PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPC 3

Case No. DP-1912-B5484

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

And

Lovebonito Singapore Pte. Ltd.

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised disclosure of personal data – Insufficient security arrangements*

Data Protection *– Protection obligation – Access controls – Two-factor authentication*

Lovebonito Singapore Pte. Ltd.

[2022] SGPDPC 3

Lew Chuen Hong, Commissioner — Case No. DP-1912-B5484

21 February 2022

Introduction

1 On 12 December 2019, Lovebonito Singapore Pte. Ltd (the "**Organisation**") informed the Personal Data Protection Commission ("**Commission**") that one of its IT systems had been hacked, and that the personal data of 5,561 of its customers had been accessed and exfiltrated by a malicious actor (the "**Incident**"). The Commission subsequently received two separate complaints from individuals affected in the Incident.

Facts of the Case

2 The Organisation operates an e-commerce platform (the "**Website**") retailing clothing and accessories. At the material time, the Organisation employed, amongst others, two third-party solutions to manage the Website. First, the Organisation employed Magento Cloud, a cloud-based service, to host and run the Website. Magento Cloud includes the Magento Content Management System ("**Magento CMS**"), an open-source e-commerce management software, which the Organisation used to change and update the Website. Second, the Organisation used a payment platform offered by Adyen N.V. ("**Adyen**") to facilitate credit card payments on the Website. When a customer indicated that they intended to pay for their purchases via credit card, Adyen's platform would load directly from their servers as a frame within the "checkout" page of the Website (the "**Checkout Page**").

3 Customers would then input the below details into Adyen's frame, and Adyen would directly collect these details and process the credit card payment:

(a) Full credit card number;

(b) Expiry date of the credit card;

(c) The CVV number of the credit card; and

(d) Customer's billing address

(collectively, the "**Credit Card Data**")

4 Once Adyen has processed the credit card payment, it would send some (but not all) of the Credit Card Data to the Organisation, namely:

(a) The last 4 digits of the credit card number;

(b) Expiry date of the credit card;

(c) Adyen's payment reference; and

(d) Billing address.

(collectively, the "**Partial Credit Card Data**")

5 The Organisation would then store the Partial Credit Card Data together with other details collected by the Organisation for the purposes of processing the order (the "**Order Data**"). The Order Data comprised the following personal data of the Organisation's customers:

(a) First name;

(b) Last name;

(c) Shipping address;

(d) Date of birth (optional);

(e) Phone number;

(f) Email address;

(g) Order details;

(h) Payment type: Paypal, credit card (i.e., Visa, Mastercard), bank transfer; and

(i) If payment was made via:

(i) Credit Card: Partial Credit Card Data; or

(ii) Paypal: the email address associated with the Paypal account (if the customer in question completed the transaction using his/her Paypal account).

6 On or around 22 November 2019, the Organisation noted a high drop in credit card authorisations for payments via Adyen's platform and began investigating the issue with Adyen. It was discovered that the Checkout Page had been configured to load an incorrect form replacing Adyen's frame on the Checkout Page. This incorrect form had not been submitted via Magento CMS or validated by any of the Organisation's employees, and the Organisation was unable to determine the source of the form. The next day, the Organisation implemented a fix to replace the incorrect form with the correct one, in order to allow the processing of credit card payments to resume through Adyen's platform, while root cause analysis was undertaken.

7 Subsequently, on or around 9 December 2019, the same issue resurfaced. As a precaution, the Organisation turned off the credit card payment functionality on the Checkout Page, and continued investigations into the issue with Adyen, Magento, and subsequently a private forensic investigator ("**PFI**").

8 Based on these further investigations, it was concluded that:

(a) One of the Organisation's Magento CMS accounts with administrator privileges was likely to have been compromised (the **"Compromised Account**");

(b) The Compromised Account was likely used to modify the Checkout Page to load and execute an unauthorised JavaScript code each time the Checkout Page was loaded ("**the Unauthorised Code**");

(c) The Unauthorised Code caused the Credit Card Data intended to be sent to Adyen to be intercepted and exfiltrated to the malicious actor instead (explaining the drop in credit card transactions); and

(d) The Compromised Account was also used by the malicious actor to access and exfiltrate Order Data from the Website via unauthorised Application Programming Interface ("**API**") calls to Magento CMS.

9 The personal data of a total of 5,561 customers was accessed and exfiltrated in the Incident of which:

(a) 4,817 customers had only their Order Data affected;

(b) 188 customers had only their Credit Card Data affected: and

(c) 556 customers had both their Order Data and Credit Card Data affected.

Remedial actions

10 Following the Incident, the Organisation:

(a) Removed the Unauthorised Code from the Website;

(b) Notified affected customers of the Incident and offered a complimentary credit monitoring service;

(c) Reset the passwords for all Magento CMS user accounts;

(d) Implemented a new password policy and two-factor authentication for all Magento CMS user accounts;

(e) Implemented session management;

(f) Reviewed its Magento CMS access permissions, refined the scope of roles, and limited the number of users with Magento CMS accounts;

(g) Implemented a remote access virtual private network;

(h) Implemented endpoint protection;

(i) Implemented a custom script to monitor for JavaScript injections;

(j) Set up API "whitelisting" to restrict network access to only approved IP addresses;

(k) Implemented a monitoring script to trigger alerts whenever there was a request from a non-trusted domain;

(l) Conducted two external penetration tests;

(m) Upgraded its version of Magento CMS to fix a security vulnerability found in the version it was using; and

(n) Implemented CAPTCHA on its Website to deter brute-force attacks.

Findings and Basis for Determination

11 As a preliminary point, both the Order Data and the Credit Card Data constituted personal data as defined by section 2(1) of the Personal Data Protection Act 2012 ("**PDPA**")[1]. In respect of the Order Data, distinct individuals could be identified from such data. In respect of the Credit Card Data, although such data could not identify any individual on its own, it could identify individuals together with other data that the Organisation had access to (viz., the Order Data).

Whether the Organisation had contravened section 24 of the PDPA

12 Section 24 of the PDPA requires an organisation 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**"). While the Organisation did not have *possession* of the Credit Card Data (i.e. because it did not collect or store the Credit Card Data), the Protection Obligation nonetheless applied, as it had *control* over the Credit Card Data.

13 As highlighted in *Re AIG Pacific Insurance Pte. Ltd.* [2018] SGPDPC 8 at [18]:

> "*While there is no definition of "control" in the PDPA, the meaning of control in the context of data protection is generally understood to cover the ability, right or authority to determine (i) the purposes for; and/or (ii) the manner in which, personal data is processed, collected, used or disclosed.*"

14 In this case, the Organisation made the decision to deploy Adyen's HTML code within a frame on the Checkout Page, and this decision directed the manner in which the Credit Card Data was collected, processed and disclosed via the Website. Thus, even though the Credit

[1] Under section 2(1) of the PDPA, "personal data" is defined as "*data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access*".

Card Data was sent to Adyen directly without first being collected and stored by the Organisation, the Organisation had control over how the Credit Card Data was collected, and the additional processing into a format which was then transmitted to Adyen. The Organisation exercised such control by implementing (or deploying) Adyen's HTML code within a frame on its Checkout Page.

15 The application of the Protection Obligation to the Order Data is more straight forward as this dataset was collected and stored by the Organisation. As the Organisation had possession of the Order Data and control over the Credit Card Data, the Protection Obligation applied in respect of both datasets.

16 In assessing the reasonableness of the Organisation's security arrangements, the fact that the data within its control included personal data of a financial nature (i.e. the Credit Card Data) was considered highly relevant. As highlighted in the Commission's previous enforcement decisions, stronger security measures are called for when protecting sensitive personal data because of the potential harm that may befall an individual from unauthorised use of such data.[2]

17 For the reasons set out below, the Organisation failed to put in place such reasonable security arrangements to protect the Order Data and Credit Card Data.

Inadequate password policy

18 A robust password policy is a key security measure that an organisation must have in place to ensure that its IT systems are not vulnerable to common hacking attempts such as brute force attacks. As noted in *Re (1) The Cellar Door Pte Ltd*; *(2) Global Interactive Works Pte. Ltd.* [2016] SGPDPC 22 (at [30(d)]):

> "*... The need to have a strong password is fundamental to the security of the database system. Weak passwords increase the chances of an intruder cracking the password and gaining full access to the database system, and, more importantly, the personal data stored therein.*"

[2] *Credit Counselling Singapore* [2017] SGPDPC 18 at [25]; *PeopleSearch Pte. Ltd.* [2019] SGPDPC 47 at [10].

19 Magento CMS had several default security settings and the Organisation confirmed that it had adopted these default settings as its password policy for its Magento CMS accounts (the "**Magento Password Policy**"). While default settings of the Magento Password Policy on password length, and the implementation of a lockout after a number of failed login attempts were in line with good practices suggested in the Commission's *Guide to Securing Personal Data in Electronic Medium* (the "**Guide**")[3], more robust and stringent measures were required.

20 First, the Magento Password Policy did not mandate periodic changes of passwords as part of the default settings, despite the availability of this functionality in Magento CMS. As stated in paragraph (g) of Table 4 in the Guide:

> "*Users are required to change their passwords regularly.* ***The frequency should be based on the risk of damage to the individual if the data is compromised.***"
>
> [Emphasis added.]

21 Second, the default settings of the Magento Password Policy did not require the Organisation's employees to refrain from using easily-guessable passwords. As highlighted in *Re Chizzle Pte Ltd* [2020] SGPDPCR 1, a password that complies with an organisation's rules on password complexity in form, could still be regarded as a weak password if it incorporated components such as the organisation's name. In this respect, the Organisation ought to have complemented the *technical* Magento Password Policy with a *written* password policy. Both written and technical policies reinforce each other. Technical policies alone may not ensure that users refrain from incorporating easily-guessable words or phrases such as their user name, real name, birth date, or the organisation's name in the password. In this case, the password of the Compromised Account – "*ilovebonito88*" – incorporated the Organisation's name, which made it easy to guess and vulnerable to brute force attacks.

22 For these reasons, the out-of-the-box default settings of the Magento Password Policy was not sufficiently robust for the Organisation's needs and failed to meet the standard of being a reasonable security arrangement under the Protection Obligation.

---

[3] Published on 8 May 2015, and revised on 20 January 2017. The Guide has recently been replaced by a new Guide to Data Protection Practices for ICT Systems. All references to the Guide in these grounds are to the 2017 edition.

Weaknesses in the Organisation's host, network, remote access, and webpage security

23 There were other significant weaknesses in the Organisation's IT systems identified by the PFI that could have also been exploited by malicious actors to gain privileged access to Magento CMS:

(a) The Organisation's system allowed insecure remote access, with no / limited system logging and no / limited system hardening;

(b) The Organisation's system was not patched / maintained;

(c) There was a lack of security monitoring for the Organisation's network;

(d) There was a lack of network ingress and egress filtering of the Organisation's network to examine network traffic;

(e) There was a lack of monitoring and logging of remote access connection attempts; and

(f) There was improper access control in respect of Magento CMS.

24 The above weaknesses indicated that the IT security measures implemented by the Organisation were inadequate in managing the risks of unauthorised access and exfiltration of the Credit Card Data and Order Data.

25 The above security measures did not meet the standard of reasonableness, and the Commissioner finds the Organisation in breach of the Protection Obligation in this regard.

The Preliminary Decision

26 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, the factors listed at section 48J(6) of the PDPA were taken into account, as well as the following mitigating factors:

Mitigating Factors

(a) The Organisation took prompt remedial actions following discovery of the Incident, including notifying affected individuals of the breach; and

(b) The Organisation was cooperative during the investigations.

27 In the preliminary decision, the Organisation's failure to implement two-factor authentication ("**2FA**") to secure privileged access to Magento CMS was also considered as an instance of breach of the Protection Obligation – this is discussed further below at [33] to [36]. Having considered all the relevant factors of this case, the preliminary financial penalty was set at $29,000.

28 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 21 June 2021 and was invited to make representations on the same.

Representations Made by the Organisation

29 On 12 July 2021, the Organisation made representations that it ought not be found in breach of section 24 of the PDPA because:

(a) The Organisation's measures to safeguard its administrative accounts were reasonable; and

(b) It could not be conclusively determined that the weaknesses in the Organisation's IT systems had directly caused the Incident.

Representations on reasonableness of security measures for Magento CMS

30 The Organisation represented that its security measures for Magento CMS were commensurate with the risks associated with a potential data breach, as:

(a) Magento CMS was only intended to collect and store the Order Data, which was less sensitive personal data; and

(b) The risk of compromise to the more sensitive Credit Card Data via Magento CMS was assessed to be relatively low, where the Credit Card Data was collected

directly by Adyen via a frame on the Website's Checkout Page loaded directly from Adyen's server, without such data being transmitted to the Organisation.

31 The Organisation's representations in this regard are not accepted. While it is accepted that the Credit Card Data was not transmitted to the Organisation and was collected directly by Adyen via the Checkout Page of the Website, access and changes to the Website were in turn managed and carried out by the Organisation via Magento CMS. There was therefore a foreseeable risk that unauthorised access to the Website using one of the Organisation's Magento CMS administrative accounts could lead to unauthorised changes to the Checkout Page, adversely affecting its intended function and performance. Such unauthorised changes could include the insertion of a malicious code to intercept and exfiltrate the Credit Card Data collected via the Checkout Page.

32 The Credit Card Data was collected via the Website, and it was for the Organisation to secure the Website against unauthorised changes in order to protect the Credit Card Data. Put differently, the Organisation's Protection Obligation extended over the Website in its entirety, including the Checkout Page. The Organisation was therefore incorrect in assessing that there was a low risk of compromise to the Credit Card Data via Magento CMS. The security measures implemented by the Organisation for Magento CMS and in its databases and systems did not constitute reasonable security measures, having regard to the risks in the context of the sensitivity and volume of the personal data in its possession and/or control.

Representations on failure to enable 2FA for administrative accounts

33 In the present case, 2FA was available as an "out-of-the-box" feature in Magento CMS. In the preliminary decision, the Organisation's failure to enable 2FA in Magento CMS was found to be another instance of its breach of the Protection Obligation.

34 The Organisation represented that 2FA was not an out-of-the-box feature in Magento CMS version 2.3.2, which the Organisation was using at the time of the Incident, and that the option to activate 2FA was only available in Magento CMS version 2.4, via a third-party vendor (GitHub) module "MSP_TwoFactorAuth". However, according to publicly available Magento version 2.3.x user guides – and contrary to the Organisation's representations – 2FA was already a feature available on Magento CMS version 2.3.2, albeit at that version, 2FA was not enabled by default.

35 The Organisation also represented that even if 2FA had been implemented, it would not have prevented the Incident as the "2FA functionality in Magento CMS version 2.4 would only have restricted unauthorised access via the graphical user interface ("**GUI**") of Magento CMS" and that "(…) 2FA would not have prevented API calls to Magento CMS, which was the actual mechanism by which the Organisation's website was modified during the Incident". In an investigation summary report prepared by Magento in respect of the Incident, Magento did not find any evidence of changes made to the Organisation's website made via the GUI, and concluded that it was "more likely" that the administrative account belonging to [redacted] was used "to make modifications and access information via API requests".

36 After careful consideration of the Organisation's representation, it is decided that the benefit of doubt ought to be given to the Organisation on the preliminary findings and its representations concerning the implementation of 2FA for two reasons. First, the external actor accessed and modified the Organisation's Website via API calls to Magento CMS (as opposed to via the GUI of Magento CMS), which made the attack a sophisticated one. Second, the Organisation's failure to consider enabling the out-of-the-box 2FA functionality within Magento CMS was but one of several instances supporting the finding of its breach of the Protection Obligation. The finding of breach is maintained on the basis of other instances of breach.

Representations on other weaknesses in IT systems

37 The Organisation's representation that it cannot be conclusively determined that the weaknesses in its IT systems had directly caused the Incident (see [29(b)] above) is rejected. The Commission's role is not limited to investigating the immediate or proximate cause of the data breach although this may have been one of the lines of inquiry. The Commission's investigations found that other weaknesses in the Organisation's IT systems posed risks to personal data in the Organisation's possession and/or control, including Order Data that it collected and processed. The Organisation ought to have implemented reasonable security measures to manage these risks. In failing to do so, the Organisation breached the Protection Obligation.

Other representations seeking reduction in financial penalty

38 The Organisation also made representations for a reduction in the financial penalty on the basis that:

(a) It was inaccurate to state the number of affected individuals as 5,561, as only 4,474 individuals in Singapore were affected;

(b) The Organisation had admitted to the Incident at first instance;

(c) The Organisation had promptly alerted customers of the Incident and offered a complimentary credit monitoring service;

(d) There were no other data breach incidents reported apart from the Incident; and

(e) The Organisation had in place existing security measures to guard against unauthorised access to databases and systems.

39 The Organisation's attempt to confine the number of affected individuals in the Incident to those in Singapore is misconceived and is rejected. The PDPA requires organisations to protect all personal data in their possession or control, and does not draw distinctions between the personal data of individuals in Singapore and outside of Singapore.

40 As to the factors raised by the Organisation at [38(b)] to [38(e)] above, these had already been taken into account in the assessment of the appropriate financial penalty to be imposed.

41 In the preliminary decision, the preliminary financial penalty was derived considering, *inter alia*, the gravity of the Organisation's breach of the Protection Obligation in failing to consider implementing 2FA, which was available out-of-the-box. As the Organisation's representations that 2FA may not have prevented the Incident are accepted, the gravity of the Organisation's breach is lessened, and it follows that the quantum of the financial penalty should also be moderated.

42 Having said that, the Organisation's breach included more *fundamental* failures, such as failing to implement a robust password policy and to refrain the Organisation's employees from using easily-guessable passwords. Regardless of whether 2FA would have prevented the

specific vector of attack adopted by the threat actor, the harm caused to data subjects in the Incident remains the same.

43 For the above reasons, the Commissioner is of the view that based on the representations made by the Organisation, the preliminary financial penalty of $29,000 should be reduced to $24,000. The Commissioner hereby requires the Organisation to pay a financial penalty of $24,000 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 would accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

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

Two- or multi-factor authentication as mandatory baseline standard for administrative accounts with privileged access to systems that host or process sensitive personal data

45 As 2FA and multi-factor authentication ("**MFA**") become more broadly available, the adoption of these tools should become the norm, at least for accounts with administrative privileges.

46 Recently, the Commission released a handbook on common causes of data breaches (*How to Guard Against Common Types of Data Breaches*[4], at page 13) that recommends 2FA / MFA for *all* administrator access to systems holding large volumes / sensitive personal data:

> "***Have stronger requirements for some administrative accounts*** *(e.g. a complex password or 2-Factor Authentication (2FA) / Multi-Factor Authentication (MFA)). With 2FA/MFA in place, access to administrative accounts would involve additional round (s) of authentication, such as a temporary code sent securely to the administrator's mobile phone. Hence, the use of a stolen password alone will not be enough to breach an account.* ***This is important for administrative accounts to systems that hold large volumes of personal data, or personal data***

[4] https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/how-to-guard-against-common-types-of-data-breaches-handbook.pdf

of a confidential or sensitive nature *(e.g. financial or health records), where a breach of such data* ***could result in adverse impact to the affected individuals***."

[Emphasis added]

47 The Commission's recent *Guide to Data Protection Practices for ICT Systems*[5] at page 16 similarly recommends using "a one-time password ("OTP") or 2FA/MFA for admin access to sensitive personal data records or large volumes of personal data", as part of the authentication and authorisation processes in ICT systems.

48 This is the baseline standard that the Commission will apply in future cases. This is not a standard that was adopted lightly, but after industry consultation and considering developments domestically and internationally.

49 In recent domestic cases, the Commission has observed that 2FA was implemented by the Organisations involved as part of **voluntary** remedial measures:

(a) In *MSIG Insurance (Singapore) Pte Ltd and Globalsign.in Pte Ltd* [2019] SGPDPC 43, an administrative account for the organisation's email marketing system was hacked, resulting in spam emails being sent to over 350,000 individuals. The organisation was found in breach of the Protection Obligation for not implementing a proper password policy or carrying out periodic security scanning. As part of voluntary remedial measures, the organisation implemented 2FA for its administrative accounts.

(b) In *Ncode Consultant Pte Ltd* [2019] SGPDPC 11, students exploited vulnerabilities in a school's administration system (which had been developed by the investigated organisation), obtained a teacher's login credentials, and modified examination results. The organisation was found in breach of the Protection Obligation for insecure coding which resulted in the exploited vulnerabilities. As part of voluntary remedial measures, the organisation implemented 2FA for the teachers' accounts.

(c) In *Learnaholic Pte Ltd* [2019] SGPDPC 31, an employee of the investigated organisation (a school IT vendor) had his email account hacked, resulting in

[5] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Tech-Omnibus/How-to-Guard-Against-Common-Types-of-Data-Breaches-Handbook.pdf

unauthorised access to a large number of students' personal data including medical information. The organisation was found in breach of the Protection Obligation for negligently leaving one of the school's servers exposed to the Internet, leaving credentials to the employee's email account in the exposed server, and storing students' personal data in the employee's email account in an unencrypted form. The organisation implemented 2FA for its employees' email accounts as part of voluntary remedial measures.

50 A review of guidance and cases from foreign jurisdictions shows that implementing 2FA (or similar arrangements) to secure privileged access to sensitive data is by now a reasonable and industry-standard practice:

(a) **United Kingdom.** In two separate guidance notes, i.e. "Multi-factor authentication for online services"[6] and "10 Steps to Cyber Security – Identity and access management"[7], UK's National Cyber Security Centre advises that MFA be enabled for all accounts with administrative privileges.

(b) **Canada.** The Privacy Commissioner of Canada ("**PCC**") has cited the failure to implement MFA to secure all remote administrative access as a significant data protection failing in the *Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner*[8], where the personal data of 36 million customers of the investigated organisation (including sensitive personal and financial data) was published online. In a subsequent note on takeaways from the investigation[9], the PCC described MFA as a commonly recommended industry practice for controlling remote administrative access, and recommended that MFA be so implemented in all such cases.

(c) **Australia.** The "Australian Government Information Security Manual", a cybersecurity framework for organisations published by the Australian Cyber Security

---

[6] https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services
[7] https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management
[8] Joint Investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner (PIPEDA Report of Findings #2016-005, 22 August 2016)<https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005>
[9] https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/safeguarding-personal-information/2016_005_ta/

Centre[10], recommends that MFA be used to authenticate all (i) privileged users, (ii) positions of trust, (iii) users of remote access solutions, and (iv) users with access to important data repositories. The Office of the Australian Information Commissioner, in its "Guide to securing personal information"[11] recommends that MFA be employed in circumstances that may pose a higher security risk, such as remote access to a system or access to sensitive or restricted personal information.

51 Henceforth, the Commission adopts the following tiered approach:

(a) First, 2FA / MFA should be implemented as a baseline requirement for administrative accounts to systems that hold personal data of a confidential or sensitive nature, or large volumes of personal data: see [46]-[47] above. Failure to do so can *ipso facto* amount to a breach, unless the organisation can show that its omission is reasonable or implementation of 2FA is disproportionate.

(b) Second, *remote access by privileged accounts* to information systems that host confidential or sensitive personal data, or large volumes of personal data, should *a fortiori* be secured by 2FA / MFA. The risks concerning remote access are higher, thus the expectation to implement 2FA / MFA will correspondingly increase.

(c) Third, organisations using IT systems to host confidential or sensitive personal data, or large volumes of personal data, are expected to enable and configure 2FA / MFA, if this is a feature that is available out-of-the-box. Omission to do so may be considered an aggravating factor.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION

[10] https://www.cyber.gov.au/acsc/view-all-content/guidance/authentication-hardening
[11] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/