PERSONAL DATA PROTECTION COMMISSION

[2017] SGPDPC 19

Case No DP-1611-B0368

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

And

ComGateway (S) Pte. Ltd.

… *Organisation*

GROUNDS OF DECISION

ComGateway (S) Pte. Ltd.

[2017] SGPDPC 19

Tan Kiat How, Commissioner — Case No DP-1611-B0368

29 December 2017

Background

1 On 29 November 2016, the Complainant, a customer of the Organisation, informed the Personal Data Protection Commission (the "**Commission**") that:

(a) when the Organisation provided a shipping details webpage ("**Shipping Webpage**"), it disclosed the Complainant's personal data (in the form of shipping details) to another customer (the "**First Data Breach**"); and

(b) the URL[1] of the Shipping Webpage of one customer could be manipulated to enable access to shipping details of other customers, by changing the last character (the "**Second Data Breach**").

2 The shipping details included personal data such as the customer's name, contact number and address.

---

1 <www.comgateway.com/ship_track_detail?shipId=MTYwMTExMQ>.

3 The Commissioner ultimately found the Organisation not to be in breach of the Personal Data Protection Act 2012 ("**PDPA**") in respect of the First Data Breach, but in breach of Section 24 of the PDPA in respect of the Second Data Breach. The Commissioner's findings are now set out below.

Material Facts

4 The Organisation operates an online portal that provides logistics, shopping ("**buy-for-me**") and shipping services to its customers.

5 The Organisation uses an electronic system and application through and on its website (the "**Website**") to process, track and manage shipping / transaction orders from its customers.

6 The Organisation had been conducting quarterly "Trustwave" vulnerability scans and annual penetration tests for its external and internal networks. The vulnerability scans were used to identify and report on network security vulnerabilities that could be exploited by cybercriminals. The internal penetration test was conducted to evaluate the resiliency of the Organisation's systems to various attacks launched against internal network resources from the perspective of an unauthenticated attack on the internal network. The external penetration test was conducted to evaluate the resiliency of the Organisation's systems and networks to various attacks launched from the Internet. The Organisation had also signed up for a managed firewall application which monitors and protects its networks against attacks and data loss.

7 Additionally, as part of its overall information technology (IT) security arrangement, the Organisation also ran automated code checks to detect any "OWASP" top 10 application security risks on its Website. The Organisation

had last passed all the mentioned scans and tests in 2016 before the occurrence of the First and Second Data Breaches.

In respect of the First Data Breach

8 On 28 November 2016, the Complainant was informed by another customer of the Organisation that when she accessed the Shipping Webpage, it displayed the Complainant's name, contact number, address and shipping details.

9 This was the first time that such an error had been reported to the Organisation; further, the Organisation was unable to reproduce the error. It had subsequently conducted tests and investigations to determine the cause of the First Data Breach, but was unable to determine conclusively the root cause because:

(a) tests conducted on the components of the Website responsible for generating unique Shipment IDs confirmed that these components were functioning properly and that each shipment / transaction record had been assigned a unique identifier;

(b) a review of the code used on the Website did not uncover any coding issues or deficiencies that could have caused the breach;

(c) there were no known session variable management issues associated with the Apache Tomcat software that the Organisation was using;

(d) a review and analysis of log files relating to the First Data Breach revealed that there was no session corruption that could have caused the breach; and

(e) attempts to reproduce or replicate the breach in the production environment of the Website, e.g. by generating multiple transactions in the same minute, were not successful.

10 Even though the root cause of the First Data Breach could not be determined, the Organisation has since taken the following remediation steps:

(a) removing all personal data from the Shipping Webpage such that even if the wrong Shipping Webpage was sent to a customer, no personal data will be included in the shipping details; and

(b) implementing a logging function that creates a log entry whenever a session variable mismatch occurred, which would provide the Organisation with diagnostic data.

In respect of the Second Data Breach

11 The complaint relating to the Second Data Breach is of a different nature. Unlike the First Data Breach, the Second Data Breach concerns the Shipping Webpage and how its Uniform Resource Locator ("**URL**") could be manipulated to enable access to the shipping and personal details of the Organisation's customers. The URL for the Shipping Webpage is sent by email to the Organisation's customers.

12 Each of these URLs would take the following form: e.g. <www.comgateway.com/ship_track_detail?shipId=MTYwMTExMQ>, which comprises the host information (i.e. www.comgateway.com), the path information (i.e. ship_track_detail?), and most importantly a unique query string that is associated with the particular shipment to which the URL concerns (i.e. shipId=MTYwMTExMQ).

13 The Website allocates a unique Shipment ID for each shipment. The unique query string of the URL for the Shipping Webpage is formed by encoding the Shipment ID in Base64 (a binary to text encoding scheme). In the example above, the query string "MTYwMTExMQ", is encoded from the Shipment ID "1601111".

14 As will be explained below, this format of URL string made it possible for anyone to gain access to a customer's Shipping Webpage by taking a URL and systematically changing the last character of the URL until, through trial and error, a workable link is derived.

15 After receiving notice of the complaint, the Organisation has since addressed this vulnerability by adding another unique variable to the URL of the Shipping Webpage to prevent manipulation.

Findings and Basis for Determination

Issues to be determined

16 The shipping details that were compromised had comprised of names, contact numbers and addresses of individuals. These were "personal data" as defined under the PDPA.

17 Section 24 of the PDPA requires an organisation to protect personal data in its possession or under its control by taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

18 The issues in the present case are:

(a) in respect of the First Data Breach, whether the Organisation had breached Section 24 of the PDPA when the Complainant's personal data was rendered accessible to another customer of the Organisation in the manner described in paragraph 8 above; and

(b) in respect of the Second Data Breach, whether the Organisation had breached Section 24 of the PDPA when personal data of other customers of the Organisation was rendered vulnerable and accessible through the manipulation of the URL of the Shipping Webpage in the manner described in paragraphs 11 to 14 above.

In respect of the First Data Breach

19 The fact that personal data had been rendered accessible to an unauthorised party by an error or flaw in an organisation's systems and processes does not automatically mean that the organisation is liable under Section 24 of the PDPA for failing to take reasonable security arrangements to protect personal data.

20 In *Re Singapore Telecommunications Limited & another* [2017] SGPDPC 4, even though a coding issue in the database script of Singapore Telecommunications Limited's ("**SingTel**") ONEPASS electronic service had caused an individual's personal data to be revealed to other customers of SingTel, the Commissioner found that SingTel was not in breach of Section 24 of the PDPA because SingTel had put in place reasonable security arrangements to protect personal data, including:

(a) a contract requiring its IT service provider, Tech Mahindra, to comply with the PDPA and SingTel's access and security policies;

(b) operational procedures and checks to ensure that its service provider had carried out its functions to protect personal data; and

(c) conducting annual on-site security reviews and penetration tests as part of its governance process.

21 The position taken by the Commissioner in SingTel is also consistent with that taken by data protection authorities in other parts of the world:

(a) In *PIPEDA Report of Findings #2014-004*[2], the Office of the Privacy Commissioner of Canada ("**OPC**") found that an organisation had appropriate safeguards in place to protect personal information at the time of a data breach, even where an individual's personal information could have been accessed by a cyber-attacker. This finding was made after the OPC determined that the organisation had numerous technical safeguards in place at the time of the data breach aimed at preventing and detecting breaches, including (i) the use of firewalls, (ii) encryption of sensitive information, (iii) separate storage and obfuscation of encryption keys, and (iv) multiple intrusion detection systems (through which the breach was detected). The effectiveness of these safeguards was also independently evaluated on a regular basis through external vulnerability scans and audits.

---

2 OPC, *PIPEDA Report of Findings #2014-004* (23 April 2014) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-004/>.

(b) In *Sony PlayStation Network / Qriocity: Own Motion Investigation Report*[3], the Office of the Australian Information Commissioner ("**OAIC**") investigated Sony Computer Entertainment Australia Pty Ltd and its related companies ("**Sony**") following reports of unauthorised access to personal information of Sony's customers on the Sony PlayStation / Qriocity Network. Upon investigation, the OAIC determined that Sony had taken reasonable steps to protect information on its network at the time of the data breach because Sony had a range of security safeguards in place to protect the personal information held, including (i) physical, network and communication security measures to protect the information collected and stored in the network, (ii) encryption of credit card information, and (iii) internal information technology security standards that are based on the ISO standards for international information security.

22 In the present case and in relation to the First Data Breach, the fact that the cause of the data breach could not be established or that it was possibly a rare computer glitch did not absolve the Organisation of liability under Section 24 of the PDPA. The Organisation must show that it had taken reasonable steps to protect personal data held in its possession and/or control. In this regard, the Commissioner is satisfied that the Organisation had, indeed, made reasonable security arrangements to protect personal data from unauthorised access. By virtue of the Organisation's IT system undergoing regular and rigorous IT security tests and scans on the system as described at paragraphs 6 and 7 above, and that the IT system had successfully passed all those tests and scans, this was

---

3 OAIC, *Sony PlayStation Network/Qriocity: Own Motion Investigation Report* (29 September 2011) <https://www.oaic.gov.au/privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity>.

a sufficient indication that the Organisation's IT security measures in place were adequate. Additionally, in respect of the First Data Breach, there was no evidence of any issues with the Website functions or services, which would affect the protection of the personal data held on the Website. This case appears to have given rise to an anomalous data breach that could not be replicated.

23 Accordingly, the Commissioner finds that the Organisation has not contravened Section 24 of the PDPA in relation to the First Data Breach.

24 As mentioned above, the Organisation has since removed all personal data from its Shipping Webpages, such that even if the same glitch were to recur, there would not be unauthorised access to personal data. While it is the prerogative of the organisation to take such steps, the Commissioner does not advocate the removal of personal data purely as a risk avoidance measure if the removal detracts from the usability of the Organisation's Website. Such steps would in the Commissioner's view be excessive and unnecessary, especially if there are other reasonable technical or operational means to achieve the objective of protecting personal data.

In respect of the Second Data Breach

25 In relation to the Second Data Breach, the Commissioner had found that the URL of the Organisation's Shipping Webpages was susceptible to manipulation.

26 From 2 July 2014 (the Appointed Day when the data protection obligations of the PDPA came into effect) until the Organisation instituted the measures described in paragraph 15 above, about 108,085 customers had made shipments via the Organisation. In this regard, the security of the personal data

of those customers (contained in the Shipping Webpages) were vulnerable to unauthorised access and could have been compromised.

27 As mentioned at paragraph 13 above, the URL of the Shipping Webpage is unique to each customer by virtue of a unique identifier (i.e. the Shipment ID encoded in Base64) at the end of the URL string. While seemingly a random string of alphabets (in upper / lowercase), encoding a Shipment ID using Base64 is not an actual means of encryption. Base64 is a common and simple encoding scheme for ensuring that only basic and printable characters are used, and to avoid reserved characters which may have special meanings. Simply put, Base64 is a means of translating the Shipment ID of "1601111" from Arabic numerals, to another language more suitable for use in URLs. Any item encoded in Base64 can be easily decoded through publicly available decoding tools.

28 A person with IT knowledge would be able to recognise that the Shipment ID in the query string was encoded in Base64. Upon decoding the query string, it would also be readily observable or deducible that the Shipment ID is simply a function of the date of shipment and its sequence. With this information, one could reverse engineer and generate valid URLs of the Shipping Webpages of the Organisation's customers or even run a script to harvest personal data from such Shipping Webpages. Even an ordinary user could systematically replace the last character of the URL of a provided Shipping Webpage to arrive at valid URLs of Shipping Webpages of the Organisation's customers, which could then be accessed for the shipping details and personal data of those customers.

29 A test conducted on the query string showed that the URL of the Shipping Webpage could be easily manipulated to obtain a valid URL of the

Shipping Webpage of another Shipment ID.[4] During the test, it was discovered that by sequentially replacing the last character of the encoded Shipment ID from A-Z (including both capital and small letters) and 0-9, it was possible to derive 3 other valid URLs.

30 The Organisation also did not place limits or restrict access to the URLs so that only a specific customer of the Organisation has access to his own shipping details. Anyone could access the URL of a Shipping Webpage and the personal data contained therein without needing to authenticate or to furnish information to verify the identity of the person that was accessing the URL. This allowed for another customer or even an outsider to have access to the customer's shipping details.

31 The personal data held on the Shipping Webpage was, therefore, not secured from unauthorised access online. The ease of manipulation of the URL of the Shipping Webpage to derive the URL of other Shipping Webpages, and the absence of any other security or access-control measures to protect the Shipping Webpages, taken together, meant that personal data on the Shipping Webpages could be easily accessed by any person. Such a person could gain access to the personal data held on the Shipping Webpages, whether or not the person was a "motivated intruder" who had sought to gain unauthorised access to personal data of other individuals, or a person who had accidentally typed in an incorrect query string into the URL address bar.

---

[4] The vulnerable URL portion, e.g. MTYwMTExMQ, when decoded, is 1601111. This string of numbers consists of the date (yy/mm/dd) and the sequence of the shipment for that date. By changing the last character to small letter "a" to "f", the decoded results are 1601111; changing to "g" to "v" yielded 1601112; and changing to "w" to "z" resulted in 1601113.

32 In the response provided by the Organisation, the Organisation admits that at the time of design and implementation of the Website and Shipping Webpage, they had not considered the susceptibility of the Shipping Webpage URL to manipulation and had, therefore, not taken any step to test or address this vulnerability.

33 Given the absence of any security arrangements to protect personal data against such unauthorised access, the Commissioner finds that the Organisation has contravened Section 24 of the PDPA in relation to the Second Data Breach.

34 Although the Organisation had in place security arrangements (described in paragraphs 6 and 7 above) to protect personal data on its Website, including regular vulnerability scans, penetration tests, risks assessments and automated code reviews; none of these arrangements, as the Organisation admits, addresses the URL manipulation vulnerability. Hence, they would not assist the Organisation in avoiding liability under Section 24 of the PDPA in respect of the Second Data Breach.

35 This is not the first case where the Commissioner has found a failure to make reasonable security arrangements to protect URLs from being easily manipulated to compromise the security of personal data, to be a contravention of Section 24 of the PDPA:

(a) In *Re Fu Kwee Kitchen Catering Services and another* [2016] SGPDPC 14, the URL of Fu Kwee Kitchen Catering Services' ("**Fu Kwee**") webpage for previewing orders could be manipulated easily (by changing the characters at the end of URL) to retrieve other orders of Fu Kwee's customers containing the customers' personal data. The Commission found Fu Kwee in breach of Section 24 of the PDPA for

failing to implement reasonable security arrangements to protect personal data.

(b) In *Re Smiling Orchid (S) Pte Ltd and others* [2016] SGPDPC 19, the URL of Smiling Orchid (S) Pte Ltd's ("**Smiling Orchid**") webpage for previewing orders could be manipulated easily (by changing the characters at the end of URL) to retrieve other orders of Smiling Orchid's customers containing the customers' personal data. The Commission found Smiling Orchid in breach of Section 24 of the PDPA for failing to implement reasonable security arrangements to protect personal data.

Directions

36 Given the Commissioner's findings that the Organisation is in breach of its obligations under Section 24 of the PDPA in respect of the Second Data Breach, the Commissioner is empowered under section 29 of the PDPA to issue the Organisation such directions as it deems fit to ensure compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million.

37 In assessing the breach and determining the directions (if any) to be made, the Commissioner considered the following factors:

(a) the Organisation handles a substantial volume of shipping transactions for individual customers in Singapore and hence a substantial amount of personal data. It is therefore imperative that security arrangements be implemented to protect personal data of its customers;

(b) the Organisation had cooperated fully with the Commissioner's investigations, including undertaking technical and security testing to determine the cause of the breaches;

(c) the Organisation took prompt action (described in paragraph 15) to remedy the breach when notified by the Commissioner; and

(d) the Organisation had been conducting regular penetration tests, vulnerability tests and code reviews to guard against online security threats.

38 In view of the factors noted above, pursuant to section 29(2) of the PDPA, the Commissioner hereby directs that the Organisation pay a financial penalty of S$10,000 within 30 days of the Commissioner's direction.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION