



FOR IMMEDIATE RELEASE

Media Release

MAS and ABS Announce Measures to Bolster the Security of Digital Banking

Singapore, 19 January 2022... The Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore (ABS) are introducing a set of additional measures to bolster the security of digital banking, in view of the recent spate of SMS-phishing scams targeting bank customers.

2. MAS expects all financial institutions to have in place robust measures to prevent and detect scams as well as effective incident handling and customer service in the event of a scam. The growing threat of online phishing scams calls for immediate steps to strengthen controls, while longer-term preventive measures are being evaluated for implementation in the coming months.

3. Banks in Singapore, in consultation with MAS, will work to put in place more stringent measures within the next two weeks, including:

- a. Removal of clickable links in emails or SMS sent to retail customers
- b. Threshold for funds transfer transaction notifications to customers to be set by default at \$100 or lower
- c. Delay of at least 12 hours before activation of a new soft token on a mobile device
- d. Notification to existing mobile number or email registered with the bank whenever there is a request to change a customer's mobile number or email address
- e. Additional safeguards, such as a cooling-off period before implementation of requests for key account changes such as in a customer's key contact details
- f. Dedicated and well-resourced customer assistance teams to deal with feedback on potential fraud cases on a priority basis
- g. More frequent scam education alerts.

These more stringent measures will lengthen the time taken for certain online banking transactions but will provide an additional layer of security to protect customers' funds.



4. Customer vigilance remains of paramount importance. Scammers are quick to adapt in targeting unsuspecting consumers. To avoid falling for online banking scams, customers must:

- a. Never click on links provided in SMSes or emails;
- b. Never divulge internet banking credentials or passwords to anyone;
- c. Verify SMSes or emails received by calling the bank directly on the hotline listed on its official website;
- d. Verify that you are at the bank's official website before making any transactions, or transact through the bank's official mobile application; and
- e. Closely monitor transaction notifications so that any unauthorised payments are reported as soon as possible to increase the chances of recovery.

5. Banks will continue to work closely with MAS, the Singapore Police Force, and the Infocomm Media Development Authority (IMDA) to deal with this scourge of scams. This includes working on more permanent solutions to combat SMS spoofing, including adoption of the SMS Sender ID registry by all relevant stakeholders. MAS is also intensifying its scrutiny of major financial institutions' fraud surveillance mechanisms to ensure they are adequately equipped to deal with the growing threat of online scams.

6. Mr Wee Ee Cheong, Chairman of The Association of Banks in Singapore said, "As an industry, we have always focused on the need to ensure robust security measures while meeting customers' expectations for convenient and swift services. Together with the MAS and ecosystem players, the banking industry will continue to strengthen consumer protection measures. We also ask that the public stay vigilant given that scams continue to evolve and are executed quickly. We remain committed to upholding the confidence with which customers can transact online safely, while still maintaining a high level of service."

7. Mr Ravi Menon, Managing Director, MAS said, "MAS is deeply concerned about the recent spate of scams and the financial losses suffered by victims. The threat of scams will not go away, but we can reduce our vulnerabilities. This requires a multi-pronged response across the ecosystem. MAS, together with the Police, IMDA and other relevant government agencies, is working closely with the financial industry, the telco industry, consumer groups, and other stakeholders to strengthen our collective resilience against scam attacks. We will ensure that digital banking remains secure, efficient, and trusted."



8. For more information on phishing scams, please refer to banks' consumer alerts and relevant content on MoneySense website and social media.
