PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2001- B5770

In the matter of an investigation under section 50(1) of the Personal Data Protection Act 2012

And

Singapore Medical Association

SUMMARY OF THE DECISION

1. On 31 January 2020, Singapore Medical Association (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that the personal data of 68 individuals in 137 emails had been forwarded to an external email address without authorisation between 28 and 30 January 2020. The personal data comprised National Registration Identification Card numbers, dates of birth, indemnity coverage, period of coverage, educational information and financial transaction information.

2. The Organisation believed an unauthorised user ("**UU**") gained entry into the affected Microsoft Office 365 email account by a brute force attack but did not have the system logs to confirm this. Regardless, the unauthorised entry enabled the UU to create an email rule to forward received emails to the external email address.

3. It was found that the Organisation failed to conduct periodic security reviews of its IT system. Consequently, it missed the opportunity to detect the following security issues that could have prevented the incident:

a. There was no periodic change to the passwords of email accounts. As an example, the password to the affected account had not been changed since first use in November 2013.

b. The Organisation collected financial information such as bank account details and swift codes and should have considered, as part of a security review, whether it needed to enhance security measures. For example, encryption of emails and/or attachments containing such sensitive personal data.

c. A reasonable security review would also have noted the absence of security arrangements against brute force attacks. Common examples of anti-brute force measures include limiting the number of failed login attempts and account lockouts. Without anti-brute force measures, a password-protected account could be subjected to unlimited and uninterrupted automated login attempts from the Internet. Given sufficient time, the attacker will succeed in arriving at the correct password.

4. The Deputy Commissioner for Personal Data Protection therefore found that the Organisation did not adopt reasonable steps to protect personal data in its possession or under its control against risk of unauthorised access. The Organisation was in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012. Upon consideration of the facts, a warning was issued to the Organisation. No directions are required as the Organisation had taken actions to address the gaps in its security arrangements.