Annex

New Anti-Digital Fraud Measures: "E-Banking Security ABC"

Enhancement measure	Supervisory expectation	Implementation timeline
1. "Authenticate in-App"		
a. Account logins and high risk transactions	• AIs should implement arrangements which allow customers with mobile banking Apps to authenticate their logins to Internet banking and high risk transactions through a bound device by default, instead of using SMS OTPs. • Any requests from customers to change this default authentication method should be regarded as a high risk transaction, and SMS OTPs should not be used to authenticate the change. Instead, other authentication methods such as biometric authentication, bound devices, call-back, verification at a physical branch, etc. should be adopted. • AIs may still allow SMS OTPs to be used for authentication under certain scenarios[1]. However, in such cases, AIs should implement appropriate risk management measures, including: i. Applying a "cooling-off" period for high risk transactions[2], so that in the event of fraud, customers have time to review and report any unauthorised activity.	Q4 2025

[1] For instance, (i) where customers have a legitimate need to rely on SMS OTPs (e.g. do not have a mobile banking App); (ii) where customers explicitly opt to use SMS OTPs; and/or (iii) other resilience/contingency considerations.

[2] This "cooling-off" period may be implemented following a risk-based approach. For instance, if an AI assesses a transaction authenticated via SMS OTP to be of higher risk (e.g. it is a large-value fund transfer), it should impose an appropriate "cooling-off" period on that transaction.

	ii. Tightened fraud monitoring of activities and transactions authenticated via SMS OTPs, which should take into account factors such as past transaction history, device information, and relevant fraud intelligence. • AIs can decide whether to implement this measure if their Internet banking platforms do not support high risk transactions, but are highly encouraged to critically consider the merits of doing so.	
b. Device binding and re-binding	• AIs are expected to strengthen the security of device binding and re-binding for individual customers. Specifically, AIs should implement facial recognition[3] or similarly stringent authentication methods rather than relying on SMS OTPs. For the avoidance of doubt, this requirement only applies to new binding and re-binding requests. • AIs may offer appropriate arrangements for customers who encounter difficulties following these device binding requirements (e.g. non-HKID holders). These alternate arrangements should be designed with regard for the latest fraud landscape, their operations and relevant prevailing supervisory requirements[4].	Q3 2025

[3] For the purpose of this circular, "facial recognition" refers to verifying a customer's facial image against the AI's records or the customer's identity document, rather than relying on the facial recognition feature of the customer's own device.

[4] For instance, the HKMA's Supervisory Policy Manual module TM-E-1 "Risk Management of E-banking" and its associated FAQs set out various risk management controls that AIs should implement when using SMS OTPs for device binding and re-binding.

2. "Bye to unused functions"		
	• AIs should provide existing customers with the option to deactivate the online registration of third-party payees and online increase of transfer limits. Once a customer has opted to deactivate a function, AIs should perform a stringent identity verification process (e.g. conducting verification at a physical branch or through facial recognition) before processing any reactivation requests from customers. • For new customers, AIs should also consider providing them with the option to opt out of these high risk functions at the outset when first opening an Internet banking account. • To better protect customers who may choose to keep these functions active for convenience, AIs should review the default fund transfer limits set for both registered and non-registered third-party payees[5], and allow customers to lower these limits at their discretion.	Q2 2025

[5] Since non-registered payees may present higher fraud risk (owing to the absence of registration-related controls), AIs are expected to set a lower default transfer limit for these payees, and at a level which is commensurate with the assessed risk.

3. "Cancel suspicious payments"		
	• AIs participating in the Suspicious Account Alert mechanism should ensure that "High Risk" alerts are displayed for a reasonable duration (i.e. at least 10 seconds), such that customers have adequate time to process and review the stated risks of a transaction before it is executed. • To achieve maximum impact during the alert duration, AIs are encouraged to consider displaying relevant anti-fraud and anti-scam messages.	Q2 2025