PERSONAL DATA PROTECTION COMMISSION

[2026] SGPDPC 2

Case No. DP-2301-C0629

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

And

COURTS (Singapore) Pte. Ltd.

… *Organisation*

DECISION

COURTS (Singapore) Pte. Ltd.

Wong Huiwen Denise, Commissioner — Case No. DP-2301-C0629

11 August 2026

Introduction

1 On 13 January 2023, the Personal Data Protection Commission (the "**Commission**") was notified by COURTS (Singapore) Pte. Ltd. (the "**Organisation**") that the Organisation had suffered a data breach incident on or around 21 September 2022, in which a threat actor ("**TA**") had introduced malware into the Organisation's IT environment which contained personal data (the "**Incident**").

2 The Commission commenced investigations to determine whether the circumstances relating to the Incident disclosed any breaches of the Personal Data Protection Act 2012 ("**PDPA**").

3 The Organisation applied for the investigation to proceed under the Expedited Decision Procedure, which the Commission acceded to. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision, and to the Organisation's breach of section 24 of the PDPA.

The Facts

4 The Organisation is a consumer electronics and furniture retailer in Singapore. As part of its operations, it regularly collects the personal data of retail customers and employees, stored in various servers across its IT environment.

5 Prior to the Incident, the Organisation implemented the following cybersecurity measures to protect the personal data in its possession and/or under its control:

(a) Access to the Organisation's Virtual Private Network ("**VPN**") required the use of an authenticator application to authenticate users' identities and access permissions;

(b) The connections of the Organisation's VPN were limited to specified hosts only (e.g., only company-issued devices);

(c) Only designated administrators were allowed to log in to the Organisation's servers;

(d) Two tiers of firewalls monitored online traffic and alerted the Organisation of any abnormality e.g. potential unauthorised logins;

(e) Monthly checks were conducted on account creations across all critical systems and the Organisation's internal IT environment was audited annually;

(f) Network security and vulnerability management tool and antivirus and cybersecurity software were installed on all endpoints, which were manually monitored by the Organisation's staff;

(g) An external consultant was engaged to carry out enterprise risk management services, and a risk exposure register was maintained; and

(h) Usage of an endpoint management tool to provide patch management services.

6 To ensure business operations continuity in the event of a catastrophic failure (for example, a ransomware attack), the Organisation also established a cluster of disaster recovery servers ("**DR Servers**") located in an external data centre.

7 Two features of the DR Servers are germane to the Incident:

(a) Two of the DR Servers were exposed to the internet (the "**Internet-facing Servers**"); and

(b) The DR Servers had several open ports[1] which functioned as gateways for data to flow between the DR Servers and other computers in the Organisation's IT environment.

[1] Ports are the virtual points where network connections start and end. An open port is able to receive traffic.

8 Investigations revealed that, at the time of the Incident, the two Internet-facing Servers had not been updated with the latest software security patch since 6 July 2022. More broadly, multiple other servers across the Organisation's IT environment were running end-of-life operating systems such as Windows Server 2008, which has not been supported by Microsoft since 14 January 2020.

The Incident

9 On or around 26 September 2022, the Organisation was notified by its IT threat response and remediation tool of the presence of malware in its IT environment. The Organisation initiated investigations and subsequently confirmed that a threat actor had likely gained entry and introduced the malware into the Organisation's IT environment.

10 The Organisation's investigations further revealed that the TA most likely gained access to the DR Servers on or around 21 September 2022 by subjecting the Internet-facing Servers to brute force attacks and port scanning, through the use of amongst other things, remote desktop tools. The TA then, through unknown means, compromised the user credentials of a domain administrator. As the DR Servers were connected to the rest of the Organisation's IT environment through open ports, the TA was able to move laterally across the Organisation's IT environment.

11 The TA proceeded to install ransomware in 26 servers comprising several of the DR Servers, as well as other servers within the Organisation's IT environment (collectively, the **"Affected Servers"**). Of the 26 Affected Servers,

the ransomware was able to fully or partially encrypt the data contained in 20 servers.

12 On 1 October 2022, an employee in the Organisation's customer service team received an email with a ransom note purporting to be from the TA claiming responsibility for the Incident. The TA demanded an unspecified payment in exchange for a decryption password to recover the encrypted files. The Organisation did not respond to the email, and there has been no further contact from the TA to date.

13 In total, the personal data of around 1,404,523 personal datasets stored in the Affected Servers was affected in the Incident ("**Affected Data**"), comprising the following datasets:

(a) For each of the Organisation's 1,399,064 personal datasets relating to its customers ("**the Affected Customers**")[2]:

(i) Name;

(ii) Identification number;

(iii) Address;

(iv) Phone number;

[2] While the Organisation admits that there were 1,399,064 unique datasets affected, the Organisation claimed that some datasets may have been duplicates involving the same person, such that the number of affected customers may have been lower. However, the Organisation was unable to establish to the Commission's satisfaction the extent of any such duplication.

(v) For some customers, partial credit card numbers (last 4 digits).

(b) For 5,459 prospective, past and present employees of the Organisation ("**the Affected Employees**"):

(i) Name;

(ii) Address / email address;

(iii) Government-issued ID number / passport number;

(iv) Creditworthiness of the individual;

(v) Employment details; and

(vi) Bank account information.

Remedial Actions

14 To contain the Incident, the Organisation engaged various IT vendors that:

(a) isolated and decommissioned the impacted servers from the Organisation's network;

(b) implemented a default deny rule on all traffic across the corporate firewall and added whitelist rules as needed;

(c) conducted a full scan of all endpoints;

(d) blocked all outgoing internet traffic and whitelist specific sites defined by the Organisation;

(e) performed Windows updates on all server machines;

(f) scheduled daily scans of all machines;

(g) disabled and decommissioned shared admin accounts; and

(h) fully restored the affected systems using the Organisation's clean backups.

15 To prevent a recurrence of the Incident, the Organisation also took measures including:

(a) resetting service credentials on the networking equipment;

(b) implementing password manager to secure user credentials;

(c) closing vulnerable ports across the environment including the DR Servers;

(d) updating the domain controller operating system and servers to the latest security patch level;

(e) implementing multi-factor authentication for VPN and other services;

(f) restricting user credential sharing and separated individual admin accounts from their daily user accounts;

(g) removing unused accounts and devices;

(h) configuring daily and weekly report generation for its network security solutions; and

(i) implementing an identity services engine for all laptop devices.

16 The Organisation assessed that the Affected Employees had suffered or were likely to suffer significant harm arising from the Incident due to their creditworthiness and bank account information being accessed by the TA without authorisation. Accordingly, the Organisation notified the Affected Employees of the occurrence of the Incident.

17 The Organisation did not notify the Affected Customers of the Incident as it assessed that that they were unlikely to suffer significant harm due to the nature of the personal data that was affected, being limited to basic identification and contact details.

18 Separately, the Organisation also engaged a threat intelligence firm to monitor the dark web and internet for a period of 12 months for signs of public disclosure of the Affected Data. There were no signs of public disclosure reported. There is also no other evidence of exfiltration of the Affected Data.

Findings and Basis for Determination

19 Based on the circumstances of the Incident as set out above, the Commission's investigation centered on whether the Organisation had breached its obligations under Section 24(a) of the PDPA to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

Whether the Organisation had contravened the Protection Obligation

20 In determining what constitutes reasonable security steps or arrangements, an organisation should have regard to the nature of the personal data in its possession and control, as well as the impact that the disclosure of the data might have on the affected persons. As stated in the Commission's Advisory Guidelines on Key Concepts in the PDPA (as revised 16 May 2022) at [17.2]:

> "There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration **the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.** For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals

as compared to more general information about the projects an employee has worked on."

(emphasis added)

21 In this regard, the volume and sensitivity (e.g. creditworthiness and bank account information of the Affected Employees) of personal data in the Organisation's possession called for a higher standard of security arrangements to be implemented in respect of such personal data.

22 The Organisation admitted to breaching the Protection Obligation by failing to (a) conduct regular and comprehensive vulnerability scanning for the DR Servers; and (b) implement sufficiently robust security patch management processes to ensure updates to the latest security patches.

Failure to conduct comprehensive vulnerability scanning

23 The Commission's Guide to Data Protection Practices for ICT Systems (rev. 14 Dec 2024) ("**ICT Guide**") emphasises the need for organisations to periodically conduct security reviews or "*vulnerability scanning and assessments*" as a basic practice to ensure compliance with the Protection Obligation[3]. The importance of periodic vulnerability scanning has also been emphasised in the Commission's past decisions[4].

[3] See page 22 of the ICT Guide

[4] Kingsforce Management Services Pte Ltd [2023] SGPDPCS 1 at paragraph [7] citing Re WTS Automotive Services Pte Ltd [2019] SGPDPC 26; Re Bud Cosmetics Pte Ltd [2019] SGPDPC 1; and Re: Watami Food Service Singapore Pte Ltd [2019] SGPDPC 12.

24 Had the DR Servers been subjected to regular and comprehensive vulnerability scanning, the Organisation would have uncovered the risks engendered by their exposure to the internet (which created an entry point to the Organisation's network), and their open ports (which granted lateral access to the rest of the Organisation's network). This, in turn, would have enabled the Organisation to take appropriate remedial steps, such as closing or securing the ports.

25 While the Organisation conducted regular vulnerability scanning for its other servers, it did not include the DR Servers as part of such exercises as it did not consider them critical, as they were not routinely used for business operations. This was not a defensible decision as the criticality of the DR Servers to the Organisation's *business* functions had no bearing on the degree of personal data-related risks posed by the vulnerabilities in the DR Servers.

26 The open ports of the DR Servers could and did enable access to a network of other servers in the Organisation's IT environment containing large volumes of personal data. Had the Organisation applied its mind to the real and foreseeable data protection risks arising from the deployment of the DR Servers, it would have included them in the scope of their regular vulnerability scanning.

27 Instead, the Organisation's failure to do so meant that the vulnerabilities exploited by the TA during the Incident went undetected and unaddressed.

Failure in patch management to ensure patch updates

28 The Commission has consistently stated that if software patches are not updated as recommended by the third-party software provider, then they may not contain the latest cybersecurity updates and therefore may compromise the organisation's defence against cyber-attacks.[5] Similarly, in *Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12, the Commission held that "patching is one of the common tasks that all system owners have to perform in order to keep its security measures current against external threats" (at [38]).

29 Investigations revealed that multiple servers in the Organisation's IT environment were running end-of-life (i.e. outdated) operating systems such as Windows Server 2008 for more than two years to the date of the breach. This is a clear security vulnerability as Microsoft no longer provided security updates for Windows 2008 since 14 January 2020. In particular, the Organisation admitted that it failed to ensure that the two Internet-facing DR Servers had been updated with the latest security patches. These were the same two servers that were used by the TA as the entry point into the Organisation's IT environment.

30 The Protection Obligation required the Organisation to implement a robust and regular patching policy and process across its IT environment – it is insufficient to rely on *ad hoc* updates without any regular patch management process. The Organisation failed to implement a patch management process to ensure regular and

[5] ICT Guide at pg 27.

timely updates to the latest security patches. In particular, the DR Servers did not receive any regular patching, updates, and/or upgrades of important software and firmware. Consequently, they were highly susceptible to unauthorised access by way of malicious activities such as brute force attacks and port scanning (to identify open or vulnerable ports).

31 In view of the above circumstances, the Commission finds that the Organisation negligently contravened the Protection Obligation by failing to conduct robust periodic security reviews and vulnerability assessments on its DR Servers and failing to implement a robust software patching process across its IT environment to ensure regular and timely patch updates.

The Commissioner's Preliminary Decision

32 In determining whether any directions should be imposed on the Organisation under section 48I of the PDPA, and/or whether the Organisation should be required to pay a financial penalty under section 48J of the PDPA, the Commission considered all the factors at section 48J(6) of the PDPA and all relevant circumstances surrounding the Organisation's non-compliance with the PDPA. As a preliminary point, the Commission notes that the Organisation's contravention of the Protection Obligation occurred prior to the date that the amendments to the PDPA effected through the Personal Data Protection (Amendment) Act 2020 came into effect *i.e.* 1 October 2022 (the **"2022 Amendments"**). The statutory maximum financial penalty that may be imposed is thus $1 million. Hence, in calculating the amount of the financial penalty to be

imposed, the Commission did not apply the financial penalty framework recently described in the Commission's decision in *Marina Bay Sands Pte. Ltd.* [2025] SGPDPC 6 ("***MBS***"), that would otherwise have considered the size of the Organisation's annual turnover in Singapore in determining the maximum financial penalty that may be imposed.

33 Looking at the nature, gravity and duration of the non-compliance, the Commission took into account that the Organisation's non-compliance of the Protection Obligation resulted in an extensive degree of unauthorised access to, and modification of the folders containing personal data by the TA, with 20 out of 26 Affected Servers fully or partially encrypted by the TA, and malware was introduced into the Organisation's IT environment. In total, the impact of the Incident was extensive as personal data relating to 1,404,523 personal datasets was affected, and a portion of the Affected Data included the bank account information and creditworthiness status of Affected Employees. The Commission has recognised that bank account information[6] and creditworthiness, or indebtedness[7], are personal data of a more sensitive nature, which are also prescribed categories of personal data deemed likely to result in significant harm to individuals if affected by a data breach[8]. The exposure of such financial personal data can expose certain individuals to risks of identity theft or actual financial losses: *Keppel Telecommunications & Transportation Ltd*. [2024] SGPDPC 3 ("***KTT***") at [38].

[6] *AIA Singapore Private Limited* [2016] SGPDPC 10 at [5] and [19].
[7] *Credit Counselling Singapore* [2017] SGPDPC 18 at [19] and [23].
[8] The Schedule to the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

34 The Organisation's negligence in failing to implement reasonable security arrangements exposed the personal data in its possession to similar risks of unauthorised access and modification. The Organisation's negligence was also systemic and protracted, including its use of end-of-life operating systems that were not patched or updated for more than two years - which is a significant duration of non-compliance, as the Commission had observed in *KTT* at [36]. Given the volume and sensitivity of the personal data in the Organisation's possession, the security arrangements it put in place were manifestly inadequate to protect the personal data from risks. A financial penalty is warranted to deter such negligence of this nature and gravity.

35 Additionally, the Organisation had been found to have contravened the Protection Obligation in two previous instances[9] which demonstrates a persistent disregard for their obligations under the PDPA. This is the Organisation's third breach of the same. Concerningly, each breach has resulted in an escalating number of affected individuals, majority of whom were their members / retail customers. The Commission's accounting of the first breach in *Courts (Singapore) Pte. Ltd.* [2020] SGPDPC 17 as an aggravating factor, should have been a warning to the Organisation to address the protection of personal data more seriously. However, the Organisation persisted in failing to implement adequate data protection practices. The Organisation's systemic failings to implement basic cybersecurity policies and practices such as security reviews and patch management despite the

[9] COURTS (Singapore) Pte. Ltd. [2019] SGPDPC 4 and COURTS (Singapore) Pte. Ltd. [2020] SGPDPC 17

previous financial penalties, warrant a higher financial penalty for more effective deterrence.

36 Nevertheless, the Commission also recognised that:

(a) the Organisation was cooperative with the Commission's investigations;

(b) the Organisation had put in place remedial measures to mitigate the effect of the Incident and prevent recurrences; and

(c) Investigations were handled under the Expedited Decision Procedure, under which the Organisation admitted to the facts set out in this decision and to its contravention of the Protection Obligation.

37 Having considered all the relevant factors in this case, the Commission preliminarily indicated that it would impose a financial penalty of S$280,000 on the Organisation.

38 In view of the remedial actions already been taken by the Organisation, no further directions need be issued to the Organisation.

39 This decision marks the Organisation's third recorded contravention of the PDPA, and the Organisation's recurrent disregard for its data protection responsibilities is concerning. The Commission will not hesitate to take robust enforcement action against recalcitrant organisations to deter persistent non-compliance with their data protection obligations.

Representations made by the Organisation

40 The Organisation was notified of the Commission's preliminary decision (including its intended imposition of a financial penalty) by way of the Commission's letter dated 30 January 2026 and was invited to make representations. On 6 March 2026, the Organisation made representations to the Commission to clarify certain facts stated in the preliminary decision, some of which the Commission accepts and has amended accordingly in this decision. Whilst the Organisation did not dispute the Commission's findings on its negligent non-compliance with the PDPA, it disputes the quantum of the preliminary financial penalty imposed by the Commission. The Organisation contended that:

(a) The presence of outdated operating systems in the Organisation's IT environment was not causative of, nor materially connected to, the Incident. Therefore, it should not be treated as an aggravating factor in assessing the appropriate financial penalty.

(b) The Commission should not have claimed that there were 1,399,064 Affected Customers arising from the Incident (out of 1,404,523 affected individuals) as that figure referred to the affected personal datasets with a high likelihood of duplications.

(c) There was no evidence that the personal data stored on the affected servers was encrypted, accessed and/or exfiltrated. Of the 26 Affected

Servers, only four servers contained folders holding personal data, including the subset of personal data that contained partial credit card numbers. The Organisation represented that while these servers were infected with malware, they were not encrypted. The Organisation contended that approximately 99.6% of the Affected Data did not include sensitive personal data, and comprised only names, identification numbers, and/or contact details. The Affected Customer dataset also included mobile phone numbers that were collected before the introduction of mandatory SIM registration by the Infocomm-Media Development Authority and were likely to be outdated, barred or invalid.

(d) The Commission should not be treating the Organisation's previous two breaches of the Protection Obligation as aggravating factors, as they are dissimilar to its contravention of the Protection Obligation in the Incident. The previous two incidents arose from issues relating to the management and functionality of the Organisation's website and did not involve unauthorised access by a threat actor or system intrusion.

(e) The Commission should accord additional mitigatory weight to the prompt detection and containment of the Incident. In particular, the Organisation highlighted that it invested approximately $2,500,000 in strengthening its IT security infrastructure and enhancing its data protection frameworks following the Incident.

(f) The preliminary financial penalty imposed appears disproportionate and excessive in comparison with the decisions issued by the Commission both before and after the 2022 Amendments:

Incidents that occurred before the 2022 Amendments

i. *Commeasure Pte Ltd* [2021] SGPDPC 11 – $74,000;

ii. *Quoine Pte Ltd* [2022] SGPDPC 2 – $67,000;

iii. *E-Commerce Enablers Pte. Ltd.* [2023] SGPDPC 6 – $74,400;

iv. *Fullerton Healthcare Group Pte. Limited and Anor.* [2023] SGPDPC 5 – $58,000 and $10,000;

Incidents that occurred after the 2022 Amendments

v. *Air Sino-Euro Associates Travel Pte Ltd* [2025] SGPDPC 5 – $47,000;

vi. *Goldheart Jewelry Pte Ltd* [2025] SGPDPC 4 – $58,000;

vii. *People Central Pte Ltd* [2025] SGPDPC 5 – $17,500;

viii. *Singapore Data Hub Pte Ltd* [2025] SGPDPC 2 – $17,500;

ix. *Ezynetic Pte. Ltd.* [2025] SGPDPCS 2 – $17,500;

x. *Consumers' Association of Singapore* – $20,000;

xi. *KTT* – $120,000; and

xii. *CH Offshore Ltd.* [2024] SGPDPC – $18,000.

41 The Commission shall address each of these representations in turn.

Outdated operating systems in the Organisation's IT environment

42 The representation at paragraph 40(a) is rejected and does not merit a reduction in the financial penalty quantum. The Organisation would have the Commission disregard its failure to update the operating system across its IT environment by characterising this as a "broader governance consideration" and claiming that there was no causative link with the Incident. However, the Organisation does not provide any reasons to explain why this governance failure occurred, when it was the Organisation's responsibility and within its control to ensure that its systems are updated.

43 The protection obligation requires the Organisation to take ***preventative measures*** to guard against the ***risks*** of unauthorised access, disclosure and modification among other similar risks, whether or not those vulnerabilities were eventually exploited. The Commission has provided ample guidance about the perils of relying on end-of-life or outdated systems[10], and organisations are expected to take steps to keep its systems updated. By failing to do so, the Organisation exhibited disregard for its data protection obligations on a systemic level. This is a relevant consideration that goes towards the Commission's

[10] See *Air Sino-Euro Associates Travel Pte. Ltd.* [2025] SGPDPC 5 at [26]; The Commission's Guide on managing and notifying data breaches under the Personal Data Protection Act (revised on 15 March 2021) at page 8 and Annex A on computer system weaknesses

assessment of the Organisation's culpability as reflected in the nature and gravity of its non-compliance with the Protection Obligation[11], and justifies a higher financial penalty quantum to deter such irresponsibility. The Commission is also empowered to look at the Organisation's overall compliance posture, and consider whether the Organisation had, despite its non-compliance, implemented adequate and appropriate measures (or in this case, inadequate measures) for compliance with the requirements under the PDPA[12].

44 In any event and contrary to the Organisation's representations, there is a causative link between its out-of-date operating systems and the Incident. The DR Servers from which the TA gained initial entry in the Organisation's IT environment, were also running on outdated software which heightened the risk of unauthorised access (see paragraph 8). This cannot be divorced from the Organisation's broader failure to update its operation systems in its entire IT environment.

Number of affected individuals

45 The Organisation's representation at paragraph 40(b) is accepted, as the Organisation has provided further evidence *after* the preliminary decision was issued, to de-duplicate and break down the Affected Customer dataset as follows:

Personal Data Categories	**Number of affected individuals**

[11] Section 48J(6)(a) of the PDPA
[12] Section 48J(6)(e) of the PDPA

Name	941,513
Identification number	263,835
Address	1,059,612
Phone number	1,261,599
Partial credit card numbers (last 4 digits)	13,993

46 In light of the foregoing, and for the purpose of assessing the appropriate financial penalty to be imposed on the Organisation, the Commission accepts the actual number of Affected Customers was **941,513**. This is because the other categories of the Affected Customer datasets are more likely to lead to individuals being identified if read in conjunction with their names[13].

47 Together with the 5,459 Affected Employees, the total number of affected individuals arising from the Incident is **946,972**. This does not materially detract from the Commission's assessment that a high number of individuals were affected by the Incident. While the Commission exercised its discretion in this case to accept the Organisation's submission of fresh evidence made *after* the issuance of its preliminary decision because the affected dataset was very large and the Organisation needed more time to provide the breakdown, the Commission cautions that it will not generally accept any fresh evidence after a preliminary decision is issued, in the absence of any strong reasons as to why that evidence could not be submitted earlier.

Impact of the Incident

[13] See also *KTT* at paragraph [18], and Advisory Guidelines on Key Concepts in the PDPA at paragraph [5.7].

48 The Organisation's representation at paragraph 40(c) is partially accepted, to the extent that while ransomware was activated to fully or partially encrypt the data contained in 20 out of 26 Affected Servers[14] (see paragraph 11), the remaining Affected Servers which contained the Affected Data were infected with *dormant* malware. While the introduction of dormant malware into the remaining Affected Servers still posed a high risk of unauthorised access, modification or exfiltration (or similar risks) of personal data, the harm is comparatively lower than if the dormant malware had been activated to encrypt the servers. Accordingly, the Commission is prepared to accord some reduction of the financial penalty to reflect this.

49 The Commission has however also considered that it was largely a result of happenstance that the malware introduced into the remaining Affected Servers remained dormant, and that the Organisation has <u>not</u> proved that there were pre-existing strong security arrangements to prevent the activation of the malware once it was introduced into the Organisation's IT environment. The Commission had already considered the type and nature of the personal data affected (see paragraph 33).

<u>The Organisation's previous breaches of the PDPA</u>

[14] The Organisation has represented to the Commission that servers containing personal data were among those not encrypted. However, the Organisation had previously informed the Commission that the SRNAVISION server contained personal data and was encrypted or partially encrypted. Nevertheless, the Commission has given the benefit of the doubt to the Organisation that the personal data was within the servers which were not encrypted but contained dormant malware.

50 The Organisation's representations at paragraph 40(d) are rejected, and the Commission maintains that the Organisation's two previous breaches of the Protection Obligation are relevant considerations in calculating the financial penalty quantum. As a matter of **statutory intent**, section 48J(6)(f) of the PDPA provides that the Commission must have regard to whether an organisation had previously failed to comply with the PDPA when calculating the financial penalty to be imposed on errant organisations. The plain wording of the statute does not require that the previous non-compliances must be similar or related to the present contravention. The purpose is to ensure specific deterrence (i.e. deterring the organisation's own ongoing or future non-compliance with the PDPA)[15] against errant organisations that have demonstrated a previous failure to comply with the PDPA. Dissimilar antecedents that demonstrate a proclivity towards a poor data protection compliance posture will be considered by the Commission.

51 In this case, the antecedents in question also involved contraventions of the Protection Obligation. This demonstrates its recalcitrance in failing to improve its data protection posture over the interim period. A higher financial penalty is thus warranted to deter the Organisation from further non-compliance, and to do more to protect the personal data in its possession and / or under its control.

<u>The Organisation's containment and remedial efforts</u>

[15] *MBS* at paragraph [66]; see also section 48J(6)(h) of the PDPA, which requires the Commission to consider whether the financial penalty is proportionate and effective to achieve compliance and deter non-compliance with the Act, as a whole.

52 The representations at paragraph 40(e) do not merit a further reduction in the financial penalty quantum. The Commission had already taken into account the prompt remedial measures implemented by the Organisation to mitigate the impact of the Incident and to prevent a recurrence of the same in determining the financial penalty quantum at paragraph 36(b). The fact that the Organisation expended a substantial amount of money to implement the remedial measures should not be accorded additional mitigatory weight, as this was a natural consequence of the scale of the Organisation's previous extensive failure to implement reasonable security arrangements across its entire IT environment.

Comparison to previous decisions by the Commission

53 The representations at paragraph 40(f) are rejected and do not merit a further reduction in the financial penalty quantum.

54 For the decisions concerning incidents that occurred before the 2022 Amendments, the Commission noted that they were distinguishable from the present case due to the fact that the Organisation has committed two previous contraventions of the PDPA, and also that the Organisation's non-compliance was systemic and widespread in nature (e.g. the failure to update its operating systems throughout its IT environment).

55 For the decisions concerning incidents that occurred after the 2022 Amendments, the Commission notes that these decisions were decided based on a different statutory regime. One of the distinguishing factors post-2022

Amendments, is that the Commission took into account the annual turnover of each organisation in calculating the financial penalty quantum in each case based on the financial penalty framework articulated in *MBS*. While the Organisation's annual turnover did not factor in the Commission's decision, the Commission highlights that all the organisations in this category of cases subjected to a lower financial penalty quantum had substantially lower annual turnovers than the Organisation.

56 Having considered the Organisation's representations, the Commission determines that the financial penalty imposed should be reduced to $178,000.

57 The Commission hereby requires the Organisation to pay a financial penalty of **$178,000** within 30 days from the date of the notice accompanying 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.

WONG HUIWEN DENISE
COMMISSIONER
FOR PERSONAL DATA PROTECTION