DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1409-A100

(1) K BOX ENTERTAINMENT GROUP PTE. LTD.
(2) FINANTECH HOLDINGS PTE. LTD.

…Respondents

Decision Citation: [2016] SGPDPC 1

GROUNDS OF DECISION

20 April 2016

Background

1. K Box Entertainment Group Pte. Ltd. ("**K Box**") operates a chain of karaoke outlets in Singapore. Finantech Holdings Pte. Ltd. ("**Finantech**") is a third party IT vendor, which is owned and managed by its sole director, [Redacted] (Replaced with Mr G).

2. On 16 September 2014, the website "The Real Singapore" ("**TRS**") published a post which indicated that a list containing personal data of about "317,000" K Box members (the "**List**") had been disclosed online at http://pastebin.com/bnVhn3mp ("**pastebin.com**").

3. The List contained personal data which all customers who sign up for a K Box membership, both before and after 2 July 2014, are required to provide, namely:

   (a) Name (as per NRIC);
   (b) NRIC / Passport / FIN number;
   (c) Mailing Address (Singapore only);
   (d) Contact number;
   (e) Email address;
   (f) Gender;
   (g) Nationality;
   (h) Profession; and
   (i) Date of birth.

4. After receiving complaints from members of the public regarding the data breach, the Commission commenced an investigation under section 50 of the Personal Data Protection Act 2012 ("**PDPA**") to ascertain whether

there had been a breach by K Box and/or Finantech of their respective obligations under the PDPA.

Material Facts and Documents

K Box's relationship with Finantech

5. As at 16 September 2014, K Box had engaged Finantech through the "*website revamp contract dated 2012*" and the "*webhosting and server management contract dated 2009*" to develop K Box's Content Management System ("**CMS**") system from the ground up and to revamp, manage and host its website. What the parties referred to as "contracts" were actually quotations sent by Finantech to K Box for their confirmation and acceptance. K Box's CMS stored and processed the personal data of its members. The CMS system also utilised FCKEditor – a software library component which allowed the user to input formatted text.

6. Mr G of Finantech was the only one who had direct and full access to all the K Box members' personal data as the sole administrator of K Box's CMS system. In the past, a former project manager of Finantech, [Redacted] (Replaced with Mrs G], whose role was to help Mr G in managing K Box's customer data, also had access through the administrative account in the CMS system, i.e. the 'admin' account with the password "admin".[1] Mrs G left Finantech on or around 2013. Apart from that, no one else, not even K Box's IT manager [Redacted] (Replaced with Mr C) or K Box's Chief Operation Officer, [Redacted] (Replaced with Ms N), had direct access to the database.

7. K Box employees with the title "Captain" and above[2] (of which there were about 75 people with such a title) had restricted access to a function that allowed viewing of members' personal data such as name, package, booking date and time, contact number, members' number and visit date and time to check and confirm members' booking. However, they could only view the details of each member one at a time, and not extract the entire members' list. As such, whenever K Box required members' personal data with selected criteria for marketing and promotional purposes, they would have to inform Mr G of the data required and he would perform the relevant queries on the database, export the information to an MS Excel document and email the document (unencrypted) via Gmail to K Box's IT manager, Mr C, who would in turn email the document to K Box's marketing department via Gmail. During investigations, it was discovered that Finantech had once sent K Box over 90,000 members' personal data via unencrypted email via Gmail.

By its own admission, K Box had never instructed Finantech to password-protect or encrypt emails containing a large volume of personal data prior to 16 September 2014.

K Box's Protection Measures

8. According to K Box, measures that were reasonable and appropriate taking into account "*the nature of the K Box's business (i.e. value for money, family-orientated, karaoke entertainment for everyone) and the fact that the data are non-financial in nature*" were adopted with regard to the security of its members' data.

9. K Box represented that secure server practices such as access controls and data protection policies that were established and observed in the organisation whether before 2 July 2014 or between 2 July 2014 and 16 September 2014 had been put in place since the implementation of its current website to protect individuals' personal data. In addition, K Box represented that before 16 September 2014, employees were required to set alphanumeric passwords consisting of eight alphabets/numbers, one capital and one special case in accordance with K Box's password policy. However, Mr C admitted that K Box did not "*conduct audit on whether the staff really use eight numbers/letters alphanumeric, one capital and one special case password (sic.)*" and Mr G had noted a receptionist using a one-letter password in the past. A software system "*to force employees to adopt passwords that adhered to the KBox's password policy (sic.)*" was only implemented in November 2014.

10. Although K Box had outsourced its website maintenance, which includes maintenance of its backend CMS, and web hosting of its website to Finantech ("**Services**"), K Box represented that Finantech agreed and undertook that it would keep K Box's data confidential as it was a term in their agreements.[3] K Box had also held regular meetings with Mr G/Finantech on all aspects of the Services including any IT security concerns and Finantech would not conduct any major works or modification to the Services without first consulting K Box. K Box had "*no reason to doubt*" the competence or integrity of Finantech or that Finantech would not comply with the security measures and undertaking. However, by Finantech's own admission, Finantech did not do any system monitoring in terms of IT security, security testing or regular IT security audits at the time of the breach and prior to 17 September 2014.

11. K Box had also represented that it did not have a Data Protection Officer ("**DPO**") since 2 July 2014 to 20 April 2015 and conceded that its privacy

policy prior to 16 September 2014 was not comprehensive. While each employee's employment contract contains a term to keep all information relating to the operations of K Box confidential, there was no policy and physical or online security system in place to monitor whether a staff removed personal data from its premises.

12. In this connection, the "contracts" between K Box and Finantech did not include any contractual clauses that required Finantech to comply with a standard of protection in relation to the personal data transferred to it that is at least comparable to industry standards. According to Finantech's representations, K Box had also never emphasised the need for data protection and their obligation towards K Box under the PDPA or informed Finantech of its data protection obligation after September 2014. Mr G had also represented that while he was aware of the existence of the PDPA, he was not aware of the specifics of it.

The List

13. On 16 September 2014, the same day that TRS published the post mentioned at paragraph 2 above, K Box's management realised, via the "*Social Media, employees and The Real Singapore website*", that K Box members' personal data had been uploaded on pastebin.com. Mr C had also received a call on his mobile phone from an unknown person to inform him that TRS had "*posted information of K Box members*" and to ask him to verify whether the information belonged to its members. Mr G investigated the breach by matching the disclosed personal data in the List with the information of K Box's members from its database and confirmed that the List matched the one in K Box's database. Thereafter, K Box notified its members of the data breach by way of a letter dated 16 September 2014 that was published online on the K Box homepage.

14. The next day, 17 September 2014, Mr C "*deleted all the accounts of the staff who left (sic.)*" and the unauthorised 'admin' account with the weak password "admin" was "*deactivated*", "*disabled*" and the "*password to the account was changed*". The CMS user activity log showed that Mr C had removed 36 accounts on 17 September 2014.

No Conclusive Evidence that Data Breach Occurred Before 2 July 2014

15. Although the List was uploaded on pastebin.com on 16 September 2014, the List only contained members' data up to 23 April 2014. There is no evidence available to conclusively ascertain when the List was obtained.

16. Based on Finantech's initial investigation on the day the List was published, Finantech deduced that the List containing the personal data of K Box members could have been obtained by the cyber-attacker on or around 23 April 2014 for the following reasons:

    (a) The List stopped at the member record that was created on 23 April 2014 at 5.43am;

    (b) The CMS's "user activity 2014.csv" ("**User Activity Log File**") recorded that someone had logged in using the 'admin' account on 23 April 2014 at 9.59am;

    (c) A new member record was created on 23 April 2014 at 12.17pm but this was not included in the List; and

    (d) Subsequent member records created after 23 April 2014 were also not included in the List.

17. The User Activity Log File recorded that the user of the 'admin' account had logged in on 23 April 2014. The 'admin' user account was the account used by Finantech's former employee, Mrs G. However, given that Mrs G had already left Finantech on or around 2013 and there was no evidence to suggest that she had been remotely accessing the 'admin' account, any use of this account after Mrs G had left Finantech would likely have been unauthorised and could be taken to be done by the cyber-attacker.

18. While it is possible that the data breach occurred on or around 23 April 2014, as there was evidence of unauthorised access to K Box's CMS system in April 2014 or even earlier in 2013, the Commission is of the view that further data breaches could also have occurred in the following months until the new CMS was put in place in November 2014 for the following reasons:

    (a) The message "*Remote session from client name a exceeded the maximum allowed failed logon attempts (sic.). The session was forcibly terminated*", indicating that more than 240 attempts were made *in a single day*, appeared frequently in the operating system log ("**System Log**"). The frequency of these messages may indicate unsuccessful attempts to hack into the operating system. The messages started appearing as early as October 2012 and continued until the latest parts of the log file in September 2014; and

(b) Finantech itself noted that the System Log showed that the "*[unauthorised user of the 'admin' account] was used to login a number of times after the breach. However, there was no indication that he had modified any user data*." The Commission has reviewed the System Log and the unauthorised user of the 'admin' account had performed about 83 logins in the period from 25 February 2014 to 16 September 2014, and about 15 logins in the entire calendar year 2013.

Probable Cause of Breach

19. While the List only contains members' data up to 23 April 2014, given the number of times the unauthorised user of the 'admin' account had logged in to K Box's CMS system, it is possible that the cyber-attacker had accessed K Box's CMS system after 2 July 2014 when the data protection provisions in the PDPA came into effect, but chose to publish the List reflecting the members' list as at 23 April 2014.

20. Finantech had hypothesised that someone hacked into K Box's CMS using the 'admin' user account with 'admin' password and planted a malware control and command centre to retrieve and export the members' data. K Box similarly represented that Mr G had informed Mr C that the breach occurred because "*he suspected someone used admin user account with the password also admin to login (sic.)*" and "*[Redacted] (Mr G) told me there was a Trojan in the hosting server and he suspected that was how the leak occurred (sic.)*".

21. While the System Log showed unauthorised usage of the 'admin' user account in 2014 and files detected as malware were found in the CMS folder, the Commission has not been able to conclusively verify Finantech's hypothesis even after analysing the User Activity Log File and System Log. Nonetheless, the Commission considers that the 'admin' user account, which had a weak password "admin" was one of the possible ways that the data breach could have occurred.

22. Having reviewed the relevant facts and circumstances, including the statements and representations made by K Box and Finantech, the Commission has completed its investigation into the matter, and sets out its findings and assessment herein.

THE COMMISSION'S FINDINGS AND ASSESSMENT

Issues for Determination

23. The issues to be determined in the present case are as follows:

    (A) Whether K Box had breached its obligation under section 24 of the PDPA (the "**Protection Obligation**");

    (B) Whether K Box had breached its obligation under sections 11 and 12 of the PDPA (the "**Openness Obligation**"), specifically, sections 11(3) and 12(a), for failure to appoint a DPO and put in place privacy policies and practices in contravention of those sections of the PDPA;

    (C) Whether Finantech is a data intermediary of K Box; and

    (D) Whether Finantech had breached the Protection Obligation.

Issue A: Whether K Box had breached the Protection Obligation

24. Section 24 of the PDPA states:

> "***Protection of personal data***
> *24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.*"

25. Pursuant to section 24 of the PDPA, K Box, being an organisation which had its members' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risk. The Protection Obligation applies equally to all personal data in the possession or under the control of the organisation, including personal data that the organisation may have collected before 2 July 2014, when the data protection provisions under Parts III to VI of the PDPA came into effect.

26. Following a careful assessment of the relevant facts and circumstances, the Commission is of the view that K Box had not discharged the Protection Obligation under section 24 of the PDPA. There are sufficient grounds (whether each on its own or altogether) to show that K Box failed to make reasonable security arrangements to protect the personal

data in its possession or under its control from 2 July 2014 to November 2014. In particular, the Commission has identified the following vulnerabilities in K Box's security arrangements which show how K Box failed to make reasonable security arrangements to protect the members' personal data:

(a) K Box could have, but failed to enforce its password policy, at least between 2 July 2014 and November 2014, thereby permitting the use of weak passwords:

(i) As noted at paragraph 9 above, K Box did not "*conduct audit on whether the staff really use eight numbers/letters alphanumeric, one capital and one special case password (sic.)*"; and

(ii) Even though it is a common industry practice to implement an organisation's password policy in its system, K Box had not done so earlier and the feature where the system would enforce the password policy by rejecting passwords that did not meet the password policy was only built into the CMS system in November 2014.

(b) K Box had weak control over unused accounts, specifically, unused accounts were not removed:

(i) As stated at paragraph 14 above, as many as 36 accounts were removed from the CMS system on 17 September 2014, which suggests that K Box may not have had the practice of deleting the accounts of staff that had left the company until it conducted the review on 17 September 2014. This is despite the fact that K Box was able to remove the unused accounts within a day after the List had been disclosed online which shows that K Box could have easily removed the unused CMS accounts earlier but it had failed to do so;

(ii) As a result of K Box and/or Finantech's failure to promptly remove unused accounts from the CMS system, the unused administrative CMS account with the user name 'admin' and a weak password of 'admin' remained in the CMS for about one year after Mrs G had left Finantech. This had put the personal data of K Box's members at risk because as noted at paragraph 20 above, Finantech itself had hypothesised that someone could have hacked into K

Box's CMS using this 'admin' user account and planted a malware control and command centre to retrieve and export the members' data.; and

(iii) Further, as noted at paragraph 18 above, there was evidence of multiple unauthorised accesses to the CMS system through this 'admin' user account in 2013 and between 25 February 2014 and 16 September 2014. As such, it is possible that K Box members' personal data could have been further compromised through this 'admin' user account between 2 July 2014 and 16 September 2014 as a result of the failure to remove the unused administrative account.

(c) K Box failed to utilise newer versions of the software library and/or to conduct audits of the security of its database and system:

(i) K Box's CMS system utilised an older version of the FCKEditor which according to security vulnerability website CVE, had at least 9 known vulnerabilities which would have allowed cyber-attackers to install remote shells and execute malicious codes and to execute such codes to extract the full member list from the database. Even though this vulnerability could have been prevented by utilising newer versions of the software library or by patching, Finantech, whose role was to manage the CMS system, had failed to do either; and

(ii) K Box had also failed to conduct audits to supervise the security of its database and system. As noted at paragraph 10 above, Finantech admitted that it did not carry out any system monitoring in terms of IT security, security testing or regular IT security audits at the time of the breach and prior to 17 September 2014.

27. K Box's weak enforcement of their password policy and weak control of unused accounts and passwords alone could have enabled an attacker to gain access to substantial personal data simply through the CMS system. Furthermore, K Box's use of vulnerable software could have allowed the attacker to gain access to the system beyond the CMS limitations and to perform direct access to all data from K Box's database and potentially misuse the personal data.

28. The vulnerabilities set out above demonstrate that K Box could have done more to protect the members' personal data that was in its possession or under its control. When viewed in totality, the Commission is of the view that K Box had failed to make reasonable security arrangements to protect the members' personal data because these vulnerabilities were preventable and were likely the main reasons for the data breach and subsequent disclosure of the List on 16 September 2014. In this regard, while K Box had outsourced the developing, hosting and managing of its CMS system to Finantech, it was still the data controller and was ultimately responsible for the security of the CMS system.

29. Apart from the system-related shortcomings highlighted above, investigations disclosed that there was also poor practises.

(a) Emails containing large volume of personal data were sent via Gmail without any password-protection or encryption:

(i) Even though the unauthorised access to the personal data of about "317,000" K Box members was not caused by a breach that was the result of the use of unencrypted emails, as noted at paragraph 7 above, Finantech had previously sent K Box over 90,000 members' personal data via unencrypted email via Gmail. The practice of sending large volumes of members' personal data via unencrypted email is a vulnerability and an example of how K Box had not sufficiently protected the members' personal data. The better practice would have been for Finantech to encrypt or to ensure that the MS Excel document containing the list of members' personal data was password protected before sending it to K Box.[4]

(b) K Box failed to effectively manage its vendor (Finantech) to ensure that they undertook adequate measures to protect members' personal data:

(i) For the reasons stated at paragraphs 33 and 34 below, the Commission finds that Finantech is a data intermediary of K Box and pursuant to section 4(3) of the PDPA, K Box has the same obligations in respect of the personal data processed on its behalf and for its purpose by Finantech as if the personal data were processed by K Box itself. As highlighted in the Commission's Advisory Guidelines on

Key Concepts in the PDPA issued on 23 September 2013 (at paragraph 6.21) that:

> "*… it is* ***very important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provisions in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question*** *including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation*."
>
> [Emphasis added.]; and

(ii) However, as noted at paragraph 12 above, K Box failed to ensure that its data intermediary, Finantech, complied with a standard of protection in relation to the personal data transferred to it that is at least comparable to industry standards through its agreements and in its interactions with Finantech.

30. On the facts of the case and the assessment conducted, the Commission finds that both K Box and Finantech did not put in place adequate IT security arrangements between 2 July 2014 and November 2014, prior to the implementation of the new CMS system in November 2014.

Issue B: Whether K Box had breached the Openness Obligation

31. Sections 11 and 12 of the PDPA together constitute the Openness Obligation under the PDPA, which provides that an organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. In particular, section 11(3) of the PDPA provides that an organisation shall designate one or more individuals, a DPO, to be responsible for ensuring that the organisation complies with the PDPA. In the same vein, section 12(a) of the PDPA requires organisations to develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisations under the PDPA.

32. Based on investigations and representations made by K Box, the Commission is not satisfied that K Box has complied with the Openness

Obligation under sections 11(3) and 12(a) of the PDPA. To begin with, as noted at paragraph 11 above, K Box conceded in its representations that it did not have a comprehensive privacy policy prior to 16 September 2014. By K Box's own admission, as there was no policy and physical or online security system in place to monitor whether a staff removed personal data from its premises, a K Box staff could have simply copied the member's list it received from Finantech and abused that list. In addition, K Box had also represented that it did not have a DPO. In fact, to date, it is unclear whether K Box has appointed a DPO because Mr C represented that K Box was in the midst of appointing a DPO even as late as 20 April 2015 when he gave his statement to the Commission. In light of the foregoing lapses, the Commission finds that K Box has been in breach of the Openness Obligation.

Issue C: Whether Finantech is a data intermediary of K Box

33. Under section 2(1) of the PDPA, a "*data intermediary*" is an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation. The term "*processing*" in relation to personal data means the carrying out of any operation or set of operations in relation to the personal data and includes, but is not limited to, any of the following: recording; holding; organisation, adaptation or alteration; retrieval; combination; transmission; erasure or destruction.[5] Section 4(2) of the PDPA confers on a data intermediary the obligation to protect personal data under section 24 of the PDPA and the obligation to cease to retain personal data under section 25 of the PDPA. Save for the aforementioned obligations, Parts III to VI of the PDPA do not impose any other obligations on the data intermediary.

34. Having considered the facts and the representations made by K Box and Finantech, the Commission is satisfied that Finantech is a data intermediary of K Box. The fact that (i) K Box employees, including K Box's IT manager and the Chief Operating Officer, only had restricted access to the information of members, and (ii) K Box relied on Mr G to extract and send them members' personal data with selected criteria from the database clearly shows that in practice, Finantech processed (by having access to, storing and retrieving) all personal data of K Box's customers pursuant to the arrangement between Finantech and K Box.

35. Notwithstanding that the "contracts",[6] which were in fact quotations sent by Finantech to K Box for their confirmation and acceptance, pre-date the commencement of the data protection provisions of the PDPA and do not identify Finantech as a data intermediary of K Box, in light of the

above practices which continued after the commencement of the data protection provisions, the Commission finds that Finantech is a data intermediary of K Box for the purposes of the PDPA.

Issue D: Whether Finantech had breached the Protection Obligation

36. Section 24 read with section 4(2) of the PDPA confers an obligation on the data intermediary to "*[make] reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks*". In view of the Commission's finding that Finantech is a data intermediary of K Box, Finantech is required to comply with the obligation under section 24 of the PDPA to protect the personal data that it was processing on behalf of K Box.

37. In this regard, on the facts and circumstances, the Commission is of the view that Finantech had failed to put in place the required security measures that K Box needed in order to provide adequate protection for the personal data in K Box's database and system. In particular, the Commission notes that Finantech had been involved in the setting up and day-to-day processing of K Box's personal databases from 2007. By dint of its role and function, Finantech is expected to up hold a certain basic professional standard and the vulnerabilities identified at paragraphs 26 to 29 above show that Finantech had not undertaken due diligence in executing its role. Finantech's failures had led to multiple unauthorised accesses and Finantech had put the personal data of K Box's members at risk.

38. If Finantech had advised K Box on its obligations but K Box had rejected their advice, the Commission could have taken this into account in its assessment of Finantech's culpability. However, investigations did not disclose any evidence to suggest that Finantech had actually advised K Box of the need to have in place adequate security measures to protect the personal data in K Box's database. In fact, as stated at paragraph 12 above, Mr G admitted that he was only aware of the existence of the PDPA but not the specifics.

39. In view of all the relevant facts and circumstances, the Commission is not satisfied that Finantech has complied with the Protection Obligation under section 24 of the PDPA.

THE COMMISSION'S DIRECTIONS

40. Under section 29(1) of the PDPA, the Commission may, "*if it is satisfied that an organisation is not complying with any provision in Parts III to VI*

of the Act, give the organisation such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision." Section 29(2) of the PDPA also empowers the Commission to make all or any of the following directions:

(a) To stop collecting, using or disclosing personal data in contravention of this Act;

(b) To destroy personal data collected in contravention of this Act;

(c) To comply with any direction of the Commission under section 28(2) of the Act; and

(d) To pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.

Other Factors Considered

41. In assessing the breach and the remedial directions to be imposed, the Commission took into consideration various factors relating to the case, including the mitigating and aggravating factors set out below.

K Box's Breach of the Protection Obligation and the Openness Obligation

42. In relation to K Box's breach of the Protection Obligation and the Openness Obligation, the Commission took into account the following factors:

(a) The remedial actions undertaken by K Box were fair and prompt when they discovered the data breach in September 2014;

(b) Most of the remedial actions were taken either in September or November 2014;

(c) The Commission found no evidence to suggest that the data breach was due to actions taken by K Box staff, through the CMS system;

(d) A fairly large amount of personal data (approximately "317,000" K Box members or more) had been disclosed as a result of the lack of security. The personal data comprising their full names, contact numbers, email addresses, residential addresses, contact numbers, gender, profession, date of birth, and member number were sensitive data because it could have led to identify theft;

(e) K Box (as the primary data owner) had disregarded its obligations under the PDPA. K Box had ample opportunities to put in place reasonable security measures from 2 January 2013 to 2 July 2014 but it did not do so. K Box had also failed to appoint a DPO or put in place privacy policies or practices as late as April 2015. K Box had also failed to put in place data protection terms and conditions in its contract with Finantech, and instructed it (as the main data processor of K Box members' personal data) to protect personal data; and

(f) K Box was not forthcoming in providing information during the investigation. They had only provided bare facts in their responses during the investigations, which did not facilitate the Commission's investigations.

Finantech's breach of the Protection Obligation

43. In relation to Finantech's breach of the Protection Obligation, the following factors were taken into consideration:

(a) The remedial actions undertaken by Finantech were fair and prompt when they discovered the data breach in September 2014;

(b) Most of the remedial actions were taken either in September or November 2014;

(c) A fairly large amount of personal data (approximately "317,000" K Box members or more) had been put at risk as a result of the lack of security. The personal data comprising their full names, contact numbers, email addresses, residential addresses, contact numbers, gender, profession, date of birth, and member number were sensitive data because it could have led to identify theft;

(d) Finantech as the data intermediary had disregarded its obligations under the PDPA. Finantech had ample opportunities to put in place reasonable security measures from 2 January 2013 to 2 July 2014 but it did not. There was no evidence to show that Finantech had advised K Box on the reasonable security measures that the owner of an online system ought to implement in order to protect personal data held by the system; and

(e) Finantech appeared not to be forthcoming in providing information during the investigation. Although the Notices to Require Production of Documents and Information under the Ninth

Schedule of the PDPA ("**NTPs**") were sent to Finantech as early as October 2014, Finantech's responses to these NTPs were only provided in April 2015 – almost seven months after the NTPs were first issued. This delayed the investigation process.

44. Having completed its investigation and assessment of this matter, the Commission is satisfied that K Box has been in breach of the Protection Obligation under section 24 of the PDPA and the Openness Obligation under sections 11(3) and 12(a) of the PDPA for the reasons cited in paragraphs 26 to 28 and paragraph 31 above. Pursuant to section 29(2) of the PDPA, the Commission hereby directs K Box to do as follows:

    (a) Pay a financial penalty of $50,000 within 30 days from the date of the Commission's direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall be payable on the outstanding amount of such financial penalty; and

    (b) Appoint a DPO within 30 days from the date of the Commission's direction (if it has not already done so).

45. The Commission is also satisfied that Finantech has not complied with the Protection Obligation under section 24 of the Act for the reasons cited in paragraphs 33, 34, 36 and 37 above. Pursuant to section 29(2) of the PDPA, the Commission hereby directs Finantech to do as follows:

    (a) Pay a financial penalty of $10,000 within 30 days from the date of the Commission's direction, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall be payable on the outstanding amount of such financial penalty.

46. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions.

LEONG KENG THAI
CHAIRMAN
PERSONAL DATA PROTECTION COMMISSION

[1] Mr G was the only employee at the material time of Finantech. Mrs G was the only person assisting Mr G in the past.
[2] Captain is the supervisor of the service crews and his or her role is to access the customers' information to check their booking.
[3] Both the Quotation for Web Hosting dated 11 September 2012 and the Quotation for Colocation Web Hosting and Server Management dated 6 November 2009 contain the following term "*FinanTech will maintain confidentiality of the client's data and undertake not to sell or give away the data to any third party.*"
[4] See paragraph 14.3 of the PDPC's Guide to Securing Personal Data in Electronic Medium issued on 8 May 2015.
[5] See section 2(1) of the PDPA.
[6] Namely, the "*website revamp contract dated 2012*" and the "*webhosting and server management contract dated 2009*".