PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2102-B7951

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

And

Tanah Merah Country Club

SUMMARY OF THE DECISION

1. On 24 February 2021, Tanah Merah Country Club (the **"Organisation"**) notified the Personal Data Protection Commission (the **"Commission"**) that an employee's (the **"Employee"**) email account had been compromised and 600 phishing emails had been sent to various individuals on 22 February 2021 (the **"Incident"**).

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited breach decision procedure. This meant that the Organisation voluntarily and unequivocally admitted to the facts set out within this decision. It also admitted that it was in breach of section 24 of the Personal Data Protection Act (the "PDPA").

3. The Organisation's investigations revealed that it was likely that the Organisation's email accounts had been subjected to password spraying attacks. Password spraying is a type of password attack where a threat actor uses a few commonly used or default passwords against many different accounts. In contrast to

traditional brute-force attacks, where the targeted account may quickly get locked-out due to account-lockout policies that only allow for a limited number of failed attempts, password spraying attacks allow a threat actor to mount an attack against many accounts with a single commonly used password, while remaining undetected, before attempting the second password. At the time of the Incident, the Employee was using the password "TMCC@1234", which the Employee had not changed for a period of nearly 5 years, since 2016 to the time of the Incident on 22 February 2021.

4. After gaining access to the Employee's email account, the threat actor accessed the personal data of 467 individuals, including:
    a. The email addresses of 155 club members and 284 members of public, which the threat actor had used to send phishing emails to.
    b. The name, and/or NRIC number, and/or email addresses of a further 28 individuals contained within the emails.

5. Prior to the Incident, the Organisation had informed its employees via an email IT newsletter in August 2018 of the need to change their password once every 3 months, and to use passwords which are at least 8 characters, with a combination of uppercase letter, lowercase letter, special character, and number. In September 2019, the Organisation sent another email IT newsletter to inform its employees of the implementation of a domain password policy. This meant that the above-mentioned password requirements became system enforced.

6. Despite disseminating these email IT newsletters where it referred to its password requirements and the implementation of a system-enforced domain password policy, the Organisation failed to further develop its password requirements into a full-fledged password policy in writing and disseminate it in such a manner whereby all its employees, new and old, could easily take reference from the password policy and consult the password policy at any time. It was only on 23 February 2021, after the Incident had occurred, that the Organisation documented its password policy in writing.

7. We had previously emphasized the importance of organisations having a written personal data protection policy so as to guide its employees and staff in *Re Furnituremart.sg* [2017] SGPDPC 7. In that case, the Commission noted at [14] as follows:

> "The lack of a written policy is a big drawback to the protection of personal data. Without having a policy in writing, employees and staff would not have a reference for the organisation's policies and practices which they are to follow in order to protect personal data. Such policies and practices would be ineffective if passed on by word of mouth, and indeed, the Organisation may run the risk of the policies and practices being passed on incorrectly. Having a written policy is conducive to the conduct of internal training, which is a necessary component of an internal data protection programme".

8. A properly documented password policy is therefore crucial for the protection of personal data. In this regard, the Organisation admitted that it had breached the Protection Obligation under section 24 of the PDPA as it failed to document its password policy in writing.

9. The Commission recently issued a “Guide to Data Protection Practices for ICT Systems” on 14 September 2021. In the Guide, we noted that in order to maintain good governance over its personal data and mitigate data breach risks throughout the data lifecycle, organisations should develop and implement ICT security policies for data protection. Key ICT policies would include a password policy.

10. Prior to the issuance of this Guide, the Commission had also released a Handbook on “How to Guard Against Common Types of Data Breaches”, which is complemented by the Checklists to Guard Against Common Types of Data Breaches. In the Handbook, the Commission identified poor management of accounts and passwords as one of the five common causes and types of data breaches. We noted that the use of default value, weak or easily guessable passwords result in accounts being particularly vulnerable to brute force or dictionary attacks. We therefore recommended that organisations adopt and implement a strong password policy, with the following good practices:

    (i) Enforcing a password history policy to ensure that employees do not reuse their previous passwords;
    (ii) Encouraging users to use passphrases such as “Iwant2l@se10kg”, which may be long and complex, yet easy to remember; and
    (iii) Discouraging users from using the same passwords across different systems.

11. In this regard, we observed that the Organisation’s email IT newsletters to its employees had cited “TMCC_Password_123” as an example of what amounts to a good password. Unfortunately, we are unable to endorse the Organisation’s

choice of “TMCC_Password_123” as an example of what amounts to a good password. In *Re Chizzle Pte Ltd* [2020] SGPDPCR 1, the Commission highlighted that a password that complies with the recommended password complexity rules in form could still be a weak password easily guessable and vulnerable to password attacks if the password incorporates components such as the organisation’s name, which is not difficult to guess and crack. In this regard, we note that in the Organisation’s password policy, which it adopted on 23 February 2021, the Organisation now recommends that its employees refrain from the use of the Organisation’s name or abbreviations such as “TMCC”.

12. In addition, the Organisation also admitted that it had failed to provide structured and organised training for its staff on how to ensure compliance with the obligations under the PDPA and how personal data should be handled in the course of their work. Only ad-hoc and informal training had been provided. As a result, the Employee lacked the awareness of the need to change her password at more regular intervals and of the need to use a strong password. The Employee did not receive system prompts to change her password as the domain password policy was not pushed down to her system due to a domain controller disruption.

13. The Commission wishes to emphasize that staff training is a critical and necessary component to ensure that an organisation is well placed to protect the personal data in its possession and/or control. The Protection Obligation under section 24 of the PDPA extends to and includes the training of all employees who have to handle personal data in the course of their work so that an organisation’s employees can then successfully adopt and implement the policies and best

practices necessary to ensure the protection of personal data in an organisation's possession and/or control.

14. In light of the above, the Deputy Commissioner for Personal Data Protection finds the Organisation in breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the "PDPA").

15. Following the incident, the Organisation engaged an IT forensic vendor for investigation. We note that the Organisation has since implemented the measures recommended by the vendor to improve its cybersecurity. The Organisation has also documented its password policy, implemented regular updates, conducted user awareness training, and other trainings on personal data protection.

16. The Organisation cooperated with the Commission's investigations, admitted to its breach of the Protection Obligation, and took prompt remedial actions.

17. Having considered the circumstances set out above, the factors listed at section 48J(6) of the PDPA, and in particular, the Organisation's voluntary admission to being in breach of section 24 of the PDPA under the Expedited Breach Decision Procedure, which is a significant mitigation factor, the Deputy Commissioner for Personal Data Protection requires the Organisation to pay a financial penalty of $4,000 within 30 days from the notice accompanying date this decision, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

18. Finally, in view of the remedial actions taken by the Organisation, no other directions are necessary.

The following is the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.