Investigation Report

Published under Section 48(2) of
the Personal Data (Privacy) Ordinance (Cap. 486)

Ransomware Attack on the Database of Fotomax (F.E.) Limited

Report Number: R22 - 18947

Date Issued: 14 November 2022

PCPD
HK
PCPD.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Investigation Report: Ransomware Attack on the Database of Fotomax (F.E.) Limited

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that "*the* [Privacy Commissioner for Personal Data] *may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report -*

(a) setting out -

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit."

This investigation report is hereby published in the exercise of the powers conferred under section 48(2) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
14 November 2022

Table of Contents

Investigation Report

Published under Section 48(2) of
the Personal Data (Privacy) Ordinance (Cap. 486)

Ransomware Attack on the Database of Fotomax (F.E.) Limited

Executive Summary

Background

1. On 1 November 2021, Fotomax (F.E.) Limited (Fotomax) notified the Office of the Privacy Commissioner for Personal Data (the PCPD) of a data breach incident (the Notification), stating that the database of its online store (the Database) had been attacked by ransomware and maliciously encrypted, and that a hacker had demanded Fotomax to pay a ransom to unlock the encrypted files (the Incident).

2. On receipt of the Notification, the PCPD immediately commenced a compliance check against Fotomax to ascertain the relevant facts relating to the Incident. Upon receiving further information from Fotomax, the Privacy Commissioner for Personal Data (the Commissioner) believed that Fotomax's acts or practices in the Incident might have contravened the requirements of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance). In December 2021, the Commissioner commenced an investigation in relation to the Incident against Fotomax pursuant to section 38(b) of the Ordinance.

Investigation

3. During the course of investigation, the Commissioner reviewed and considered the information provided by Fotomax in relation to the Incident, including conducting seven rounds of enquiries regarding the security measures adopted for the Database, and examining the investigation reports provided by two independent information security consultants (the Consultants) engaged by Fotomax. The Commissioner also considered the follow-up and remedial measures taken by Fotomax in the wake of the Incident.

4. Fotomax reported that a total of 544,862 members and 73,957 visitors who had ordered products and/or services on its online store between 16 November 2020 and 26 October 2021 were affected in the Incident.

The Incident and the Associated Security Vulnerability

5. In March 2018, Fotomax purchased a firewall (the Firewall) from a service provider (the Service Provider) and installed and activated the Firewall in April to enhance network security. Fotomax subsequently enabled Secure Sockets Layer Virtual Private Network (SSL VPN) in March 2019 to allow staff of the Information Technology (IT) Department to remotely access its system when necessary.

6. In May 2019, the Firewall manufacturer issued a security advisory (the Advisory) on its website stating that it was aware of a vulnerability in its operating system (the Vulnerability) disclosed by a hacker. The Vulnerability would enable an attacker to bypass security restrictions and directly obtain SSL VPN account names and passwords to execute any programme in the target system. According to the Advisory, the Firewall manufacturer urged users to disable SSL VPN immediately until the

operating systems were upgraded and all account passwords were reset. Meanwhile, users were recommended to enable multi-factor authentication.

7. In August 2019, the Government Computer Emergency Response Team Hong Kong (GovCERT.HK) issued a high threat security alert on the Vulnerability, advising organisations to patch any affected systems immediately. If no patch could be deployed immediately, users should disable SSL VPN until the vulnerable systems have been patched. Subsequently, in December 2020, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) also reminded the corresponding local network providers and organisations to take appropriate remedial measures against the Vulnerability as soon as possible.

8. On the morning of 26 October 2021, staff of Fotomax's IT Department discovered that the online store and the Database could not be accessed as usual. In addition to the Database, some of the servers and computers in the office were also encrypted by ransomware.

The Consultants' Investigation Findings

9. After the Incident, Fotomax commissioned the Consultants to inspect the security of its information systems. The Consultants' findings, based on the two reports prepared by the Consultants, were that (i) Fotomax did not patch the affected system, thus allowing the hacker to exploit the Vulnerability, get hold of its SSL VPN account names and passwords, intrude into the system to obtain system administrative privileges, deploy ransomware and eventually succeed in encrypting the Database; and (ii) Fotomax did not enable multi-factor authentication for SSL VPN.

Responses from Fotomax to the Incident

10. Fotomax admitted to the PCPD that it was aware of the Vulnerability as early as September 2019 and alleged that it had discussed the matter with the Service Provider over the phone.

11. Fotomax explained that as a series of information security measures including anti-virus software, anti-ransomware programme and firewall had been put in place, it was considered unnecessary to immediately patch the Vulnerability after consultation with the Service Provider and internal assessment.

12. Fotomax also admitted that it did not conduct a comprehensive assessment on the Vulnerability because SSL VPN was only permitted for use by the IT Department to access the system remotely when needed. Even though work-from-home arrangements were subsequently implemented in response to the local outbreak of COVID-19 pandemic and employees were allowed to access the system remotely through SSL VPN, Fotomax did not re-evaluate the Vulnerability so that it remained unpatched at the time of the Incident.

Findings and Contravention

<u>Fotomax Being the Data User in the Incident</u>

13. Fotomax operates in Hong Kong and collects and manages the personal data in the Database. Fotomax is therefore a data user as defined under section 2(1) of the Ordinance and is required to comply with the requirements of the Ordinance, including the six Data Protection Principles (DPPs) set out in Schedule 1 to the Ordinance.

PCPD's understanding of the Cause of the Incident

14. Having reviewed the investigation reports of the Consultants, the responses from Fotomax to the Incident and all the information obtained by the PCPD during the course of investigation, the Commissioner agreed with the investigation reports that the Incident was caused by Fotomax's failure to patch to the affected system, which allowed the hacker to exploit the Vulnerability, get hold of its SSL VPN account names and passwords, intrude into the system to obtain system administrative privileges, deploy ransomware and subsequently succeed in encrypting the Database. Meanwhile, Fotomax did not enable multi-factor authentication for SSL VPN to enhance the security of the system.

Fotomax Contravened DPP4(1)

15. DPP4(1) stipulates that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use.

16. Having considered the facts of the Incident and the evidence obtained during the course of investigation, the Commissioner found that there were serious deficiencies in risk awareness and personal data security measures of Fotomax, which led to the avoidable intrusion of the Database and access to personal data stored therein by the hacker through exploitation of the security vulnerability: -

(1) Misevaluation of Security Vulnerability Risk: Although Fotomax was aware of the Vulnerability in the Firewall as early as September 2019, it did not take any action as it considered, upon internal assessment, that the then information security measures were sufficient to address the threat posed by the Vulnerability. The

Commissioner considered it regrettable that Fotomax was overly optimistic or even fluky about the known risks, and apparently misjudged the risk posed by the Vulnerability to its information system which contained personal data and the possible consequences in the event of hacker's intrusion of the information system. The Commissioner considered that if Fotomax had taken the reminders issued by the Firewall manufacturer, GovCERT.HK and HKCERT seriously and adopted a prudent approach to review its previous decisions, it could have identified the serious potential risk posed by the Vulnerability to its system and could have patched the Vulnerability as early as possible to prevent the Incident from happening.

(2) Deficiencies in Information System Management: Fotomax did not develop stringent patch management procedures, resulting in its failure to patch the security vulnerability of the Firewall in time thus allowing the hacker to intrude into the system successfully and encrypt the Database. In addition, Fotomax failed to enforce the password policy, resulting in more than 30 accounts in the system having insufficient password strength and being vulnerable to hacker attacks; Fotomax also had other information security deficiencies. The Commissioner considered that all of the above showed that the personal data security management of Fotomax was unsatisfactory, lacked stringent measures to regulate staff behaviour and system settings that enable timely system review, so that the security of information system which contained personal data was ineffective in addressing risks and threats.

(3) Procrastinated Implementation of Multi-factor Authentication: Back in May 2019, the Firewall manufacturer urged users to immediately disable SSL VPN until the operating system was updated

and all account passwords were reset so as to prevent attackers from bypassing security restrictions and directly obtaining account names and passwords by exploiting the Vulnerability. It also recommended that multi-factor authentication be enabled. However, Fotomax still had not implemented multi-factor authentication for SSL VPN to prevent hackers from using the leaked passwords to attack its system by the time of the Incident.

17. Having considered all evidence of this investigation, the Commissioner considered that Fotomax: -

(1) misjudged the risk of security vulnerability and failed to take any action for system security, thereby exposing the personal data in the Database to the risk of hacker's attacks;

(2) failed to properly manage the information system which contained personal data, such as not having a robust patch management program, which resulted in the failure to patch the security vulnerability in a timely manner, thus allowing the hacker to successfully intrude into the system through the Vulnerability and encrypt the Database; and

(3) failed to implement multi-factor authentication for SSL VPN as recommended by the Firewall manufacturer before the corporate-wide implementation of work-from-home arrangements to prevent hackers from attacking the system using the passwords acquired.

18. **In this case, the Commissioner found that there were serious deficiencies in risk awareness and personal data security measures of Fotomax which led to the ransomware attack on its Database. The Commissioner considered it regrettable that Fotomax was overly optimistic or even fluky about the known risks, and apparently**

misjudged the risk posed by the Vulnerability to its information system which contained personal data and the possible consequences in the event of hacker's intrusion of the information system. The Commissioner considered that Fotomax had not taken all practicable steps to ensure that the personal data involved was protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP4(1) concerning the security of personal data.

19. While the Incident reveals room for improvement on Fotomax's part, the Commissioner is pleased to note that Fotomax made a timely data breach notification, cooperated with the PCPD's investigation, and is committed to learning from the Incident. After the Incident, Fotomax has implemented various organisational and technical measures and fixed the security vulnerability to enhance the overall system security for the protection of personal data privacy.

Enforcement Action

20. The Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an enforcement notice on Fotomax (the Enforcement Notice), directing it to take the following steps to remedy and prevent recurrence of the contravention:

(1) Thoroughly review the security of Fotomax's systems containing personal data to ensure that they are free from known malware and security vulnerabilities;

(2) Engage an independent data security expert to conduct reviews and audits of Fotomax's system security (including the database of Fotomax's online store) on a regular basis;

(3) Revise the system security policy to explicitly require Fotomax to conduct regular vulnerability scans on its network equipment (including firewalls and/or servers);

(4) Revise the system security policy to specify the policies and requirements for patch management and take measures to ensure that relevant staff members and service providers providing system maintenance services should comply with those policies and requirements; and

(5) Provide documentary proof to the Commissioner within three months from the date of the Enforcement Notice, showing the completion of items (1) to (4) above.

Recommendations

21. Through this report, the Commissioner would like to remind organisations that handle customers' personal data to pay particular attention to the following areas: -

(1) **Stay Vigilant to Prevent Hacker Attacks:** In the wake of different security vulnerabilities, organisations should always stay vigilant and conduct regular risk assessments to review the potential impact of hacking on their systems and enhance the protection of the systems which contain personal data such as email servers, customer databases, etc.

(2) **Establish a Personal Data Privacy Management Programme:** Organisations should have a robust personal data privacy management programme, use and retain personal data in compliance with the Ordinance, and manage the entire lifecycle of personal data

from collection to destruction effectively, so that they could respond to data breach incidents promptly and gain trust from customers and other stakeholders.

(3) **Appoint Dedicated Officer as Data Protection Officer:** Organisations should clearly define the roles and responsibilities of a data protection officer, including monitoring compliance with the Ordinance and reporting to senior management, as well as incorporating data protection issues raised by staff and experiences and lessons on data breach incidents involving customers' personal data into the organisation's training materials.

(4) **Enhance Information System Management:** Organisations should develop effective patch management procedures to patch security vulnerabilities as early as possible and adopt appropriate technical security measures having regard to the amount and sensitivity of personal data contained in the system, such as using multi-factor authentication when connecting to a virtual private network, to provide additional security to systems and accounts.

(5) **Maintain Proper Documentation of Internal Communications:** When an organisation is confronted with different advice from a network equipment manufacturer and an information system service provider, it should exercise prudence and due diligence by consulting the manufacturer concerned in writing to seek further advice or clarify appropriate follow-up actions. Organisations should keep all correspondence during the consultation period for reference in future reviews.

Other Comments

22. The Commissioner understands that many organisations offer membership schemes, some of which allow purchases to be accumulated and converted into cash discounts for future transactions which adds value to membership accounts. However, consumers may not manage their accounts regularly and inactive accounts that remain idle for a long period of time not only impose extra cost on organisations to protect personal data, but also increase the risk of data breach. Moreover, the longer the data is retained, the greater the chance that the data becomes inaccurate owing to obsolescence.

23. According to the information provided by Fotomax, about 65% of the 544,862 affected members (around 350,000 members) had no login activity between the time they created their accounts and the time of the Incident. While Fotomax stated that members could request deletion of their membership and personal data, **the Commissioner considered that it might not fall within customers' reasonable expectation of personal data privacy for organisations to retain inactive users' personal data over a prolonged period simply because they have not received a request for account termination.** Fotomax subsequently informed the Commissioner that it would purge the personal data of dormant members if there were no sales engagements with the member in the past three years.

24. **In addition, the Commissioner noted that Fotomax had ceased to collect members' days of birth since 16 November 2020 after the revamp of its online store. The Commissioner considered that organisations should carefully consider the purposes for which personal data is collected and should be mindful to set a retention period for personal data without compromising the purposes for which the data is to be used, instead of retaining personal data solely for operational convenience. The Commissioner took the opportunity to**

remind Fotomax to review its database and delete unnecessary personal data as soon as possible (including examining the necessity of continuing to keep the records of days of birth of members that have been collected).

25. The increased digitisation of data and interconnection of information and communications technology (ICT), together with the increasing value of data, have exacerbated personal data security risks. This is evidenced by the upward trend in the number of data security incidents reported both in Hong Kong and other jurisdictions. The impact of a data security incident – both in terms of reputational damage and financial cost – could be devastating to a data user of any size, from small- and medium-sized enterprises to multinational companies.

26. The Commissioner wishes to point out that a robust data security system is an essential element of good data governance. The Commissioner is mindful that as the steps required of a data user to protect personal data may vary from case to case, data users should consult their own data security experts and legal advisers on whether the relevant requirements under the Ordinance are met. Reference may also be made to the "Guidance Note on Data Security Measures for Information and Communications Technology"[1] recently published by the PCPD, so as to understand the proposed ICT-related data security measures and good practices in enhancing data security systems.

[1] www.pcpd.org.hk//english/resources_centre/publications/files/guidance_datasecurity_e.pdf

I. Introduction

1. On 29 October 2021, China-Hongkong Photo Products Holdings Limited, the parent company of Fotomax (F.E.) Limited (Fotomax), made an announcement[2] that the photofinishing and imaging solutions database of the system of Fotomax was accessed without authorisation on 26 October 2021. The affected database contained personal data of Fotomax's customers.

2. On 1 November 2021, Fotomax notified the Office of the Privacy Commissioner for Personal Data (the PCPD) of a data breach incident (the Notification), stating that the database of its online store (i.e. the aforementioned photofinishing and imaging solutions database) (the Database) had been attacked by ransomware and maliciously encrypted, and that a hacker had demanded Fotomax to pay a ransom to unlock the encrypted files (the Incident).

3. On receipt of the Notification, the PCPD immediately commenced a compliance check against Fotomax to ascertain the relevant facts relating to the Incident. Upon receiving further information from Fotomax, the Privacy Commissioner for Personal Data (the Commissioner) believed that Fotomax's acts or practices in the Incident might have contravened the requirements of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance). In December 2021, the Commissioner commenced an investigation in relation to the Incident against Fotomax pursuant to section 38(b) of the Ordinance.

[2] www1.hkexnews.hk/listedco/listconews/sehk/2021/1029/2021102900963.pdf

II. Statutory Powers and Relevant Legal Requirements

Statutory Powers

4. Section 38 of the Ordinance empowers the Commissioner to conduct investigations under the following circumstances:

   (i) Where the Commissioner receives a complaint from the affected data subject or his representative, the Commissioner shall, in accordance with section 38(a) and subject to section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in the complaint is a contravention of a requirement under the Ordinance; or

   (ii) Where the Commissioner has reasonable grounds to believe that an act or practice relates to personal data has been done or engaged in, or is being done or engaged in by a data user, which may be a contravention of a requirement under the Ordinance, the Commissioner may, in accordance with section 38(b), carry out an investigation in relation to the relevant data user to ascertain whether the act or practice is a contravention of a requirement under the Ordinance.

5. After initiating an investigation, the Commissioner may, in accordance with section 43(1)(a) of the Ordinance, for the purposes of the investigation be furnished with any information, document or thing from such persons, and make such inquiries, as she thinks fit.

6. Section 48(2)(a) of the Ordinance stipulates that the Commissioner may, after completing an investigation and if she is of the opinion that it is in the public interest to do so, publish a report setting out the result of the

investigation, any recommendations and other comments arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the Ordinance by the class of data users to which the relevant data user belongs.

7. Section 50(1) of the Ordinance provides that following the completion of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, the Commissioner may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent recurrence of the contravention.

8. Under section 50A of the Ordinance, a data user who contravenes an enforcement notice commits an offence and is liable to a maximum fine at level 5 (i.e. HK$50,000) and imprisonment for 2 years on first conviction.

Relevant Legal Requirements

Data User

9. The Ordinance, including the Data Protection Principles (DPPs) in Schedule 1 thereof, aims to regulate the acts and practices of data users. Under section 2(1) of the Ordinance, a data user, in relation to personal data, means "*a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*".

Personal Data

10. Data users falling within the purview of the Ordinance are required to comply with the DPPs in handling "personal data". Under section 2(1) of the Ordinance, "personal data" means "*any data* –

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable."

Data Security

11. DPP4(1) provides for the principle on personal data security, which states that: -

"*All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to –*

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data."

12. "Practicable" is defined in section 2(1) of the Ordinance to mean "*reasonably practicable*".

13. Regarding the "harm" test set out in DPP4(1)(a) above, considerations have to be given to whether the security measures undertaken by the data users are commensurate with the sensitivity of the personal data concerned;

and the harm that might result from unauthorised or accidental access to such data.

III. Information and Evidence Obtained from the Investigation

14. During the course of investigation, the Commissioner reviewed and considered the information provided by Fotomax in relation to the Incident, including conducting seven rounds of enquiries regarding the security measures adopted for the Database, and examining the investigation reports provided by two independent information security consultants (the Consultants) engaged by Fotomax. The Commissioner also considered the follow-up and remedial measures taken by Fotomax in the wake of the Incident.

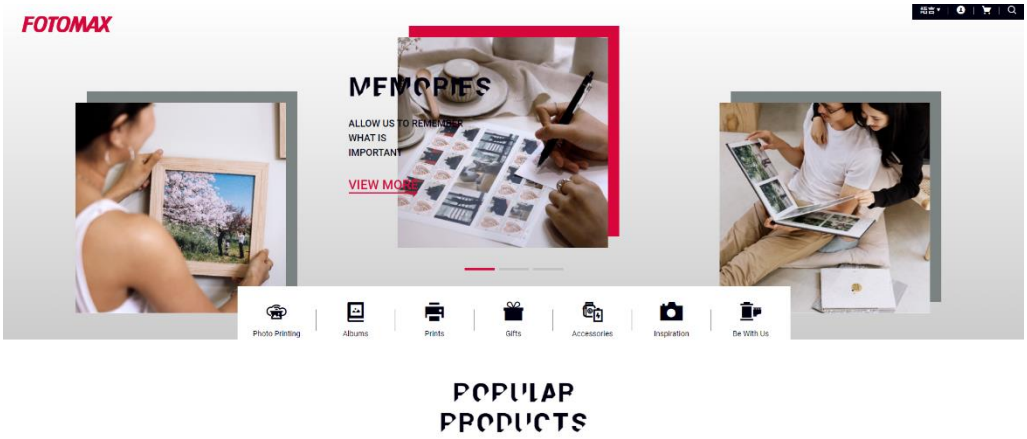
Company Background and Membership Programme

15. Established in 1982, Fotomax has been a wholly owned subsidiary of China-Hongkong Photo Products Holdings Limited since 2001. It operates 55 physical stores and online shops, providing retail services in film processing, photofinishing, passport photo services and peripheral products in Hong Kong.

16. Fotomax has been operating a membership programme since October 2000. To become a member, a customer is required to complete an application form[3] and provide his personal data online. Personal data collected included name, gender, day and month of birth[4], email address and phone number. Membership is considered permanent and Fotomax retains the membership information indefinitely unless and until a member requests deletion of membership.

[3] www.fotomax.com/en-us/account/register

[4] The collection of day of birth has been ceased since 16 November 2020 after the revamp of the online store.



Screenshot of Fotomax's Website (August 2022)

The Incident and the Associated Security Vulnerability

17. On the morning of 26 October 2021, staff of Fotomax's Information Technology (IT) Department discovered that the online store and the Database could not be accessed as usual. In addition to the Database, some of the servers and computers in the office were also encrypted by ransomware.

18. Fotomax immediately reviewed the activity logs of the firewall and discovered that a hacker had used a compromised staff account to log in to Fotomax's system through the Secure Sockets Layer Virtual Private Network (SSL VPN)[5] on the evening of 25 October. The hacker then infiltrated other computers and servers, including the system administrator account, through brute force attack[6] and installed ransomware to demand a ransom.

[5] SSL VPN allows users to use an Internet browser to connect their virtual private network devices through an encrypted communication channel. (www.infosec.gov.hk/en/best-practices/business/vpn-security)

[6] Brute force attack is the crack of credentials using all possible combinations by trial-and-error method until the password is guessed correctly. (www.infosec.gov.hk/en/knowledge-centre/bruteforce)

A ransom note provided by Fotomax

19. According to the information provided by Fotomax, only one of the servers affected in the Incident contained the Database and personal data.

20. Fotomax stated that it purchased a firewall (the Firewall) from a service provider (the Service Provider) in March 2018, and installed and activated the Firewall in April to enhance network security. Fotomax subsequently enabled SSL VPN in March 2019 to allow staff of the IT Department to remotely access its system when necessary.

21. In May 2019, the Firewall manufacturer issued a security advisory (the Advisory)[7] on its website stating that it was aware of a vulnerability in its operating system[8] (the Vulnerability)[9] disclosed by a hacker. The Vulnerability would enable an attacker to bypass security restrictions and directly obtain SSL VPN account names and passwords to execute any programme in the target system. According to the Advisory, the Firewall manufacturer urged users to disable SSL VPN immediately until the operating systems were upgraded and all account passwords were reset.

[7] www.fortiguard.com/psirt/FG-IR-18-384

[8] The affected operating systems included FortiOS 5.4.6 to 5.4.12; FortiOS 5.6.3 to 5.6.7 and FortiOS 6.0.0 to 6.0.4.

[9] According to the Security Bulletin of the Hong Kong Computer Emergency Response Team Coordination Centre, the identifier of the Vulnerability was CVE-2018-13379. (www.hkcert.org/security-bulletin/fortinet-fortos-multiple-vulnerabilities)

Meanwhile, users were recommended to enable multi-factor authentication.

22. The Government Computer Emergency Response Team Hong Kong (GovCERT.HK) issued a high threat security alert on the Vulnerability in August 2019, advising organisations to patch any affected systems immediately. If no patch could be deployed immediately, users should disable SSL VPN until the vulnerable systems have been patched[10].

23. In November 2020, a hacker shared a list (the List) of IP addresses[11] of more than 49,000 devices that had not yet been patched for the Vulnerability online. The Firewall manufacturer then issued another article in the same month reminding users to deploy the patch as soon as possible[12].

24. Subsequently in December 2020, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) also pointed out that around 1,000 IP addresses on the List came from Hong Kong and reminded the corresponding local network providers and organisations to take appropriate remedial measures against the Vulnerability as soon as possible[13].

Policies of Fotomax on Information Security

25. During the course of investigation, Fotomax submitted the following policies relating to the protection of personal data to the PCPD: -

[10] www.govcert.gov.hk/en/alerts_detail.php?id=414
[11] Equivalent to Internet Protocol
[12] www.fortinet.com/blog/psirt-blogs/update-regarding-cve-2018-13379
[13] www.hkcert.org/blog/patch-fortios-ssl-vpn-vulnerability-cve-2018-13379-immediately

26. Prior to the Incident, Fotomax had put in place an "*Information Security Policy*" (IS Policy) which set out the overall security management framework for the data held by it, including the acceptable use policies for Internet and email, file access restrictions and physical security policy.

27. Fotomax issued a "*Password Policy*" (the Password Policy) and a "*Bring-Your-Own-Device Policy*" in April 2018 and October 2019 respectively. The former specified the password validity period, minimum password length and complexity requirements for different types of accounts, while the latter required employees to register their own devices with the IT Department and to affirm that an effective antivirus software had been installed on the relevant devices before they could be used in office.

28. Fotomax stated that prior to the Incident, it had provided the abovementioned policies to its employees via the Intranet. In addition, employees who are employed after 1 November 2016 must sign to acknowledge that they have read and agree to comply with the IS Policy.

Affected Personal Data

29. Fotomax reported that a total of 544,862 members and 73,957 visitors who had ordered products and/or services on its online store between 16 November 2020 and 26 October 2021 were affected in the Incident.

30. According to Fotomax, the personal data concerned of the affected members and visitors were as follows: -

Affected Members	**Affected Visitors**
(i) Name (ii) Gender (iii) Month and day of birth	(i) Name (ii) Phone number (iii) Email address

Affected Members	Affected Visitors
(iv) Phone number (v) Email address (vi) Contact address (vii) Delivery address	(iv) Delivery address

31. Fotomax provided the PCPD with the relevant figures for each type of personal data affected by the Incident: -

	Affected Members	Affected Visitors
Name	544,862 (100%)	73,957 (100%)
Gender	358,012 (65.7%)	
Month of birth	330,378 (60.6%)	
Day of birth	202,514 (37.2%)	
Phone number	486,050 (89.2%)	73,414 (99.3%)
Email address	544,862 (100%)	73,957 (100%)
Contact address	3,293 (0.6%)	
Delivery address	1,030 (0.2%)	1,190 (1.6%)

(Figures in brackets are the quantities of affected personal data as a percentage of the total number of data subjects in that category)

32. Fotomax confirmed that no credit card data (including name, credit card number and expiry date) used for online store transactions was stored in its system as the data was handled by a third-party online payment system directly.

33. Fotomax stated that members were only required to provide their name, phone number and email address during registration while the remaining items were optional. As regards visitors, they were only required to register with their name, phone number and email address. Members could fill in their contact address as the default delivery address after registration. If members and visitors requested delivery service instead of in-store pickup, they must fill in a delivery address separately.

The Consultants' Findings

34. After the Incident, Fotomax commissioned the Consultants to inspect the security of its information systems and submitted reports to the PCPD for review in the course of investigation. Based on the reports prepared by the Consultants: -

(i) Fotomax did not patch the affected system, thus allowing the hacker to exploit the Vulnerability, get hold of its SSL VPN account names and passwords, intrude into the system to obtain system administrative privileges, deploy ransomware and eventually succeed in encrypting the Database. System logs indicated that the earliest suspicious login activity could be dated back to 1 October 2021, implying that the hacker had lurked in Fotomax's system for a certain period of time prior to the Incident;

(ii) Fotomax did not enable multi-factor authentication for SSL VPN;

(iii) More than 30 accounts in the system had insufficient password strength. Some passwords contained only digits, were similar to the account names or were default passwords. However, the reports did not contain sufficient evidence to prove that insufficient password strength was one of the factors contributed to the successful hacking of the system; and

(iv) The security review identified a series of deficiencies[14], although there was no indication that these deficiencies had directly led to the Incident.

Responses from Fotomax to the Incident

35. Fotomax admitted to the PCPD that it was aware of the Vulnerability as early as September 2019 and alleged that it had discussed the matter with the Service Provider over the phone.

36. Fotomax explained that as a series of information security measures including anti-virus software, anti-ransomware programme and firewall had been put in place, it was considered unnecessary to immediately patch the Vulnerability after consultation with the Service Provider and internal assessment. However, as Fotomax's discussions with the Service Provider were not documented, the Commissioner could not know the contents and other details of the discussions.

37. Fotomax also admitted that it did not conduct a comprehensive assessment on the Vulnerability because SSL VPN was only permitted for use by the IT Department to access the system remotely when needed. Even though work-from-home arrangements were subsequently implemented in response to the local outbreak of COVID-19 pandemic and employees

[14] The details are redacted to protect sensitive information of the relevant information system security.

were allowed to access the system remotely through SSL VPN, Fotomax did not re-evaluate the Vulnerability so that it remained unpatched at the time of the Incident.

Follow-up Actions and Remedial Measures

38. Fotomax stated that it suspended the affected systems including SSL VPN, despatched personnel to check other systems and updated the anti-virus software immediately after the Incident.

39. Fotomax has subsequently updated the operating system of the Firewall to patch the Vulnerability, changed all system administrator account passwords, and reset all SSL VPN account passwords to increase their complexity.

40. In response to other recommendations made by the Consultants set out in the investigation reports, Fotomax took the following remedial measures to prevent recurrence of similar incidents: -

    (i) Implemented two-factor authentication for SSL VPN;

    (ii) Installed programmes on its computers and servers to detect suspicious network traffic so as to enhance protection against network attacks;

    (iii) Conducted regular vulnerability scans and checked for patches available for installation, and retained relevant assessment records; and

(iv) Implemented a series of enhancement measures[15] on its information security system to enhance system security.

[15] The details are redacted to protect sensitive information of the relevant information system security.

IV. Findings and Contravention

41. In accordance with DPP4(1), all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use. In the present case, the factors considered by the Commissioner include: (i) whether the Incident is a data breach; (ii) who is the data user accountable for the data breach; and (iii) whether all practicable steps have been taken by the data user to protect the personal data held by it in accordance with the requirements of DPP4(1). The findings of the Commissioner are set out herein below.

Nature of the Incident

42. A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use, which may amount to a contravention of DPP4 of the Ordinance.

43. During the course of investigation, Fotomax advised the PCPD that there was insufficient evidence to substantiate that the Incident resulted in personal data leakage. However, the Commissioner considered that as the hacker exploited the Vulnerability to access the Database containing personal data, it constituted a prima facie case of unauthorised access and/or processing of personal data.

Fotomax Being the Data User in the Incident

44. Fotomax operates in Hong Kong and collects and manages the personal data in the Database. Fotomax is therefore a data user as defined under section 2(1) of the Ordinance and is required to comply with the requirements of the Ordinance, including the six DPPs set out in Schedule 1 to the Ordinance.

PCPD's understanding of the Cause of the Incident

45. Having reviewed the investigation reports of the Consultants, the responses from Fotomax to the Incident and all the information obtained by the PCPD during the course of investigation, the Commissioner agreed with the investigation reports that the Incident was caused by Fotomax's failure to patch to the affected system, which allowed the hacker to exploit the Vulnerability, get hold of its SSL VPN account names and passwords, intrude into the system to obtain system administrative privileges, deploy ransomware and subsequently succeed in encrypting the Database. Meanwhile, Fotomax did not enable multi-factor authentication for SSL VPN to enhance the security of the system.

Serious Deficiencies in Data Security

46. DPP4(1) stipulates that all practicable steps shall be taken to ensure that any personal data held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to –

(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means of otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

47. When considering whether Fotomax complied with the requirements of DPP4(1) in this case, the Commissioner took into consideration the security measures taken by Fotomax in respect of the Database at the material time (i.e. at the time of the Incident) and how Fotomax dealt with the known data security risks.

48. Having considered the facts of the Incident and the evidence obtained during the course of investigation, the Commissioner found that there were serious deficiencies in risk awareness and personal data security measures of Fotomax, which led to the avoidable intrusion of the Database and access to personal data stored therein by the hacker through exploitation of the security vulnerability.

(1) *Misevaluation of Security Vulnerability Risk*

49. Although Fotomax was aware of the Vulnerability in the Firewall as early as September 2019, Fotomax stated that it did not take any action as it considered, upon internal assessment, that the then information security measures were sufficient to address the threat posed by the Vulnerability.

50. Since Fotomax failed to provide any documentary evidence to prove that it had discussed the Vulnerability with the Service Provider and did not provide any relevant internal assessment records, the Commissioner was not satisfied with Fotomax's aforesaid explanation based on objective evidence. The evidence and information obtained from the investigation

indicated that Fotomax had not conducted any formal or documented risk assessment on the Vulnerability and the Vulnerability remained unpatched at the time of the Incident.

51. The Commissioner regarded firewall as an important barrier to keep systems protected. The fact that the hacker exploited the Vulnerability to obtain account names and passwords is, in nature, equivalent to password leakage and the security risk should not be understated. In this case, the Commissioner considered it regrettable that Fotomax was overly optimistic or even fluky about the known risks, and apparently misjudged the risk posed by the Vulnerability to its information system which contained personal data and the possible consequences in the event of hacker's intrusion of the information system.

52. From September 2019 when Fotomax decided not to take any action on the Vulnerability till the Incident in October 2021, the Firewall manufacturer, GovCERT.HK and HKCERT had repeatedly reminded users to patch the Vulnerability. The Commissioner considered that if Fotomax had taken these reminders seriously and adopted a prudent approach to review its previous decision, it could have identified the serious potential risk posed by the Vulnerability to its system and could have patched the Vulnerability as early as possible to prevent the Incident from happening.

(2) *Deficiencies in Information System Management*

53. The Commissioner considered that Fotomax did not develop stringent patch management procedures, resulting in its failure to patch the security vulnerability of the Firewall in time after becoming aware of it thus allowing the hacker to intrude into the system successfully and encrypt the Database. The Commissioner considered that Fotomax had clearly failed

to discharge the duties of a data user and had not taken all practicable steps to protect the personal data stored in the Database.

54. In addition, from the investigation reports prepared by the Consultants, the Commissioner noted the following deficiencies in the security measures of Fotomax's information system at the time of the Incident: -

(i) The Password Policy was not enforced, resulting in more than 30 accounts in the system having insufficient password strength and being vulnerable to hacker attacks; and

(ii) Other information security deficiencies[16].

55. Although there was no indication that these deficiencies directly led to the Incident, the Commissioner considered that all of the above showed that the personal data security management of Fotomax was unsatisfactory, lacked stringent measures to regulate staff behaviour and system settings that enable timely system review, so that the security of information system which contained personal data was ineffective in addressing risks and threats.

(3) *Procrastinated Implementation of Multi-factor Authentication*

56. The Advisory issued by the Firewall manufacturer in May 2019 suggested that an attacker could bypass the security restrictions and directly obtain the Secure Sockets Layer Virtual Private Network (SSL VPN) account names and passwords, and execute any programme on the target systems by exploiting the Vulnerability. The Firewall manufacturer therefore urged users to immediately disable SSL VPN until the operating system was updated and all account passwords were reset. It also recommended that multi-factor authentication be enabled. However, Fotomax still had not

[16] The details are redacted to protect sensitive information of the relevant information system security.

implemented multi-factor authentication for SSL VPN to prevent hackers from using the leaked passwords to attack its system by the time of the Incident.

57. In response to the local outbreak of COVID-19 pandemic, Fotomax implemented work-from-home arrangements on three occasions between 2020 and February 2021, each lasted for approximately four weeks and allowed employees to use their own devices or company-owned laptops to connect to its system through SSL VPN.

58. Regarding the fact that multi-factor authentication was not activated before the corporate-wide implementation of work-from-home arrangements, Fotomax explained that since each work-from-home arrangement lasted for a short period of time, it was assessed that the then security measures were sufficient to protect against cyberattacks.

59. The Commissioner considered that Fotomax was overconfident in its data security measures, and had adopted a reckless attitude on work-from-home arrangements which lasted for a total period of approximately three months without conducting a proper and prudent risk assessment and adopting appropriate data security measures. The Commissioner also considered that based on the recommendations made by the Firewall manufacturer and the fact that Fotomax allowed its employees to remotely access its system through SSL VPN under work-from-home arrangements, Fotomax should have reasonably implemented multi-factor authentication to enhance security measures and to safeguard its system containing personal data. In the Incident, Fotomax's exposure of its information system which contained personal data to known risks was the primary reason why the Database suffered a ransomware attack under avoidable circumstances.

60. In considering the elements of adequate data security controls, the Commissioner referred to the best practice of network security provided by the Office of the Government Chief Information Officer[17]. These recommendations include the following:

(1) Plan for network security: address all security requirements and issues in the selection and deployment of networks and servers including the management policy, technical training and outsourcing requirements, and address security.

(2) Configure servers: for example, secure the server operating system by uninstalling unnecessary services and software, patch the system in a timely manner and disable unused accounts.

(3) Secure the application: by means of installing security patch, enhance application settings or lock the environment in which applications operate.

(4) Develop security management procedure: for example, security log monitoring procedure, change management procedure or patch management procedure.

(5) Maintain documentation of configuration and procedure.

(6) Train the staff: training should be given to network/security administrator and supporting staff as well as general staff to ensure that they follow the security best practice and follow security policies.

[17] www.infosec.gov.hk/en/best-practices/business/securing-company-network

61. The Commissioner noted that Fotomax failed to comply with most of the security measures recommended in the above guidelines at the material time, thus failing to safeguard the personal data in the Database from hacker's attack.

Conclusion – Contravention of DPP4(1)

62. The Commissioner acknowledges that the steps required of a data user under DPP4(1) to protect the personal data held by the data user vary from case to case, and that a host of factors will need to be taken into account. These include the volume, nature and sensitivity of data, the harm and damage that could result from data breach, data governance and organisational measures, as well as the technical policies, operations, controls and other security measures of the quality and standard reasonably expected of similar organisations.

63. The Commissioner considered that Fotomax, as a data user operating a number of physical stores and online shops which provides retail services in photofinishing throughout Hong Kong, holds a significant amount of customers' personal data. It should have formulated comprehensive policies relating to the collection, holding, processing and use of customers' personal data, conducted proper risk assessments and taken all practicable security measures to ensure that the personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use in accordance with DPP4(1).

64. Having considered all evidence of this investigation, the Commissioner considered that Fotomax: -

(1) misjudged the risk of security vulnerability and failed to take any action for system security, thereby exposing the personal data in the Database to the risk of hacker's attacks;

(2) failed to properly manage the information system which contained personal data, such as not having a robust patch management program, which resulted in the failure to patch the security vulnerability in a timely manner, thus allowing the hacker to successfully intrude into the system through the Vulnerability and encrypt the Database; and

(3) failed to implement multi-factor authentication for SSL VPN as recommended by the Firewall manufacturer before the corporate-wide implementation of work-from-home arrangements to prevent hackers from attacking the system using the passwords acquired.

65. **In this case, the Commissioner found that there were serious deficiencies in risk awareness and personal data security measures of Fotomax which led to the ransomware attack on its Database. The Commissioner considered it regrettable that Fotomax was overly optimistic or even fluky about the known risks, and apparently misjudged the risk posed by the Vulnerability to its information system which contained personal data and the possible consequences in the event of hacker's intrusion of the information system. The Commissioner considered that Fotomax had not taken all practicable steps to ensure that the personal data involved was protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP4(1) concerning the security of personal data.**

66. While the Incident reveals room for improvement on Fotomax's part, the Commissioner is pleased to note that Fotomax made a timely data breach notification, cooperated with the PCPD's investigation, and is committed

to learning from the Incident. After the Incident, Fotomax has implemented various organisational and technical measures and fixed the security vulnerability to enhance the overall system security for the protection of personal data privacy.

V. Enforcement Action

67. Having found that Fotomax contravened DPP4(1) in Schedule 1 to the Ordinance, the Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an enforcement notice on Fotomax (the Enforcement Notice), directing it to take the following steps to remedy and prevent recurrence of the contravention:

(1) Thoroughly review the security of Fotomax's systems containing personal data to ensure that they are free from known malware and security vulnerabilities;

(2) Engage an independent data security expert to conduct reviews and audits of Fotomax's system security (including the database of Fotomax's online store) on a regular basis;

(3) Revise the system security policy to explicitly require Fotomax to conduct regular vulnerability scans on its network equipment (including firewalls and/or servers);

(4) Revise the system security policy to specify the policies and requirements for patch management and take measures to ensure that relevant staff members and service providers providing system maintenance services should comply with those policies and requirements; and

(5) Provide documentary proof to the Commissioner within three months from the date of the Enforcement Notice, showing the completion of items (1) to (4) above.

68. Under section 50A of the Ordinance, a data user who contravenes an enforcement notice commits an offence and is liable, on first conviction, to a maximum fine at level five (i.e. HK$50,000) and imprisonment for two years.

VI. Recommendations and Other Comments

69. Section 48(2)(a) of the Ordinance stipulates that the Commissioner may, after completing an investigation and, if she is of the opinion that it is in the public interest to do so, publish a report setting out the result of the investigation, any recommendations and other comments arising from the investigation that the Commissioner thinks fit to make.

Recommendations

70. The Commissioner understands that the cyber landscape has been evolving rapidly and organisations might not be able to respond appropriately in the face of security risks due to limited information available at the time. In particular, in light of the COVID-19 epidemic, many organisations have experienced a dramatic change in their mode of operation as work-from-home arrangements or hybrid work-from-home model becomes a "new norm". In the present case, SSL VPN was initially used by the IT Department on a need basis only but subsequently work-from-home arrangements were widely implemented within the organisation in response to the epidemic, rendering previous security measures inapt. The Commissioner therefore considers it particularly important for organisations to monitor information about security risks to personal data system on a regular basis.

71. Through this report, the Commissioner would like to remind organisations that handle customers' personal data to pay particular attention to the following areas: -

(1) **Stay Vigilant to Prevent Hacker Attacks:** In the wake of different security vulnerabilities, organisations should always stay vigilant, conduct regular risk assessments to review the potential impact of

hacking on their systems, and enhance the protection of the systems which contain personal data such as email servers, customer databases, etc.

(2) **Establish a Personal Data Privacy Management Programme:** Organisations should have a robust personal data privacy management programme, use and retain personal data in compliance with the Ordinance, and manage the entire lifecycle of personal data from collection to destruction effectively, so that they could respond to data breach incidents promptly and gain trust from customers and other stakeholders.

(3) **Appoint Dedicated Officer as Data Protection Officer:** Organisations should clearly define the roles and responsibilities of a data protection officer, including monitoring compliance with the Ordinance and reporting to senior management, as well as incorporating data protection issues raised by staff and experiences and lessons on data breach incidents involving customers' personal data into the organisation's training materials.

(4) **Enhance Information System Management:** Organisations should develop effective patch management procedures to patch security vulnerabilities as early as possible and adopt appropriate technical security measures having regard to the amount and sensitivity of personal data contained in the system, such as using multi-factor authentication when connecting to a virtual private network, to provide additional security to systems and accounts.

(5) **Maintain Proper Documentation of Internal Communications:** When an organisation is confronted with different advice from a network equipment manufacturer and an information system service provider, it should exercise prudence and due diligence by

consulting the manufacturer concerned in writing to seek further advice or clarify appropriate follow-up actions. Organisations should keep all correspondence during the consultation period for reference in future reviews.

Other Comments

72. The Commissioner understands that many organisations offer membership schemes, some of which allow purchases to be accumulated and converted into cash discounts for future transactions which adds value to membership accounts. However, consumers may not manage their accounts regularly and inactive accounts that remain idle for a long period of time not only impose extra cost on organisations to protect personal data, but also increase the risk of data breach. Moreover, the longer the data is retained, the greater the chance that the data becomes inaccurate owing to obsolescence.

73. According to the information provided by Fotomax, about 65% of the 544,862 affected members (around 350,000 members) had no login activity between the time they created their accounts and the time of the Incident. While Fotomax stated that members could request deletion of their membership and personal data, **the Commissioner considered that it might not fall within customers' reasonable expectation of personal data privacy for organisations to retain inactive users' personal data over a prolonged period simply because they have not received a request for account termination.** Fotomax subsequently informed the Commissioner that it would purge the personal data of dormant members if there were no sales engagements with the member in the past three years.

74. **In addition, the Commissioner noted that Fotomax had ceased to collect members' days of birth since 16 November 2020 after the revamp of its online store. The Commissioner considered that organisations should carefully consider the purposes for which personal data is collected and should be mindful to set a retention period for personal data without compromising the purposes for which the data is to be used, instead of retaining personal data solely for operational convenience. The Commissioner took the opportunity to remind Fotomax to review its database and delete unnecessary personal data as soon as possible (including examining the necessity of continuing to keep the records of days of birth of members that have been collected).**

75. The increased digitisation of data and interconnection of information and communications technology (ICT), together with the increasing value of data, have exacerbated personal data security risks. This is evidenced by the upward trend in the number of data security incidents reported both in Hong Kong and other jurisdictions. The impact of a data security incident – both in terms of reputational damage and financial cost – could be devastating to a data user of any size, from small- and medium-sized enterprises to multinational companies.

76. The Commissioner wishes to point out that a robust data security system is an essential element of good data governance. The Commissioner is mindful that as the steps required of a data user to protect personal data may vary from case to case, data users should consult their own data security experts and legal advisers on whether the relevant requirements under the Ordinance are met. Reference may also be made to the "Guidance Note on Data Security Measures for Information and Communications Technology"[18] recently published by the PCPD, so as to

[18] https://www.pcpd.org.hk//english/resources_centre/publications/files/guidance_datasecurity_e.pdf

understand the proposed ICT-related data security measures and good practices in enhancing data security systems.

— End —