The Mobilisation of Banking Law

Caroline Bergin-Cross is a PhD candidate at University College Dublin and the author of 'Electronic Fund Transfers in the Republic of Ireland', published in 2015 by Lonsdale Law Publishing. She is a Barrister-at-Law and holds LLM (Comm) and BCL degrees. She is currently the Editor-in-Chief of the University College Dublin Law Review.

Dear Editor,

The spread of mobile phones across the developing world is one of the most remarkable technology stories of the past decade. Consumer adoption of smart phones is growing internationally at a phenomenal rate. Smart phones present significant m-commerce opportunities for all organisations, however, such potential has yet to be realised. To realise such potential there must be engagement with mobile service providers in order to make m-payments secure, private, reliable and easy to effect. The first part of this letter will illustrate what an m-payment is. Part two shall look at the growth of mobile banking, taking into account the implications of same, especially in respect of regulation and privacy. Finally, this letter will discuss the future development of m-payments.

1.1. WHAT IS AN M-PAYMENT?

A mobile payment (m-payment) may be defined, for our purposes, as any payment where a mobile device is used to initiate, authorise and confirm an exchange of financial value in return for goods and services. M-payments are a natural evolution of e-payment schemes that facilitate m-commerce. Mobile devices may include mobile phones, wireless tablets and any other device that connect to mobile telecommunication networks and make it possible for payments to be made. The realisation of m-payments will make possible new and unforeseen

ways of convenience and commerce.

There is no universal form of m-payments; rather, purposes and structures vary from country to country. The systems offer a variety of financial functions, including micropayments to merchants, bill-payments to utilities, person-to-person transfers between individuals, and long-distance remittances. Currently, different institutional and business models deliver these systems. Some are offered entirely by banks, others entirely by telecommunications providers, whilst others involve a partnership between a bank and a telecommunications provider.

Mobile phone operators have identified m-payments as a potential service to offer their customers, which will increase loyalty, and generate fees and messaging charges. Financial institutions see m-payments as a form of 'branchless banking'. Government regulators see a similar appeal but are presently working out the legal implications of the technologies, particularly concerning security and taxation.

1.2. EFFECTING AN M-PAYMENT

M-payments may broadly be classified as a 'contactless' or 'remote' payment. In a mobile 'contactless payments', the payer and payee and the mobile telecommunications device are in the same location and communicate directly with each other using contactless radio technologies, such as near field communications, which use Bluetooth or infra to transfer data. For mobile 'remote payments', the transaction is conducted over telecommunication networks such as the internet, and can be conducted irrespective of the location of the payer and their mobile telecommunications device. Creating ease, convenience and trust for end-customers is regarded as critical for the further development of m-payments.

2.1. M-PAYMENT MODEL

In m-commerce, it is often required that personal data, as well as financial data, be exchanged among the transacting parties to facilitate the purchase. This sharing of personal data imposes a risk in the case of data misuse. Even if consumers' personal data is used correctly, consumers inevitably have to forfeit parts of their privacy when interacting with businesses online. Consequently, trust in the vendor is essential for the necessary disclosure of personal information.

2.2. BENEFITS AND DISADVANTAGES

The benefits of m-commerce will not be realised until the tangible benefits outweigh the intrusion and privacy concerns of consumers. While m-commerce can provide significant benefits and efficiencies for consumers, the potential risks have to be evaluated and appropriate data protection and privacy safeguards must be established, monitored, and reviewed, to lower this risk and significantly reduce any fears that consumers may harbour. Authentication, confidentiality, data integrity and non-repudiation are key issues cited by consumers.

Consumers' perceptions of the security and privacy controls employed by smart phone service providers are a critical element of their willingness to make m-payments. Such controls should be specified in legislation and governments should adopt legislation which stipulates the standards of service, thereby setting the legal rights of m-commerce consumers. To ensure the robustness of this legislation and governance, an independent objective third party regulatory authority should be established to ensure service providers are fulfilling their obligations under the m-commerce legislation. Furthermore, this will improve consumer confidence that regulatory bodies have sufficient powers to take actions against mobile service providers who do not adhere to such frameworks. Such legislation will help build consumer trust in m-

payments and rebut concerns that their personal data can be violated or captured during transmission or by hacking databases and spoofing identities.

2.3. MAIN ISSUES AND CONCERNS

Security

For widespread use and customer acceptance of m-payment services, both perceived and technical levels of security should be high. For customers, privacy should not be compromised and there should be no possibility of financial losses. For businesses, customer authentication is important. As per the general framework of any secure messaging system, confidentiality, integrity, non-repudiation and authentication should be guaranteed by m-payment service providers.

Standards

M-payments lack cohesive technology standards. Consolidation of standards in the m-commerce arena is critical and will enable producers and consumers to make investments that produce value. The lack of standards gives rise to many local and fragmented versions of m-payments offered by different stakeholders. Standards need to address security and privacy concerns of consumers as well as interoperability between various stakeholders. Standards formation is a process of negotiation between various stakeholders, more like political negotiations than technical discussions. There is currently no consensus in respect of m-payment standards setting. Certain start-up companies have proposed standards and they hope to make these de facto by being the first movers with strategic advantage and early market selection. The battle over standards occurs both at the firm level and at the inter-consortia level.

Regulatory Issues

Although m-payments may allow parties to make economic exchanges, it is not a form of recognised legal tender. That is, it lacks the status of other payment instruments such as cash, which is a medium of exchange that is authorised, adopted and guaranteed by the government. To overcome this problem, legislation that will make m-payments legal tender must be enacted.

3.1. FUTURE OF M-PAYMENTS

The European Payments Council (EPC) published the latest version of its white paper on m-payments in October 2012. This paper incorporated submissions from 17 parties representing various stakeholders in the m-payments ecosystem.[1] On 29 June 2015, the ERPB, chaired by the ECB, considered the future of person-to-person m-payments and the recommendations of the White Paper. The members of the ERPB subsequently agreed to endorse the vision of allowing any person initiate a pan-European person-to-person m-payment safely and securely, using a simple method with information the counterparty is prepared to share in order to make a payment. In particular, payment service providers offering person-to-person m-payment services should make use of existing infrastructure as far as possible.[2] Moreover, a harmonised process should be created, allowing person-to-person m-payment data to be exchanged between local solutions across borders. It is most unfortunate that the EPC has taken a deferential approach and has decided against introducing regulations or directives to harmonise m-payments across the EU.

3.2. APPLE PAY

Apple Pay is simple to use and works with the cards already owned on devices used every day. As your card details are never shared when you use Apple Pay, and are not stored on your

[1] These included infrastructure manufacturers, service providers and retail organisations.
[2] For example IBANs.

device at all, using Apple Pay on your iPhone, Apple watch, or iPad is the safer and more private way to pay. However, customers need to use a bank card from one of Apple Pay's partners.[3]

If the customer has a credit or debit card registered with their Apple ID, they can add it to Apple Pay directly. If not, or the customer wishes to add a new card, Apple encrypts the whole process, wrapping up the card details in a unique identifier before handing it over to their card operator.

Assuming the customer is credit-worthy, the operator sends back an authorisation key that is stored in the Secure Element in the iOS device or watch. Secure Element is an industry standard chip and the customer is not relying on Apple alone to maintain the technology. As each one is unique to the device in which it resides, it reliably ties the device to the customer's account. That way, the card processor knows exactly whose account to debit without passing their details over the network again or handing them to the retailer itself.

Apple Pay has proven to be an extremely safe and secure form of m-payment. To use the payment the customer inputs a six digit passcode rather than four, and payments can only be authorised from iOS devices with near field communication and the device-unique Secure Element chip built in.

CONCLUSION

Many challenges must be overcome for m-payments to be widely accepted as a mode of payment. Businesses, merchants and consumers have to come forward and make value-producing investments. A regulatory framework and widely accepted standards will be the

[3] Current Apple Pay partners are NatWest, Nationwide, RBS, Santander, Ulster Bank, American Express, MBNA. HSBC, first direct, Bank of Scotland, Halifax, Lloyds Bank, M&S Bank and TSB Bank.

pillars on which m-payment applications will be built in order to have a robust system which consumers have confidence in.

Consumers' fears over their data and privacy appear to presently outweigh consumers' perceived benefits of m-commerce. Consumers' unwillingness to make m-payments is the greatest barrier to future growth of m-commerce.

Apple Pay has shown that a convenient, secure and reliable m-payment system can be established, however, the deferential approach by the EPC to setting standards and regulations for m-payments is unfortunate. Without a standardisation of m-payments, customers' unwillingness to use m-payments will continue.

Is mise le meas,

Caroline Bergin-Cross BL