The Central Depository (Pte) Limited

[2020] SGPDPC 12

Tan Kiat How, Commissioner — Case No DP-1905-B3847

Data Protection – Protection obligation – Unauthorised access to and disclosure of personal data – Insufficient security arrangements

30 March 2020

Introduction

1 The Central Depository (Pte) Limited (the "**Organisation**") provides integrated clearing, settlement and depository facilities for its account holders ("**CDP Account Holders**") in the Singapore securities market. On 3 May 2019, the Organisation notified the Personal Data Protection Commission (the "**Commission**") that dividend cheques of some CDP Account Holders had been mailed to outdated addresses, resulting in the disclosure of their personal data to other individuals.

Facts of the Case

2 Prior to 10 December 2018, the Organisation used a software known as the Post Trade System ("**PTS**") for the purposes of post trade processing. The Organisation developed and customised additional modules that interfaced with PTS, including a module for the printing of dividend cheques ("**Dividend Cheque Module**"). The Dividend Cheque Module was used to automate the generation of dividend cheque mailers (i.e. mailers enclosing dividend cheques to be posted to CDP Account Holders).

3 Subsequently, the Organisation purchased another software, the New Post Trade System ("**NPTS**") to replace the PTS. In comparison to the PTS, the NPTS facilitated record keeping that was more comprehensive. The PTS only recorded a CDP Account Holder's latest address, while the NPTS kept records of the CDP Account Holder's updated address as well as historical addresses.[1] Arising from the new feature of the NPTS that kept records of CDP Account Holders' updated addresses and historical addresses, the Organisation updated the programming logic of the Dividend Cheque Module (and all other modules that required retrieving of addresses) to extract the CDP Account Holders' updated addresses.

4 Prior to migration from PTS to NPTS, the Organisation conducted several tests, which included the following:

(a) A test for the change of address for the module that generated notification letters acknowledging a change of address. This included checking that the notification letters extracted the updated address (the "**Notification Letters Test**");

(b) A test for the extraction of CDP Account Holders' personal data for the Dividend Cheque Module. The scope of this test **did not** include the scenario of change of address (i.e. whether the Dividend Cheque Module would extract the updated address in the event a CDP Account Holder changed its address) (the "**Dividend Cheque Module Test**"); and

(c) Manual code review of the additional modules (including the Dividend Cheque Module).

[1] As there was only one address for each CDP Account Holder stored in the PTS, a query for the address would always extract that address of the CDP Account Holder.

5 On 10 December 2018, the Organisation migrated from PTS to NPTS. As the tests mentioned at [4] did not detect any errors, the Organisation was unaware that the Dividend Cheque Module may not consistently extract a CDP Account Holder's updated address.

6 On 20 March 2019, a CDP Account Holder complained that the Organisation had mailed a cheque for dividends to an outdated address ("**First Incident**"). The Organisation commenced investigations immediately. However, the Organisation's technical team was unable to replicate the error and identify the issue that caused the First Incident. The results for the Dividend Cheque Module Test returned the correct addresses, including the complainant's correct address.

7 Subsequently, on 12 April 2019, the Organisation's customer service team received an email from the Monetary Authority of Singapore ("**MAS**") in relation to a complaint ("**Second Incident**"). Meanwhile, notwithstanding that the Organisation's technical team was unable to identify the issue that caused the First Incident, to further reinforce the programming logic, they introduced a defensive measure with a clause to consistently extract the updated addresses (the "**Fix**"). On 20 April 2019, the Organisation deployed the Fix into the production environment.

8 After several rounds of correspondence and additional information provided by MAS on 30 April 2019 in relation to the Second Incident, the Organisation realised that the issue pertaining to the First Incident and Second Incident may have a wider impact than originally anticipated. The Organisation conducted further investigations which revealed that all of the modules involving the retrieval of addresses were correctly coded except the Dividend Cheque Module. The error in the code in the Dividend Cheque Module (which resulted in the programme logic not consistently extracting a CDP Account Holder's updated address) had

caused the First Incident and Second Incident. Due to the implementation of the Fix as mentioned at [7], the error had been permanently resolved by this time.

9 According to the Organisation, 542 CDP Account Holders were due to receive dividend cheque mailers, and had previously updated their addresses. Out of the 542 CDP Account Holders whose personal data was at risk of unauthorised disclosure, the Organisation confirmed that 331 CDP Account Holders had presented their dividend cheques, indicating that their dividend cheque mailers had been sent to the correct addresses. By deduction, there were accordingly 211 CDP Account Holders ("**Affected Individuals**") whose dividend cheque mailers were sent to outdated addresses.

10 The information disclosed in the dividend cheque mailers (collectively, "**Disclosed Data**") were:

(a) Name of client;

(b) NRIC number;

(c) Central Depository (Pte) Limited ("**CDP**") account number;

(d) Name of security;

(e) Quantity of security held; and

(f) Dividend amount.

11 During the course of its investigations into the First Incident and Second Incident, the Organisation took the following remedial actions:

(a) On 20 April 2019, introduced an additional measure to ensure that the updated address of CDP Account Holders would be extracted in the Dividend Cheque Printing Module;

(b) Reviewed all modules which interfaced with NPTS and which involved the extraction of addresses to confirm that the error was specific only to the Dividend Cheque Module; and

(c) Re-issued replacement cheques and explanation letters to the Affected Individuals.

12 In addition, the Organisation will also be conducting refresher training to ensure that its teams report issues under their respective purview as soon as practicable (even when similar type of issues had previously been raised), so that necessary follow up action may be taken.

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

13 It is undisputed that the Disclosed Data constitutes "personal data" as defined in section 2(1) of the Personal Data Protection Act 2012 ("**PDPA**"), and the Organisation had possession and/or control over the Disclosed Data at all material times.

14 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. The fact that the Disclosed Data included NRIC numbers and personal data of a financial nature (i.e. CDP account number, name and quantity of security held, and dividend amount) is relevant in assessing the standard of reasonable security arrangements required. As emphasized

in previous decisions, when it comes to the protection of personal data of a sensitive nature, stronger security measures must be put in place due to the actual or potential harm, and the severity of such harm, that may befall an individual from an unauthorised use of such data.[2] Having in mind the sensitivity of the Disclosed Data, the Organisation failed to put in place reasonable security arrangements to protect the Disclosed Data for the reasons explained below.

15 When the Organisation migrated from PTS to NPTS, it had an obligation to conduct proper and adequate testing of the NPTS and its implementation that simulated real world usage of the system. This was critical in order to prevent errors from compromising the security of the Disclosed Data. In particular, and as mentioned at [3], the NPTS had a new feature which kept records of both the updated addresses of CDP Account Holders as well as their historical addresses, and the Organisation was relying on the NPTS and its customised additional modules to extract the correct address when generating the dividend cheque mailers.

16 The Commission's investigations revealed that the Organisation failed to conduct sufficient testing before migrating from PTS to NPTS for the following reasons:

(a) First, the scope of the testing for the Dividend Cheque Module was too narrow and did not include the scenario of change of address. This omission was unacceptable given that (i) change of address was a known scenario (which was tested in the module with respect to generation of notification letters that acknowledged change of address); and (ii) the Organisation relied on the Dividend Cheque Module to extract the updated address and automate the generation of dividend cheque mailers;

[2] See for example, *Re Credit Counselling Singapore* [2017] SGPDPC 18 at [25]; *Re Aviva Ltd* [2018] SGPDPC 4 at [17]; *DS Human Resource Pte. Ltd.* [2019] SGPDPC 16 at [9(c)]; and *AIA Singapore Private Limited* [2019] SGPDPC 20 at [12].

(b) Secondly, the Organisation should have tested the Dividend Cheque Module in an environment that simulated real world usage of the system. This required the Organisation to not only scope the tests to include the change of address scenario, but also to have a sufficient number of test cases to properly test these scenarios; and

(c) Thirdly, the Organisation had conceded that there was a "reasonable chance" that the error in the Dividend Cheque Module may have been detected if the scope of the tests had included the change of address scenario with a sufficient number of tests cases.

17 For the reasons above, the Commissioner found the Organisation in breach of section 24 of the PDPA.

Representations by the Organisation

18 In the course of settling this decision, the Organisation made representations on the amount of financial penalty that was to be imposed. The Organisation raised the following factors for consideration:

(a) The Organisation had expended its best efforts in testing:

(i) Prior to migration from PTS to NPTS, the Organisation carried out the Notification Letter Test and the Dividend Cheque Module Test. Both tests did not return any errors. In view of this, the Organisation did not contemplate further targeted testing at the material time.

(ii) Even if the Organisation had expanded the scope of the Dividend Cheque Module Test to cover the change of address scenario and increased the relevant test cases, such testing may have still failed to reveal the defect. In this

regard, after being informed of the First Incident, the Organisation was unable to replicate the error through repeated testing with real world cases.

(b) There was no risk of actual financial loss.

(i) The dividend cheques were made out to the names of the Affected Individuals and could only be encashed into accounts bearing such names.

(ii) The Disclosed Data of each Affected Individual was disclosed only to a single recipient, as opposed to the world at large. The Disclosed Data was also insufficient, in and of itself, to be used by a recipient to impersonate or execute any transaction in the name of an Affected Individual.

(iii) The Organisation used a specific envelope for the mailing of dividend cheques to minimise unauthorised access to the Disclosed Data, save in wilful circumstances. Each envelope was marked "Private & Confidential" and "To be opened by addressee only". A return address was printed on the face of the envelope, to cater for the event that the letter was not properly delivered to the addressee.

(c) Upon establishing the number of dividend cheques affected on 3 May 2019, the Organisation promptly notified the Affected Individuals and the Commission. The Organisation also took proactive and prompt remedial steps at [11].

(d) The financial penalty imposed should be consistent with the Commission's previous decisions and commensurate with the scale of the Incident. Taking into consideration the number of Affected Individuals in the present case and financial penalties imposed in the Commission's previous decisions involving similar number of

affected individuals, a warning would suffice. In the alternative, the Organisation submitted that any financial penalty imposed should not exceed $5,000.

19 Having carefully considered the representations, the Commissioner has decided to maintain the financial penalty set out at [21] for the following reasons:

(a) As explained in [15] to [16], the Organisation failed to conduct sufficient testing before migrating from PTS to NPTS. The module that generated notification letters acknowledging a change of address was coded independently from the Dividend Cheque Module. The Organisation should not have relied on test results from the Notification Letters Test as assurance that there were no errors in the Dividend Cheque Module, and it would consistently extract a CDP Account Holder's updated address.

(b) The Organisation's representations that there was no risk of financial loss cannot be accepted. Although the risk of financial loss was reduced because the dividend cheques were made out to the names of the Affected Individuals, there was still a risk of fraud i.e. the unauthorised individuals who received the dividend cheque mailers could have fraudulently altered the names on the dividend cheques and presented them for encashment. In addition, for the period between the Incident and the Organisation issuing the replacement cheques, the Affected Individuals would have been deprived of the use of funds they would have otherwise access to. As for the Organisation's representations on the specific envelopes used for the mailing of dividend cheques, the fact that the dividend cheques mailers were sent to unauthorised individuals meant that there was a risk of further unauthorised access, use and disclosure of the Disclosed Data.

(c) The Organisation's voluntary notification of the Incident to Affected Individuals and the Commission, as well as the Organisation's proactive and prompt remedial steps had already been taken into consideration in determining the financial penalty at [21].

(d) With respect to the Organisation's representations comparing the present case to earlier decisions, it needs only to be said that each decision is based on the unique facts of each case. The decision in each case takes into consideration the specific facts of the case so as to ensure that the decision and direction(s) are fair and appropriate for that particular organisation.

The Commissioner's Directions

20 In the assessment of the breach and determination of the directions, if any, to be imposed on the Organisation under section 29 of the PDPA, the fact that the Affected Individuals were put at risk of actual financial loss was an aggravating factor. The dividend cheques mailers were sent to outdated addresses and there was a risk that they may have been banked in by unauthorised persons. The Affected Individuals would also have been deprived of the use of the funds they would have otherwise access to, had they received and banked in the dividend cheques. On the other hand, the following mitigating factors were also considered:

(a) the Organisation took prompt remedial actions to rectify the error and mitigate the effects of the breach; and

(b) the Organisation was cooperative with the Commission's investigations.

21 In consideration of the relevant facts and circumstances, the Commissioner hereby directs the Organisation to pay a financial penalty of $32,000 within 30 days from the date of

the directions, 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. The Commissioner has not set out any further directions given the remediation measures already put in place.
