MOBILE PAYMENTS

Singapore’s authorities turn their attention to m-payments

Quek Li Fei, Simon Trevethick and Paul Yap of Colin Ng & Partners LLP analyse mobile payments in Singapore, examining the attention Singapore’s authorities are now giving to the technology and infrastructure integral to this sector.

The term ‘mobile payments’ (or ‘m-payments’) encompasses a number of different models; for the purposes of this article, we have taken the term to mean the use of a mobile phone or other mobile device loaded with the necessary software as a payment instrument in itself, as opposed to the use of the mobile phone as a means to access existing online banking and other payment services. In this regard, we refer to m-payments in the context of the ability to use a mobile phone to make contactless or Near-Field Communication (‘NFC’) payments for goods and services at the point of sale.

Due to the high degree of reliance on technology and the sensitivity of personal and financial information, authorities in Singapore have come up with appropriate measures to regulate the m-payment industry.

The state of m-payments in Singapore

Whilst mobile banking services have been around for some time, the technology and infrastructure for m-payments has only received attention more recently from the Singapore authorities. These include the Infocomm Development Authority of Singapore (‘IDA’) and the Monetary Authority of Singapore (‘MAS’). On 25 October 2011, the IDA announced that from the middle of 2012, consumers may use m-payments to effect various consumer-type purchases. This was made possible through the Call-for-Collaboration (‘CFC’) by the IDA with industry players to deploy a nationwide interoperable NFC infrastructure as part of the IDA’s Next-generation e-Payments Programme. This program was developed as part of the IDA’s Intelligent Nation 2015 (‘iN2015’) Masterplan. The crux of the iN2015 Masterplan is to grow the information and communications (‘Infocomm’) sector and to use Infocomm technologies to enhance the competitiveness of key economic sectors. As of 3 August 2012, over 30,000 retail points accepted m-payments for the purchase of goods and services. It must be noted, however, that m-payments at such retail points are mostly low-value consumer-type transactions.

The CFC was awarded to a consortium of companies comprising Gemalto Pte. Ltd., Citibank Singapore Limited, DBS Bank Ltd., EZ-Link Pte Ltd, as well as the three local MNOs: M1 Limited, SingTel Mobile Singapore Pte. Ltd. and StarHub Mobile Pte Ltd. Gemalto is developing and operating the neutral Trusted Third Party’s infrastructure, whilst DBS, EZ-Link and Citibank will enable a wide range of their credit/debit scheme cards and stored value payment products to be issued through Gemalto and stored on the secure chips on the user’s NFC-enabled mobile phones. Users will be able to pay for their purchases using any of those payment products at NFC-ready retail points. To enjoy the use of m-payments, however, users need to be equipped with NFC-enabled mobile phones, which are sold by local MNOs.

M-payment software applications provided by MNOs in Singapore include the SingTel mWallet Application; in general, these m-payment applications allow users to store their credit cards, to store tickets and vouchers, to read NFC promotion codes, and to perform transactions seamlessly with the use of a single device.

Risks faced by the various stakeholders

The MAS and banks in Singapore: The MAS is concerned about the security of m-payments, specifically their susceptibility to fraud, theft and loss, as well as unauthorised storage or use of confidential information, and the security of the system from malicious attacks.

On 21 June 2013, the MAS issued the Technology Risk Management Guidelines (‘TRM Guidelines’), technology-neural guidelines that consolidate past circulars on endpoint security and data protection, information systems reliability, and the availability and recoverability of lost data. The TRM Guidelines explain that m-payments are extensions of online financial services and payment services, which banks offer and are accessible from the internet. The MAS has recommended that the banks implement security measures similar to those of online financial and payment systems onto m-payment systems, particularly measures to counteract payment card fraud.

The MAS has also cautioned banks against theft/loss of phones, and advised that banks should thus ensure there is adequate protection of sensitive and confidential information involved in m-payments. In this regard, banks should have sensitive and confidential information encrypted to ensure the confidentiality and integrity of the information in storage and transmission. Banks should conduct the processing of sensitive and confidential information in a secure environment. Finally, banks are...
strongly encouraged to educate their customers on security measures to protect their own mobile phones from malicious software that may harm the mobile phone and the m-payment system.

The MAS also released a Notice on Technology Risk Management for various industries on 21 June 2013 (the ‘TRM Notices’), technology-neutral notices setting out legal requirements relating to technology risk management for financial institutions as a whole, including requirements for a high level of reliability, availability and recoverability of critical IT systems, and for financial institutions to implement controls to protect customer information from unauthorised access or disclosure. The TRM Notices will take effect on 1 July 2014. Financial institutions that fail to comply with any of the requirements will be in contravention of the enabling legislation under which the respective TRM Notices are issued.

Further, the MAS has, in collaboration with the Ministry of Home Affairs and the Ministry of Finance, published the Singapore National Money Laundering and Terrorist Financing Risk Assessment Report 2013 (the ‘NRA Report’). The NRA Report articulated that terrorist and criminal elements have been quick to exploit new payment technologies and trends to carry out illicit activities and covertly move funds.

New payment technologies such as m-payment technology (therein referred generally to payments made on mobile phones, and not specifically NFC payments) have enabled fund transfers to be made from and to almost anywhere in the world. The MAS has flagged the risk that terrorists and other criminal elements may exploit the opportunity to execute financial transactions where there is no requirement for know your customer and customer due diligence processes conducted by banks or MNOs. However, the requirement that an account be set up with a bank and an MNO in order to use m-payments in Singapore would tend to lower the likelihood of m-payments (as defined in this article) being exploited for illicit activities.

Consumers, service providers and retailers: Consumers would be concerned with the integrity of the nationwide interoperable NFC infrastructure when providing their personal data to service providers. Service providers (e.g. EZ-Link, the MNOs, financial institutions such as banks and Gemalto) will have to ensure that they abide by the Personal Data Protection Act (in particular, Part III to Part VII thereof, relating to personal data protection which will come into force on 2 July 2014), particularly since these service providers possess a large volume of consumer information. Retailers would also be concerned with the device authentication. In the past, magnetic strips were the Achilles heel of payment card security, but with advances in technology, SIM cards and accredited mobile phones they are now less susceptible to cloning and counterfeiting.

Conclusion

While growing in popularity, the usage of conventional NFC payment systems (e.g. Visa ‘PayWave’) still remains relatively insignificant, accounting for 0.2% of transactions in Singapore. It is believed that m-payments in Singapore have not yet reached critical mass, given that they are used in Singapore mostly for low-value payments. Nonetheless, the MAS has taken cognisance of this emerging industry and has attempted to ensure that the identified risks are minimised.

Quock Li Fei Partner
Simon Trevethick Senior Associate Manager
Paul Yap Associate
Colin Ng & Partners LLP, Singapore
ltqquek@cnplaw.com
strevethick@cnplaw.com
pyap@cnplaw.com

1. ‘Mobile Payments’ (Paul Anning, Kate Johnson and Emily Jones, June 2013, Practical Law Company).
4. ‘Near Field Communication Services Go Live in Singapore’ (Infocom Development Authority of Singapore, 3 August 2012).
5. A TTP serves as a single neutral point of contract between the service provider and mobile operators. It provides a secure channel for service providers such as banks and Payment Service Providers (PSP) to send confidential payment information of their customers to a tamper-proof chip in their NFC mobile phones. It is also responsible for managing the payment application on the secure chip, on behalf of the banks and PSPs. A TTP infrastructure eliminates the need for any service provider to establish separate technical connections with individual mobile operators.
6. http://info.singtel.com/personal/phones-plans/mobile/SingTel_mCommerce/mWallet
8. Technology Risk Management Guidelines (Monetary Authority of Singapore, June 2013 at pp 38 and 39).

06