Media Releases

Published Date: 15 September 2021

SMS one-time passwords diverted to perform fraudulent card payments

Singapore's banking and telecommunication systems not compromised

Singapore, 15 September 2021…The Infocomm Media Development Authority (IMDA), Monetary Authority of Singapore (MAS), and Singapore Police Force (SPF) said today that malicious actors overseas had diverted and used SMS one-time passwords (OTPs) to perform fraudulent credit card transactions affecting 75 bank customers in Singapore. These transactions, amounting to approximately S$500,000 in total, occurred between September and December 2020. Customers had reported that they had not initiated the transactions nor received the SMS OTPs required to perform these transactions.

2 Investigations by the banks found that their systems were secure, uncompromised, and not the cause of these incidents.

3 Subsequent joint investigations by SPF and IMDA, with the support of the banks, revealed that malicious actors abroad had gained unauthorised access to the systems of overseas telecommunication operators and used them to modify the location data of the mobile phones used by the victims in Singapore. The malicious actors were thus able to divert to overseas mobile network systems the SMS OTPs sent by the banks to their customers. Having separately obtained their victims' card details, the malicious actors then made fraudulent online card payment transactions and authenticated these transactions using the diverted SMS OTPs. The compromised overseas telecommunication networks have already been identified and notified, while investigations are ongoing to identify the perpetrators and bring them to justice.

4 SMS diversion is a mode of attack that requires highly sophisticated expertise to compromise the systems of overseas telecommunication networks. While our local telecommunication networks are secure and had not been compromised, IMDA, in consultation with the Cyber Security Agency of Singapore (CSA), has required operators to put in place additional safeguards, including specialised firewalls and system safeguards to monitor and block suspicious diversions of SMS.

5 As card details would be needed to perform the fraudulent card payments, we urge members of the public to be alert and vigilant against malware and phishing attempts that seek to obtain their personal details. The public is advised to heed the following:

a) Keep bank account, credit and debit card details safe at all times. Never disclose to anyone these details and the personal identification number, passwords and codes (e.g. OTPs).

b) Keep devices updated with the latest security patches and anti-virus software.

c) Use only credible online services. These includes downloading applications only from official online application stores and making online purchases via trustworthy platforms.

d) Never click on suspicious links from unknown sources.

e) Set low thresholds for payment transaction alerts so that unauthorised activities are detected early. Alert the banks as soon as possible should there be any discrepancies or unauthorised transactions.

6 Banks have reviewed these cases with the assistance of SPF. Given the unique circumstances of these cases, banks will provide a goodwill waiver to affected customers who had taken care to protect their credentials.

***