# Singapore Telecommunications Limited

## [2019] SGPDPC 49

Yeong Zee Kin, Deputy Commissioner — Case No DP-1802-B1732

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

31 December 2019

### Introduction

1 On 21 February 2018, the Personal Data Protection Commission (the "**Commission**") received a complaint from an individual mobile subscriber of Singapore Telecommunications Limited (the "**Organisation**") asserting that when the subscriber accessed account details using the Organistion's "MySingTel" mobile application (the "**App**"), the subscriber was able to view the personal information of another subscriber.

### Facts of the Case

2 The Commission's investigations revealed that due to a technical issue that occurred during a limited period, certain mobile subscribers of the Organisation were able to view the personal data of other subscribers when they used the App (the "**Incident**"). The Incident took place over a period of approximately 11 hours on 20 February 2018 and the personal data of 750 subscribers (the "**Affected Subscribers**") were exposed to the risk of access by other subscribers. Of these, the personal data of 39 subscribers were, in fact, accessed by other subscribers. The specific cause of this incident is described below.

3 The Incident arose during the Organisation's migration of its database of mobile customer accounts from its existing billing system (the "**Existing System**") to a new billing system (the "**New System**"). [Redacted].

4 However, an issue arose when there was a mobile number previously assigned to a subscriber ("**historical numbers**") that was subsequently reassigned to another subscriber. One situation in which this happened was when a subscriber ported over an existing mobile number from another mobile telephone operator to the Organisation. In order to effect the porting over, the Organisation would first issue the subscriber with a temporary mobile phone number (this is referred to as a "**dummy number**") as part of the overall porting mechanism. After the subscriber's existing mobile telephone number had been successfully ported over to the Organisation, the dummy number will cease to be linked to the subscriber [redacted].

5 [Redacted].

6 During the migration period, when a subscriber logged in to the App, the App would query the Organisation's Master Routing Database ("**MRD**") to check if the subscriber's data had been migrated and then route the query to the relevant billing system. On 20 February 2018, due to slow response times, queries by MRD to the Existing System encountered timeouts. When these timeouts occurred, even if the subscriber had been migrated to the New System, the query would by default be routed to the Existing System. If the subscriber had a historical number, such as a dummy number [redacted], [in certain circumstances] the service information associated with *both* the current mobile number and the historical number would be retrieved and made available to the subscriber. The service information of the historical number could be viewed by clicking on the mobile number and information bar. If the historical number had been reassigned to an Affected Subscriber, the service information of the Affected Subscriber would have been retrieved and made available to, and therefore at risk of access by, the subscriber. In this way, the associated information of the 39 subscribers were accessed during the timeouts.

7 The types of personal information of the Affected Subscribers (the "**Personal Data**") which were accessible through the App included:

(a) mobile numbers;

(b) mobile plans subscribed to;

(c) usage details;

(d) account numbers; and

(e) add-on services subscribed to. The relevant subscribers[1] could also modify the add-on services tied to the Affected Subscribers' mobile number; 6 such subscribers had tried to make such modifications.

8 Upon being notified by the Commission, the Organisation ensured that migrated Subscribers who encountered timeouts when using the App were shown an error message, and performed testing to verify that this was the case.

**Findings and Basis for Determination**

9 Section 24 of the Personal Data Protection Act 2012 (the "**PDPA**") requires an organisation to 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.

*Whether the Organisation Complied with Section 24*

10 With respect to the design of the MRD, the Organisation asserted that it did not intend for the MRD to route queries to the Existing System in the event of a timeout, and that the Organisation's intentions was for an error message to be displayed instead. I give the Organisation the benefit of doubt and accept its assertion. Since the intention was to display an error message, this ought to have been included as a scenario for user testing. Consequently, this Incident was caused by the following lapses on the Organisation's part:

(a) The Organisation had not carried out more thoroughly scoped tests to firstly ensure that dummy numbers in these circumstances did not produce any unintended effects; and

(b) the test plan should have anticipated likely scenarios, such as session time-out.

11 If these had been done, the Organisation could have discovered the potential erroneous

retrieval and unauthorised disclosure of the Affected Subscribers' Personal Data for such accounts, and consequently, implemented measures to prevent the Incident from occurring. In view of the above, I found the Organisation in breach of section 24 of the PDPA.

12 The Organisation in its representations made the point that, in their view, the data breach "happened only where there was an obscure combination of factors". While, it is accepted that a combination of events had to occur before personal data would have been disclosed, I do not think that the combination of factors was obscure. First, session timeout for MRD queries was foreseen, with the intention for an error message to be displayed. Second, the Organisation had full knowledge of how dummy numbers are assigned as a temporary bridge for number porting, and that these dummy numbers are eventually re-assigned. The combination of factors giving rise to the Incident was foreseeable and I do not think that the combination is obscure. The impact of the Incident was contained because of its prompt action in implementing a temporary fix.

**The Deputy Commissioner's Directions**

13 In determining the directions to be imposed on the Organisation under section 29 of the PDPA, I took into account the following mitigating factors:

(a) the Organisation was cooperative during the investigations;

(b) the Organisation took prompt action to mitigate the impact of the Incident by implementing a temporary fix within 11 hours; and

(c) although the Personal Data of 750 individuals were at risk, only 39 of such individuals' Personal Data were subject to unauthorised disclosure.

14 Having carefully considered all the relevant factors of this case, I hereby direct the Organisation to pay a financial penalty of $9,000 within 30 days from the date of the directions, failing which interest at the rate specified in the Rules of Court in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

15 As the Organisation had completed its migration on 19 August 2018 and there are no

further risks to the Personal Data arising from the retrieval of Subscriber information from the Organisation's Existing System, I have assessed that the remedial actions set out at [8] had sufficiently addressed the risks to the Personal Data arising from the Incident. I have therefore not made further directions for the Organisation.

---