whilst setting out a clear regulatory framework in advance may be desirable, in practical terms it is hard to do so covering all eventualities and without becoming overly prescriptive. A pragmatic approach is to set a relatively open regulatory framework and then continue to develop regulation as the market evolves and issues arise.

The Central Bank of Kenya's oversight of M-PESA is a classic example of this (see Figure 4.4) adopting a very open stance to regulation, allowing M-PESA to experiment and built its business relatively freely, and then developing clearer regulations as the scale of the service increased, and potential risks and issues with the service became clearer.

Figure 4.4: Case Study: Central Bank of Kenya's oversight for M-PESA

Central Bank of Kenya (CBK) had two of its departments engaged in evaluating the M-PESA proposal for the 2007 launch. The Financial Institutions Supervision Department (FISD) was enquiring whether M-PESA service is stretching or breaking any rules in the financial industry. National Payment System Department (NPSD) on the other hand viewed M-PESA more as a payment system than the financial institution and hence was more open to permit experimentation with the MNO-led model. Overall, the CBK handled the process on a relatively ad-hoc basis allowing M-PESA to launch with basic regulation compliance and a lot of free space to experiment. When the number of customers was growing at higher than expected rates and the mobile payment products were introduced CBK developed regulations further working with the provider.

Source: Greenwich-Consulting Research

Depending how openly regulation is defined this 'wait and see' approach can increase the risk of misuse. But this can be mitigated by specific measures such as putting relatively strict transaction limits on payments and deposits and also by ensuring regular and on-going communication with providers.

4.3.2 Setting regulation in proportion to risks

Rather than applying catch-all regulations to financial services, regulation should be tailored based on realistic assessment of the risks involved to avoid over-burdening services when the associated risks are small.

This should also take into account the alternatives currently in use. For issues like money-laundering cash transactions make it very difficult if not impossible to track which parties are making or receiving payments. As cash transactions are replaced by electronic means, payments become significantly easier to track. So even if regulations are relatively light mobile payments are likely to be safer than cash transactions. This creates an incentive from a security point of view to increase the adoption of mobile and other sorts of digital payments.

A key tool that can be employed by regulators is the ability to impose limits on transactions and deposits. In the case of transactions for instance this could be a limit on the size of any single transactions, or daily, weekly, or monthly limits. So long as these are enforced it provides a simple way for regulators to manage risk.

Combining limits with a philosophy of risk-based regulation can enable relatively light frameworks that enable service adoption while still mitigating against significant risks. Selected examples are provided below:

Example: Lowering KYC/AML barriers

One example of balancing availability of services with prevention of misuse is customer due diligence (KYC) requirements for setting up new customer accounts. Many unbanked customers, particularly in emerging markets, may not have access to identifying documents (e.g. ID, proof of address) that would typically be required. At the same time there are genuine risks of overlooking this such as money laundering.

The Central Bank of Nigeria provides an example of a regulator taking a risk based approach to this issue, as shown in Figure 4.5, lowering KYC requirements for low risk accounts[24]. Basic accounts can be opened with only a full name and a telephone number, but have strict limits on transactions, deposits and withdrawals. Customers can upgrade to accounts with less restricitions but the ID requirements are higher.

Figure 4.5: Central Bank of Nigeria KYC requirements applied to MyPaga services

Customer Level	Verification Requirements	Per Transaction	Daily limits		
			Other transactions	Deposits	Withdrawals
Level I	Phone Number and Full Name	N 3,000[1]	N30,000	Up to N50k at Paga agents; N150k at bank branches	Up to N50k at Paga agents; N150k at bank branches
Level II	Phone Number, Full Name, Full Address and Copy of Verifiable ID Card to be provided to agent	N 10,000	N100,000	Up to N100k at Paga agents; N250k at bank branches	Up to N100k at Paga agents; N250k at bank branches
Level III	Same as for Level II, plus additional KYC as would be required when opening a bank account	N100,000	N1,000,000	Up to N100k at Paga agents; N1m at bank branches	Up to N100k at Paga agents; N1m at bank branches

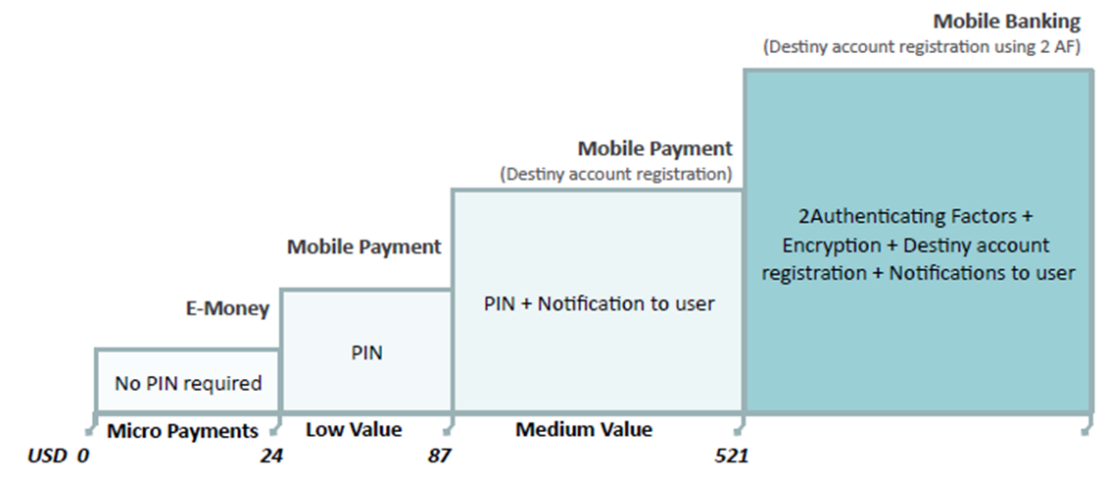
1. Nigeria Naira to US Dollar exchange rate is 158:1 (as of May 2013)

Source: Greenwich-Consulting Research

Example: Lowering authentication requirements

Authentications help ensure that transactions are legitimate. At the same time they may present a barrier to adoption by adding some complexity to the payment process for customers and providers. Mexico provides an example of a risk-based solution where authentication requirements for very small payments are minimal, but steadily escalate with the size of the transaction with larger transactions requiring multiple authentication factors and user notifications

Figure 4.6: Progressive risk managements structure in Mexico



Source: Banco de México

4.3.3 Support of Industry Development

There is a potential further role for regulators in helping to tackle some of the types of challenges raised in Section 3 around consumer and merchant adoption, and supply-side issues. A number of strategic suggestions are provided below, encouraging debate around these and other ways regulators can support industry development:

- Carrying out consumer research to support industry understanding of customer needs and barriers to wider adoption[25]
- Supporting to raise consumer and merchant awareness of the availability and benefits of mobile payments and banking services
- Supporting industry pilots to test new services and reach new customer groups
- Boosting demand for mobile payments by working with government departments to make payments such as welfare and pension payments via mobile services
- Support an industry move to interoperability of services [26]

The last point on interoperability is particularly important and can have a significant impact on service uptake. The example of credit card services where "an initial rapid deployment slowed in the face of low usage …[but was] followed by exponential growth immediately after interoperability was introduced' was noted in a Report from Analysys Mason[27]. Forcing interoperability at an early stage may harm the commercial incentive to set up services and innovate, however widespread adoption of mobile payments is almost certainly dependent on interoperability and telecoms regulators should consider being prepared to support this as the market develops.

5 Conclusions

There is continuing momentum around mobile payments with the value of transactions growing at 50%+ year on year in many regions and the number of launches gathering pace. Oft cited success stories like EcoCash in Zimbabwe, MTN Uganda, SMART Money in the Philippines and M-PESA in Kenya demonstrate the potential not only for rapid adoption but also how providers have quickly extended the breadth of services they offer. Innovation in services offered has also been matched in *how* they are offered and by who with a wide variety of models adopted and a proliferation of non-bank providers. However, while there are many positive signs there remain challenges with many providers struggling to meet albeit high expectations.

From a consumer point of view some challenges around awareness and recognition of benefits will need to be fixed by the market, and similarly for merchants struggling to decide which services to accept. There is however a role for telecom regulators for instance in continuing to tackle security concerns, and addressing, if not already doing so, interoperability which can make services more appealing to users.

Provider challenges are characteristic of new markets including fragmentation of supply, a lack of established standards, and understanding on the best business model to adopt. Again, much of this will be addressed by the market as it evolves. But there is also a supportive role from regulators here that is being played to different extents in different countries. Part of this is simply helping providers to understand which regulations apply to them specifically and what the implications are. Another part is the setting, or fine-tuning of regulatory frameworks to manage concerns for instance around security, but in a way that is proportional to the risks involved and allows for, or even encourages, innovation.

Mobile payments and banking services see the intersection financial services regulation, telecoms, technology and retail/consumer protection, and implies a break from the past for all parties involved. With the local nature of adoption of services and existing regulatory set-up, responses of different regulators to these changes have varied. What it does call for is on-going collaboration between the different types of regulators within regions, and also across regions to understand local practices, share knowledge and consider cross-border frameworks.

A key role for regulators is clearly developing regulations to protect consumers and prevent misuse. However there is often a trade-off between the protection given by strong regulation, and the ability to create an enabling environment for adoption of services. When markets are new and still evolving a pragmatic approach is to set a relatively open regulatory framework and develop regulation as the market evolves and issues arise – Kenya provides a good example of this with M-PESA.

Further, regulations should be set in proportion to the risks involved, and using tools like transaction limits – Nigeria and Mexico are good examples of this approach in action. Measures beyond specific regulation can include carrying out consumer research and raising consumer awareness of services, supporting pilots into new areas, and also

supporting a move towards interoperability – on the later point, Mexico and Nigeria again are examples, along with Ghana and India.

To summarise, while many of the issues facing what is still a very promising industry will be met by the market, the role of regulators will also be a defining factor.

[1] This can be true even in developed markets – Boston Federal Reserve report that users notice a missing mobile phone 4-8 times faster than a wallet; text about suspicious activity can be sent instantly and reach customers at any time and place; mobile phones can provide an extra layer of authentication in the form of a user set device password

[2] APAC mature covers 'economically developed' countries in Asia Pacific such as Japan and South Korea

[3] See GSMA's Mobile Money for the Unbanked tracker at http://www.gsma.com/mobilefordevelopment/programmes/mobile-money-for-the-unbanked/

[4] Visa, The Future of Technology and Payments, Edition 2

[5] Demirguc-Kunt and Klapper, 2012

[6] GSMA paper International Remittance Service Providers: An Overview of Mobile International Remittance Service Provider Service Offering (2010)

[7] http://europa.eu/rapid/press-release_IP-13-415_en.htm

[8] Consumers and Mobile Financial Services 2013, Board of Governors of the Federal Reserve System

[9] Refers to the provider of the mobile payment service, not the provider of debit or credit card used

[10] Merchandise purchases refer to a user case of a mobile payment on purchases of physical merchandise either in-stores or on-line using a smartphone; ticketing refers to mobile payment for purchase of tickets for the use of public transportation and entertainment events; p-paid top ups refer to top-ups of prepaid services such as mobile phones, fixed lines, internet services, and gift cards –top ups can take the form of both MMT and P2P type services

[11] For instance as pure payment providers consider moving into more advanced mobile banking services including offering interest bearing accounts

[12] "At the level of ITU, Study Group 13 (Future Networks) has developed two Recommendations related to securing mobile financial services. Recommendation ITU-T Y.2740 elaborates approaches to developing system security for mobile commerce and mobile banking in the next generation networks (NGNs). Recommendation ITU-T Y.2741 specifies the general architecture of a security solution for mobile commerce and mobile banking in the context of NGN. It describes the key participants, their roles, and the operational scenarios of the mobile commerce and mobile banking systems. It also provides examples of implementation models for mobile commerce and mobile banking systems. ITU-T Study Group 2 is currently working on the development of a Recommendation on Telecom Finance, which will provide an overview of mobile money services from the operators' perspective to enhance the customer experience in telecom service and strengthen B2B, C2C and B2C financial infrastructure." Extracted from the ITU-T Technology Watch Report on Mobile Payment revolution, at: www.itu.int/en/ITU-T/techwatch/Pages/mobile-money-standards.aspx.

[13] Ovum, Mapping Mobile Payments, 2012

[14] See Federal Reserve Bank of Boston, Mobile Payments and Technology Landscape, 2012 for discussion on regulatory challenges in the US market.

[15] A proprietary security standard for organisations handling cardholder information

[16] In a lot of cases so far telecoms regulators simply defer to the existing financial services regulatory regime, but this is not necessarily the optimal case

[17] Refer to the following documents as further reading on the subject: Risk Management Principles for Electronic Banking, Bank for International Settlements (2003) and Mobile Financial Services Risk Matrix, US Aid with multiple authors (2010)

[18] See FSA http://www.fsa.gov.uk/doing/regulated/tcf

[19] European Commission, Digital Agenda for Europe, 'Legal Analysis of a Single Market for the Information Society' (2011)

[20] http://edition.cnn.com/2009/TECH/07/01/china.virtual.currency/index.html

[21] Economist, 'How does Bitcoin work?' (2013).

[22] Economist, 'Taking a Liberty' (2013).

[23] The concept of a 'test and learn' approach is referred to in the Alliance for Financial Inclusion (AFI)'s Policy Note *Mobile Financial Services: Regulatory approaches to enable access,* which refers to the G20 Financial Inclusion Experts group's paper *The Principles for Financial Inclusion* http://fas.imf.org/misc/G20%20Toronto%20Principles%20for%20Innovative%20Financial%20Inclusion.pdf

[24] Source: Service provider MyPaga's website: https://www.mypaga.com/paga-web/mobile/terms.paga

[25] For example the kind of research carried out by the US Federal Reserve Board in their *Mobile Financial Services Survey (2012)*

[26] Interoperability is discussed in detail in the GSR Paper The Regulatory Landscape for Mobile Banking (2012); examples of regulators taking more extreme action and requiring degrees of interoperability include Mexico, India, Nigeria and Ghana

[27] Analysys Masons, Mobile Payment in Asia: Regulatory Changes could Stimulate this Fragmented Market (2012)