PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC 24

Case No DP-1706-B0895 and DP-1707-B0908

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

And

1. The Central Depository (Pte) Limited

2. Toppan Security Printing Pte Ltd

…Organisation(s)

DECISION

Re The Central Depository (Pte) Limited & Anor.

[2019] SGPDPC 24

Tan Kiat How, Commissioner – Case No DP-1706-B0895 – Case No DP-1707-B0908

22 July 2019

1. Organisations may employ vendors to carry out the printing and mailing of documents containing the personal data of their customers on their behalf. The process may involve both the organisations and vendors, which requires a concerted effort to protect personal data. This case presents the issue of division of responsibility in protecting personal data under the PDPA in such circumstances.

Background and Material Facts

2. This case concerns the unauthorised disclosure of personal data of 1,358 account holders of the Central Depository (Pte) Limited ("**CDP**") when their personal data was wrongly printed in the notification letters of other account holders and sent out. The incident occurred on or about 27 June 2017.

3. The exposed data included the name and/or CDP securities account number ("**exposed primary identifiers**") which constitute personal data of the individual. In some notification letters, additional information on the securities owned by the individual (eg name of security and total amount of dividends or distribution for the security) was also disclosed. These, when combined with the exposed primary identifiers, also constitute personal data of the individual.

Parties

4. CDP provides integrated clearing, settlement and depository facilities for customers in the Singapore securities market. Toppan Security Printing Pte Ltd ("**TSP**") was engaged by CDP to carry out secure printing and dispatch of documents, including notification letters of CDP's customers. Part of TSP's engagement with CDP included developing the necessary bespoke software to print the relevant documents.

The printing process between CDP and TSP

5. There were three categories of notification letters to be printed depending on the type of investment(s) held by the account holder – (i) Distribution Reinvestment Plan – "**DRP**" or "**D Type**", (ii) Scrip Dividend Scheme – "**SRP**" or "**S Type**", and (iii) "Others" – "**Others**" or "**O Type**". In this case, only the "DRP" or "D Type" notification letters are relevant because the data breach only affected this category of notification letters. Notification letters are sent to account holders to notify them of changes to and movements in their accounts.

6. During investigations, CDP and TSP represented to the Personal Data Protection Commission ("**PDPC**") that the notification letters were printed in the following manner:

(a) CDP sent the raw data in files over an encrypted channel to TSP. According to CDP, each file may have contained raw data for all 3 types of notification letters.

(b) TSP decrypted the files for processing. The processing included the pre-processing, layout and printing stages.

(c) The file provided by CDP contained the raw data in a plain text file. The data for a single account consisted of multiple lines. Each line

comprised a label, which identified the type of data, and the corresponding data. To illustrate, a sample of the raw data would be supplied in the following manner:

D00001ABC TRUST CO	12345678X						
D000029876-54321-12346	MR ABC	123 ST	DEF	DEF EST	65432 1	Y	SINGAPORE
D00004Taxable Income	329862520						
D00004Tax Exempt Income	194494560						
D00004Capital	077797824						
D00004Other Gains	058348368						
D00005660503272							
D000029876-12345-64321	MS JKL	321 RD	GHI		78945 6	Y	SINGAPORE
D00004Taxable Income	000001240						
D00004Tax Exempt Income	000000560						
D00004Capital	000000101						
D00004Other Gains	000000090						
D00005000001991							
D00001LMN TRUST CO	87654321X						
D000029876-00019-24689	MR QLM	98 ST	WXY		98745 6	Y	SINGAPORE
D00004Taxable Income	000012541						
D00004Tax Exempt Income	000001560						
D00004Capital	000001201						

D00004Other Gains 0000002
90
D00005000015592

The raw data above is purely for illustrative purposes and the information is fictitious. As can be seen from the above table, the labels were designated "**D00001**", "**D00002**", "**D00004**" and "**D00005**". For the lines with D00001, D00002 and D00005 labels, there was only one such line per account, while there could be more than just one line with D00004 labels for each account. The type of data that correspond to each of the labels is as follows:

Label	**Type of data**
D00001	name of the security.
D00002	account number, account holder name and mailing address
D00004	information on credits to the account for the security. The data corresponding to the D00004 label can be further categorised into Taxable Income, Tax Exempt Income, Capital and Other Gains, such that there could be up to 4 lines with the D00004 label for each account.
D00005	total value of the D00004 lines for each individual account

At the pre-processing stage, TSP's program would carry out checks on the raw data to determine the integrity of the data and format the data into a consistent structure ('formatted data'), primarily to insert D00001 lines where multiple account holders have invested in the same security.

(d) At the layout stage, a program extracts the formatted data and populates the data in each of the notification letters in the following layout:

Date Securities Account Number:

Dear Sir/Madam

ABC Trust Co
Distribution Reinvestment Plan

We are pleased to inform you that your securities account has been credited with the following unit(s) on DD MM YYYY:

	Taxable Income*	Tax-Exempt Income	Capital	Other Gains	**TOTAL**
Unit(s) Credited	A	B	C	D	**X**

Please refer to the company's announcement at www.sgx.com/company_announcements for more information.

Kindly notify us of any error within 7 days from the date of this notification.

Note
* Tax applied as per declaration form submitted by corporate account holders and is not applicable to individual holders.
(This is a computer generated advice and no signature is required.)

(e) The final stage is the printing stage where the notification letters are printed as laid out and populated in the layout stage.

7. Before the deployment of the printing process, TSP had carried out user acceptance tests ("**UAT**") on behalf of CDP, and the test results were presented to and approved by CDP.

The data breach incident

8. Prior to the data breach incident in June 2017, TSP had carried out successful print runs for S Type notification letters.

9. However, as indicated at paragraph 2 above, when the D Type notification letters were printed the first time, they were printed incorrectly. This occurred as

the raw data only contained one D00004 line for some accounts instead of the four D00004 lines of data for which the layout stage of TSP's system was programed.

10. Where only one D00004 line was present, the notification letter should have appeared in a format similar to the following sample letter

Date Securities Account Number:

Dear Sir/Madam

ABC Trust Co
Distribution Reinvestment Plan

We are pleased to inform you that your securities account has been credited with the following unit(s) on DD MM YYYY:

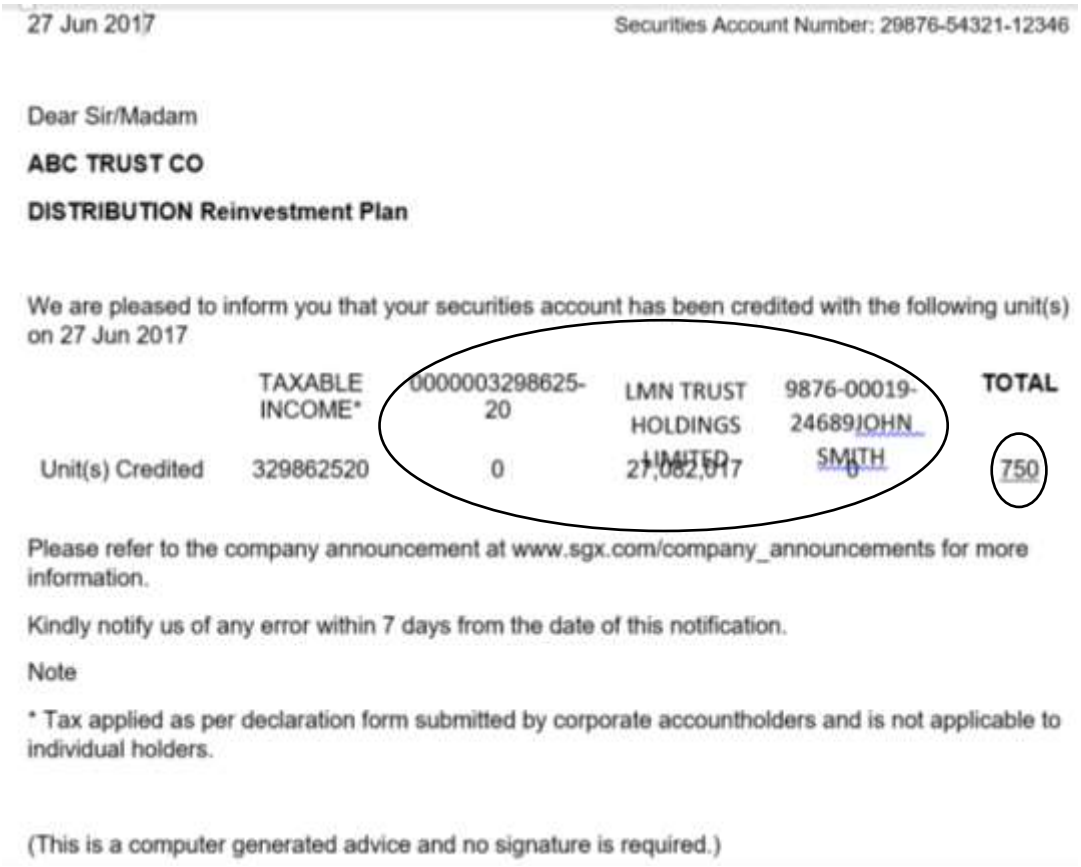
	Taxable Income*	**TOTAL**
Unit(s) Credited	A	X

Please refer to the company's announcement at www.sgx.com/company_announcements for more information.

Kindly notify us of any error within 7 days from the date of this notification.

Note
* Tax applied as per declaration form submitted by corporate account holders and is not applicable to individual holders.
(This is a computer generated advice and no signature is required.)

11. Instead each incorrectly printed notification letter included data which did not belong to that account. An example of a notification letter (using fictitious information) that was printed and sent out follows:



27 Jun 2017 Securities Account Number: 29876-54321-12346

Dear Sir/Madam

ABC TRUST CO

DISTRIBUTION Reinvestment Plan

We are pleased to inform you that your securities account has been credited with the following unit(s) on 27 Jun 2017

	TAXABLE INCOME*	0000003298625-20	LMN TRUST HOLDINGS LIMITED	9876-00019-24689/JOHN SMITH	TOTAL
Unit(s) Credited	329862520	0	27,082,017	0	750

Please refer to the company announcement at www.sgx.com/company_announcements for more information.

Kindly notify us of any error within 7 days from the date of this notification.

Note

* Tax applied as per declaration form submitted by corporate accountholders and is not applicable to individual holders.

(This is a computer generated advice and no signature is required.)

12. A comparison between the sample notification letter which was correctly printed as shown in paragraph 10 above and an example of the incorrectly printed letter shown in paragraph 11 above shows that the information marked out within the larger oval ought not to have been printed. The information in the 3rd, 4th and 5th columns, which has been marked out, shows information relating to another individual, including his name (ie John Smith), securities account number (ie 9876-00019-24689) and the security invested in (ie LMN Trust Holdings). Also the total marked out within the smaller oval is also incorrect.

13. The incorrectly printed notification letters resulted from the programming of TSP's system at the layout stage to expect exactly four lines of D00004 data for each account, instead of allowing it to accept up to a maximum of four lines of D00004 data. As will be discussed below, this was due to TSP misunderstanding each account to always consist of four D00004 lines (i.e. the categories of Taxable

Income, Tax Exempt Income, Capital and Other Gains). However, in reality each account may consist of between one to four D00004 lines. The manner in which this error resulted in the incorrectly printed notification letters is described as follows:

(a) Taking the below table of raw data as an example, at the layout stage, the program had correctly read the 1st and 2nd lines, which had the D00001 and D00002 labels respectively.

Line No.						
1	D00001ABC TRUST CO	12345678X				
2	D000029876-54321-12346	MR ABC	123 DEF ST	654321	Y	Singapore
3	D00004Taxable Income	329862520				
4	D00005329862520					
5	D00001LMN TRUST CO	87654321X				
6	D000029876-00019-24689	MR QLM	98 WXY ST	987456	Y	Singapore
7	D00004Taxable Income	000012541				
8	D00005000012541					

(b) The program did the same for the 3rd line which had a D00004 label (i.e. for the Taxable Income category).

(c) However, as the raw data did not include any D00004 lines for the "Tax Exempt Income", "Capital" and "Other Gains" categories, the layout program instead assigned lines 4 (which was the total credits to the account), 5 (the name of the security for the next account) and 6 (and the account holder name and residential address of the said next account) to these D00004 categories in respect of the first account.

(d) The program then ignored the 7th line from the D00004 label of the next account.

(e) Accordingly, when the printing was subsequently triggered, the notification letter that was printed had contained the data of the

D00001, D00002 and D00004 labels from the next account. It also skipped the printing of the notification letter for that next account, since parts of the data had been merged with the current notification letter and the trailing data field was ignored.

(f) This error was repeated for the other notification letters of the affected account holders.

14. Following the incident, CDP had issued apology letters to the affected account holders, and halted its engagement with TSP in respect of its print services.

Findings and Assessment

Issues for determination

15. The issues to be determined by the Commissioner are as follows:

(a) What obligations did CDP and TSP each owe under the Personal Data Protection Act 2012 ("**PDPA**") in respect of the personal data of the affected account holders;

(b) Whether CDP complied with its obligation under section 24 of the PDPA in respect of the data breach incident that occurred;

(c) Whether TSP complied with its obligation under section 24 of the PDPA in respect of the data breach incident that occurred.

CDP's and TSP's obligations to protect personal data under the PDPA

Relevant provisions under the PDPA

16. Section 24 of the PDPA provides that an organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or similar risks (the "**Protection Obligation**").

17. This obligation is also conferred on the data intermediary under Section 4(2) of the PDPA. Further, Section 4(3) of the PDPA provides that an organisation shall have the same obligation under the PDPA in respect of the personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

18. The duties of an organisation and data intermediary under section 24 of the PDPA has been examined in precedents, e.g. *Re Singapore Cricket Association and Another* [2018] SGPDPC 19. This case gives occasion to re-state that duty.

Relationship between CDP and TSP in complying with Section 24 of the PDPA

19. In this case, CDP is the organisation and TSP is the data intermediary in respect of the personal data of the account holders. Both CDP and TSP are obliged under the PDPA to protect the personal data of account holders pursuant to Section 24 of the PDPA stated above.

20. The overlap in obligation for organisation and data intermediary to protect personal data means, in practical terms, that organisations and their data intermediaries would necessarily have to work together in formulating the right protective measures and processes.

21. This is especially pertinent in this case because both CDP and TSP had roles in developing the system or process by which the notification letters were printed. Amongst other things, CDP was the one which determined the format of the raw data and the specifications for which TSP would build its program around to generate the notification letters which required the processing of personal data and the printing and dispatch of those notification letters.

22. Hence, both CDP and TSP had the obligation to ensure that the printing system and process they developed would sufficiently protect the personal data it was handling and processing. As part of this, there needed to be proper testing of the system and implementation of exception handling and checks to prevent errors from compromising the security of the personal data. In the Commissioner's view, this responsibility fell on both CDP and TSP.

23. One of the ways in which organisations can develop a system which protects personal data is by adopting a Data Protection by Design approach in which organisations consider the protection of personal data from the earliest possible design stage of any project and throughout the project's operational lifestyle. This may be very relevant to organisations which are looking to develop any new processes that deals with personal data (as in this case). This is a design approach that is advocated in the PDPC's Guide to Developing a Data Protection Management Programme.[1]

Whether CDP complied with its obligations under section 24 of the PDPA

24. CDP's duty under section 24 was to make reasonable arrangements to protect the personal data to be processed on its behalf. As explained at paragraphs 21 and 22 above, CDP had the responsibility in the development, testing and

[1] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-developing-a-dpmp---011117.pdf at p22

implementation of exception handling of the system to ensure that they would adequately protect personal data. In the Commissioner's view, this entails:

(a) Providing clear specifications and representative test data that covered the full range of data to be processed and the various processing scenarios. Specific to the present context, this meant making clear that there was a range in the number of D00004 lines (ie between 1 to 4 lines) per account in the data file supplied by CDP. In *Re Singapore Cricket Association and Another* [2018] SGPDPC 19, the Deputy Commissioner had found that the provision of proper and clear instructions to a developer of a website that holds personal data should form part of the protection obligations of the organisation. In failing to do so, the Singapore Cricket Association was found in breach of Section 24 of the PDPA. The same principles apply here.

(b) Advising on the scope of the UAT since the test is based on test data provided by CDP. CDP would therefore need to supply test data that covered the full range of scenarios for processing in order for there to be proper UAT testing. Again, this included supplying test data that allowed for a range of D00004 lines to be tested.

(c) Ensuring that the requirements that it provided anticipated and catered for processes that could handle exceptions and could verify that the processing was carried out correctly.

25. The Commissioner finds that CDP did not discharge its duty under section 24 of the PDPA:

(a) CDP did not provide reasonably clear specifications to TSP. CDP knew that some of its D Type letters had just 1 D00004 line instead of

4. However, the specifications that CDP provided to TSP did not make this clear:

i. There was no explicit statement by CDP making clear to TSP that the number of D00004 lines may vary.

ii. Instead, what was indicated in CDP's specification was that the D00004 lines was "repetitive". This could be understood to mean that there would be more than one D00004 line, and since CDP had only provided TSP with samples which had four D00004 lines at that stage, TSP misunderstood this to mean that they would always occur four times, ie four D00004 lines for each notification letter. Had there been more clarity from CDP on what it meant at that point, the issue may have been averted.

(b) CDP did not ensure that the UAT carried out was robust enough to test for variations in the number of D00004 lines that may be encountered in actual cases. This is because CDP had only supplied test data that had exactly four D00004 lines per account, for both initial tests as well as UAT, and, as such, did not detect any problems with variations to the number of D00004 lines of data. The test data supplied also gave the mistaken impression that there were exactly four D00004 lines of data for each notification letter. A wider range of test data would have allowed for broader scoping of the UAT, which is lacking in this case.

(c) CDP did not specify exceptional scenarios and how the printing system would handle exceptions or verify that processing was correct.

i. As the organisation with primary and supervisory responsibility to protect personal data,[2] CDP did not ensure that the printing system could detect and raise alerts when an exception or error was encountered.

ii. As will be examined below, TSP's layout program did not detect that there was only one line of D00004 data supplied in respect of some accounts, instead of the four D00004 lines it was hard coded to read, and to trigger an alert. Instead, it continued to extract or ignore the subsequent lines erroneously. TSP's layout program had therefore lacked the capability to handle exceptions or issues arising from the data supplied.

iii. Additionally, CDP also did not satisfy itself during UAT that TSP's system had the means to verify that the data was processed correctly throughout all the stages of the process.

26. Having regard to the above, the Commissioner finds CDP to be in breach of section 24 of the PDPA.

Whether TSP complied with its obligations under section 24 of the PDPA

27. The Commissioner likewise finds that TSP has did not discharge its duty under section 24 of the PDPA. First, TSP ought to have ensured that the software it used correctly processed and printed out the relevant data. Giving TSP the benefit of doubt and assuming that it had processed them correctly, TSP would have understood the requirements to mean that there were always four lines of D00004 data. TSP's layout program did not detect that in this case, there was only one line

[2] See *Re The Management Corporation Strata Title Plan No. 3696 and Another* [2017] SGPDPC 11 and *Re The Cellar Door and Another* [2016] SGPDPC 22

of D00004 data; and it went on to read the subsequent lines as though they were D00004 data. If the program was hardcoded correctly to expect 4 lines of D00004 data, it ought to have recognised that some accounts only contained one line of D00004 data and the system ought to have raised an alert in cases of deviation.

28. The program read the subsequent lines incorrectly as if they were D00004 data as the program did not check for four occurrences of D00004 labels per account but assumed that this was always the case. Thus, even based on TSP's misunderstanding that there will always be four D00004 lines per account, TSP's program was not designed to detect an exception to this (albeit mistakenly) expected feature. The incorrect processing of the data by TSP's program at the layout stage was what caused the notification letters to be printed and sent wrongly. There was a lack of exception and error handling such that it cannot be said that TSP had implemented a reasonable security arrangement that would protect personal data.

29. The incident may have been prevented if the developers of the program had co-ordinated and adopted the same interpretation of the requirements. In this regard, TSP's program incorporated 2 checksum tests at the pre-processing stage. One checksum test was a check that the value of the D00005 data for each account correctly totalled the value of the D00004 lines for each account. The second checksum test calculated the total value of the D00005 data of all the accounts sent to TSP for printing. The pre-processing stage of TSP's system would then check if the data it received is accurate by comparing the total value of the D00005 data of all accounts CDP sent to TSP with the total value stored in the very last line of the file as a separate record. However, these checksum tests at the pre-processing stage were ineffective to address the unauthorised disclosure in this matter; it was merely a check on the integrity of the file received by TSP.

30. Ultimately, TSP did not implement the proper capability to detect or handle exceptions or errors in the processing and printing of the notification letters. It is

fundamental to the protection of personal data that the system handling personal data is able to detect and carry out exception and error handling. Otherwise, this may lead to a system failure which poses risks of a data leak or data breach (as in this case).

31. It is timely for the Commissioner to refer to the PDPC's Guide to Printing Processes for Organisations[3], which states that organisations should consider the following, amongst other things, for their printing process:

> "**Appropriate juncture** for the check(s) i.e. performed at a suitable stage for corrective actions to be able to reverse and/or eliminate any potential error(s).
> **Intensity and extent** of check(s) should be proportionate to the volume and sensitivity of the personal data present in the printing process."

32. TSP did not carry out a proper test on the system. It ought to have tested for variations in the number of D00004 lines that is provided to verify whether TSP's program is able to handle those variations such as different number of lines for the D00004 labels. These variations may occur due to inadvertence or mistake, and TSP ought to test whether its program is able to handle them.

33. For the reasons above, the Commissioner finds TSP to be in breach of section 24 of the PDPA.

[3] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Printing-Processes-for-Organisations-030518.pdf

Directions

34. The Commissioner is empowered under section 29 of the PDPA to give the Organisations such directions as it deems fit to ensure the Organisations' compliance with the PDPA. This may include directing the organisations to pay a financial penalty of such amount not exceeding S$1 million as the Commissioner thinks fit.

35. Pursuant to section 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that CDP and TSP did not make reasonable security arrangements and are in breach of section 24 of the PDPA.

36. Having carefully considered all the relevant factors of this case, the Commissioner hereby directs:

(a) That CDP pays a financial penalty of S$24,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty;

(b) That TSP pays a financial penalty of S$18,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

37. In assessing the breach and determining the directions to be imposed on CDP in this case, the Commissioner took into account the following aggravating and mitigating factors:

(a) CDP is the central depository for financial market account information in Singapore. Individual account holders must be able to rely on CDP to protect their personal data.

(b) The personal data that was disclosed comprised of financial information of the individual, which is sensitive personal data.

(c) That said, CDP took steps to prevent recurrence following the data breach incident.

(d) CDP also promptly notified the affected individuals and the PDPC.

38. CDP submitted representations on the proposed decision in this case by way of a letter dated 8 April 2019. In its representations, CDP acknowledged that the specifications, test data and test scope provided to TSP could have been, and should be, improved. However, it was of the view that it had not breached section 24 of the PDPA.

39. In this regard, CDP asserts that TSP ought to have reviewed the specifications, test data and user acceptance tests ("UAT") for both the S Type and D type letters, instead of just the D Type letters, as the specifications for the print programme would have been similar. According to CDP, it had provided a S Type letter template to TSP which consisted of a maximum of two D00004 lines and provided UAT test data for S Type letters which consisted of one D00004 line. CDP asserts that "[f]rom this TSP ought to have been aware that the actual data sent by CDP for printing may vary from the templates/test data provided". Also, CDP asserts that it has specified in the specification that the number of the D00004 lines would be "repetitive", i.e. "not a fixed number of lines of crediting details but with variations within this type of crediting details". Further, CDP asserts that it had used the word "always" to indicate if a value or the number of lines is fixed or static and it did not indicate that the number of D00004 lines "always" consisted of 4 lines.

40. The Commissioner agrees that TSP is also liable for unauthorised disclosure of personal data in the wrongly printed notification letters and has already found

TSP to be in breach of section 24 of the PDPA. Nevertheless, CDP's representations do not absolve CDP of its shortcomings in respect of this incident. CDP's use of the word "repetitive" in its specifications was ambiguous when considered together with the fact that the test data provided to TSP for the D Type letters all contained four D00004 lines per account. This led TSP to assume that "repetitive" meant four D00004 lines for each account. It did not help that even though the test data provided had some records with four D00004 lines and others with fewer D00004 lines, the records with four D00004 lines were associated with D Type letters. Even though CDP intended for the dataset to be applicable for all types of letters, its omission to inform TSP led TSP to make the assumption that D Type letters always had four D00004 lines. CDP could have expressly instructed TSP that the test data provided was to be treated as applying across all the various types of letters and not merely the individual types of letters to which the test data corresponded.

41. CDP also asserted that it had requested TSP to conduct an additional visual check on the notification letters and that if TSP had done so, they would have caught the error. In relation to this, CDP referred to a Document Management Services Agreement ("DMSA") entered into between CDP and TSP to support its assertion. However, a review of the DMSA does not reveal a specific requirement to conduct a visual check of the letters that are sent out. In the circumstances, the Commissioner did not accept CDP's representations that it had instructed TSP to conduct a visual check of the notification letters.

42. Finally, CDP requested that, should the Commissioner maintain his finding that CDP was in breach of section 24 of the PDPA, the financial penalty imposed be reduced. In this regard, CDP made 2 submissions. First, CDP acknowledged that the disclosed personal data was sensitive but asserted that the potential harm to the affected individuals was relatively limited and not likely to lead to any loss or prejudice. The Commissioner agrees that there is no evidence of financial loss or damage. The absence of financial loss or damage has already been taken into consideration in determining the financial penalty imposed in this case.

43. Secondly, CDP also referred to its prompt notification of the error to affected individuals and to the PDPC, as well as to the proactive and prompt steps CDP took to remediate the matter. The Commissioner accepts these points and has included them in paragraph 37(d) above.

44. In the circumstances, the Commissioner maintains his finding that CDP was in breach of section 24 of the PDPA. However, taking into account CDP's representations, the Commissioner has decided to reduce the financial penalty from the initial quantum of $30,000 to the amount stated in paragraph 36(a) above.

45. In assessing the breach and determining the directions to be imposed on TSP in this case, the Commissioner took into account the following aggravating and mitigating factors:

(a) The personal data that was disclosed comprised of financial information of the individual, which is sensitive personal data.

(b) TSP was cooperative and willing to provide information on a timely basis to the Commission;

(c) TSP took steps to prevent recurrence following the data breach incident.

46. The Commissioner hereby directs CDP to carry out the following within 60 days:

(a) For CDP's data protection officer (appointed under section 11(3) of the PDPA) to be given authority to assess the data protection requirements in developing new printing processes that involves personal data; and

(b) For CDP to provide the full range of expected processing scenarios in the test script during development testing and UAT for all types of printing jobs (except for ad-hoc printing jobs) which are being carried out by TSP as at the date of this direction.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION