MAYER·BROWN JSM

Legal Update
Banking & Finance
Intellectual Property
Privacy & Security
Technology, Media & Telecommunications
Hong Kong
11 December 2013

Best Practices on NFC Mobile Payments Issued in Hong Kong

Near field communication (NFC) mobile payment services are on the rise in Hong Kong, and are offered in many retail outlets as a payment method. To facilitate the growth of such technology whilst balancing the security concerns of the public, the Hong Kong Association of Banks (HKAB), in consultation with the Hong Kong Monetary Authority (HKMA), has recently issued a Best Practice on NFC Mobile Payments in Hong Kong (Best Practice). The Best Practice is intended to provide the minimum security requirements and other best practices for the development of NFC mobile payments in Hong Kong.

Background

NFC mobile payment services are already offered in Hong Kong by, amongst others, HSBC, Hang Seng Bank and the Bank of China. The Octopus Group is also set to introduce NFC mobile payments as an alternative to its widely popular Octopus card, and Jetco recently announced that it will team up with several banks to build an NFC mobile payment platform. With the growing popularity of NFC mobile payments, concerns have arisen as to the security and infrastructure of this new payment method.

In March 2013, the HKMA released the results of a consultancy study aimed at identifying an effective NFC mobile payment structure designed to achieve the following four long-term development objectives for NFC mobile payments:

1. the ability of users to use multiple payment services from different banks and service providers on a single NFC-enabled mobile phone;
2. the continuity of payment services despite users switching to different mobile network operators;
3. the continuity of payment services despite users changing phones; and
4. a high level of security that is consistent with international standards and regulatory requirements.

One of the recommendations of the study was to develop a set of standards and guidelines that dealt with the implementation of NFC mobile payment services in Hong Kong. To achieve this goal, the HKMA established an NFC task force under the HKAB to formulate the standards and guidelines in consultation with the HKMA. On 25 November 2013, the Best Practice was issued by the HKAB.

The Best Practice

The Best Practice applies to banks that are members of the HKAB as well as other stakeholders of mobile payment services. This includes mobile network operators, phone manufacturers, etc. The Best Practice covers three areas: security requirements, technical standards and operational processes.

SECURITY REQUIREMENTS

The security requirements are the minimum that must be implemented. They cover the security of the backend infrastructure, the frontend device and software applications installed on the mobile phone. They include, amongst other things, the following:

1. Management of Secure Elements – NFC payment credentials must be adequately segregated from each other, by creating secure domain structures and hierarchies.
2. Card Issuance and Provisioning – measures must be implemented to ensure that the connections and data within the NFC environment are secure.

3. Mobile Payment Services Management:
    a. Mobile Wallets – a mobile wallet, which is the software application installed by a customer onto their handset, acts as an interface to manage the NFC services in the secure environment. The safety and security of a mobile wallet is essential.
    b. Management of Multiple Payment Credentials – measures should be implemented to ensure that access controls and authentications in the secure element are put in place, so that only authorised mobile wallet applications can access the assigned payment credentials stored in the secure element.
    c. Authentication Codes – mobile wallets must include PIN protection, which should be stored inside the secure element. Customers may be given the option of turning this PIN protection off, but the default position should always be for the PIN protection to be on.
    d. Access to Sensitive Information – access to sensitive information should only be allowed upon correct PIN entry. Sensitive information should also be adequately segregated where the mobile wallet has multiple NFC payment credentials linked to different issuers. Measures should be implemented to ensure that access to and use of transaction data is restricted to the authorised end-user or the entity that owns the data.
4. Payment Transactions:
    a. Audit Trail and Record – effective procedures and audit trails must be implemented to prevent and detect any unconfirmed transactions. Refunds should promptly be made upon the detection of any unconfirmed transactions.
    b. Transactions Through Contactless Interface – all payment transactions should only be allowed via contactless interfaces, unless effective security measures have been put in place to prevent any potential attacks through a contact interface.
    c. Transaction Limit – NFC mobile credit card payments should be restricted to the same transaction limit that applies to no-signature contactless credit card payments. This is currently set at HK$1,000 per transaction. For transactions that are higher than the current limit, additional security measures must be in place, e.g., provision of a PIN.
5. Cardholder Authentication:
    a. Know Your Customer – the existing KYC due diligence process for normal payment card products should be followed in order to identify the customer. This is mandatory for financial institutions.
    b. At Service Activation – cardholder authentication is mandatory during the activation process. The activation process involves the installation of the mobile wallet application onto the phone, and the insertion of the customer's payment credentials into the application. If an activation code is used as part of the authentication process, then the activation code should be given through a different means from the one used to activate the service, e.g., via SMS.
    c. Mobile Pin Management – mobile PINs should be used in the NFC mobile payment service.

The HKMA will take the Best Practice security requirements into account during its continual supervision of NFC mobile payment services offered by authorised institutions, to ensure that they maintain a high level of security.

TECHNICAL STANDARDS

For the technical standards, the aim was to establish principles with reference to industry and international standards, in order to assist in the interoperability of different NFC infrastructures, mobile devices and terminals. As such, the Best Practice requires the adoption of widely accepted standards set by industry and international organisations. This includes the ISO, ETSI, GlobalPlatform, and EMVCo standards.

OPERATIONAL PROCESS

The Best Practice introduces a standardised operational process, in order to improve user experience. For example, it recommends that for transactions that exceed the current limit of HK$1,000, and for which additional authentication is therefore required, a mobile PIN should be adopted as the method for additional verification.

Other Developments

The HKMA is clearly focused on developing the legal structure in relation to retail payment systems (e.g., mobile payments, stored value payment facilities, etc.) in order to protect the public and, in so doing, inspire consumer confidence which will help further promote the use of new innovative payment methods. Whilst the Best Practice is only a guideline, and does not have the force of law, it may not be long before other measures come into place.

In May 2013, the HKMA and Financial Services and the Treasury Bureau released for public consultation, a proposal on the introduction of a regulatory regime for stored value facilities and retail payment systems in Hong Kong. In brief, under the proposed regime:

1. all issuers of multi-purpose stored value facilities (SVF) in Hong Kong (whether device or non-device based) would be required to obtain a licence from the HKMA before issuing the SVF;
2. issuers of multi-purpose SVFs would be required to keep the float separate from its own funds, which must be fully protected by safeguard measures; and
3. the HKMA would have the power to designate certain retail payment systems which would be subject to the HKMA's continuous oversight.

The consultation period ended on 22 August 2013, and a bill is expected to be introduced to the Legislative Council in the first half of 2014 for its consideration.

Contact Us

For inquiries related to this Legal Update, please contact the following persons or your usual contacts with our firm.

Gabriela Kennedy
Partner
T: +852 2843 2380
E: gabriela.kennedy@mayerbrownjsm.com

Karen H.F. Lee
Associate
T: +852 2843 4452
E: karen.hf.lee@mayerbrownjsm.com