** CONFIDENTIAL **

FAQ on SMS OTP for Card-Not-Present (CNP) ~~Credit~~ Payment Card Transaction

Question:

Apart from e-banking services mentioned in the Supervisory Policy Manual (SPM) module on Risk Management of E-banking (TM-E-1), are there specific security measures that need to be implemented by AIs who act as ~~credit~~ payment card issuers when using SMS one-time-password (OTP) as a means to authenticate the identity of a cardholder for Card-Not-Present (CNP) ~~credit~~ payment card transactions?

Answer:

Currently, FAQ#5 of subsection 4.1 for SPM module TM-E-1 stipulates that AIs are expected to ensure that the authentication factors used for e-banking services are reliable, effective and secure. FAQ#5(1) further suggests security measures that AIs should consider implementing when using SMS OTP as an authentication factor. Among other things, AIs should ensure that the details of a transaction, including the transaction type, transaction amount and partial information about the account number or other identifiers of the payee where relevant, are prominently displayed before the OTP in the SMS message containing the OTP.

Notwithstanding that TM-E-1 does not normally cover controls for managing the risks associated with AIs' credit card business (as set out in subsection 1.2.2), except for certain guidance on ~~the notifications to be sent to customers regarding Card-Not-Present (CNP) credit~~controls over payment card transactions, the risks underlying ineffective or unsecure SMS OTP for e-banking services and CNP ~~credit~~ payment card transactions are similar and may be exploited by fraudsters.

Accordingly, from the perspectives of prudent risk management and customer protection, the HKMA expects AIs to take into account FAQ#5(1) of subsection 4.1 for SPM module TM-E-1, when using SMS OTP to authenticate the identity of the cardholder for CNP ~~credit~~ payment card transactions.