HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

5 October 2021

The Chief Executive
All Authorized Institutions

Dear Sir / Madam,

Authentication and Fraud Prevention Controls for Simplified Electronic Direct Debit Authorization

I am writing to share the results of a recent review undertaken by the HKMA with respect to simplified electronic direct debit authorization (eDDA) and recommend authorized institutions (AIs) to adopt a set of good practices identified during the review.

eDDA is a value-added service of the Faster Payment System (FPS) which enables the payer to pre-authorize his or her account to be debited by direct debit payments. An eDDA instruction can be initiated by the payer (Standard eDDA) or by the payee (Simplified eDDA). The convenience and instantaneous nature of the creation of eDDA instructions has facilitated the development of new usage of direct debit payments with enhanced customer experience. Specifically, by setting up a Simplified eDDA instruction, a bank customer can instantly withdraw funds from one deposit account to another with a different institution, without the need to switch between different internet banking applications. This circular seeks to address this specific usage of eDDA.

In view of the growing popularity of Simplified eDDA service, the HKMA has conducted a review of the robustness of the authentication and fraud prevention controls for the service adopted by AIs. Reference has been made to the relevant requirements in the HKMA's Supervisory Policy Manual (SPM) module on "Risk Management of E-banking" (TM-E-1) and the operating rules of the Hong Kong Interbank Clearing Limited (HKICL). The review has assessed whether the existing controls of AIs are adequate to guard against different risk scenarios. These include the scenarios where the fraudsters have managed to impersonate the customer to open fraudulent bank accounts in his or her name using stolen personal information, and where the fraudsters have obtained access to the customer's existing accounts using stolen authentication passcodes.

The findings of the review underscore the importance for AIs to observe the control requirements stipulated in HKICL's operating rules for Simplified eDDA. Specifically, the payee bank should authenticate the customer's identity before passing on the eDDA instruction to the payer bank; it should provide the customer's personal and account information to the payer bank for verification; and the payer bank should issue a notification to the customer after the setting up or any amendment of a Simplified eDDA instruction.

The review has also identified a set of good practices which can help guard against different fraud scenarios. The HKMA recommends AIs to adopt these practices to strengthen their authentication and fraud prevention controls for Simplified eDDA service. These practices include:

<u>For the Payee Bank</u>

1. Regarding Simplified eDDA instructions raised via e-banking channels as high-risk transactions and accordingly requiring the customer to go through two factor authentication to verify his or her identity;

2. Sending an SMS OTP to the mobile number specified by the customer as an identifier for payment (or putting in place other effective device binding arrangements) when the customer initiates a Simplified eDDA instruction, in order to ensure that he or she is really in possession of the mobile number;

3. Sending both the customer's bank account number and mobile number to the payer bank for verification, instead of sending either one of them as required by the operating rules of HKICL;

4. Setting default single transaction limits and daily limits at the account level, which may be adjusted by the customer after proper authentication;

5. Restricting the creation of Simplified eDDA to transfers between same-name accounts so as to limit the risk of unauthorized transactions to a third party; and

<u>For the Payer Bank</u>

6. Sending an additional SMS notification for each subsequent debit payment, on top of sending an SMS notification to the customer immediately after the creation of a Simplified eDDA instruction and any subsequent amendments.

The HKMA will keep the authentication and fraud prevention controls for eDDA payments under regular review to ensure that they remain robust notwithstanding technological advancement and the evolvement of fraudulent activities. Should you have any questions regarding this circular, please feel free to contact Mr Patrick Lo on 2878-1084 or Mr Patrick Cheng on 2878-1660.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)