IN RE: SMART COMMUNICATIONS, INC. NPC BN 18-142

x----------x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is a confidentiality breach concerning the disclosure of the names and e-mail addresses of tourists who registered for a free LTE Subscriber Identity Module (SIM) card from SMART Communications, Inc. (SMART).

Facts

On 29 July 2018, SMART received an email from JS, a tourist visiting the Philippines.[1] He informed SMART that its registration platform (Google Forms) where tourists register for a free LTE Tourist SIM contained an option to view the "*summary of previous responses.*"[2] According to JS, through this option, registrants may view the earlier responses that indicate the names and e-mail addresses of SMART's prospective customers.[3]

SMART claimed that it immediately disabled and took down the functionality to view a summary of previous responses from the registration portal.[4] SMART also reported that its initial investigation showed that "no data exfiltration happened," and that "access to data may have been possible only by viewing the list on the screen."[5]

---

[1] Data Breach Notification – SMART LTE Tourist SIM Registration Matter, 01 August 2018, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

On 01 August 2018, SMART notified the National Privacy Commission (NPC) of the incident containing a narration of the remedial actions it took.[6]

On 24 April 2020, the NPC, through its Complaints and Investigation Division (CID), requested SMART to submit an updated breach notification report that includes the results of the investigation SMART conducted.[7]

On 15 November 2021, the CID, ordered SMART to submit a full report detailing the incident.[8]

On 03 December 2021, SMART submitted its Compliance in relation to the incident.[9]

According to SMART, it took the following measures to address the breach:

> 1. The settings of the Google Forms were reviewed and it was determined that the data breach could be resolved by removing the "see previous responses" option.
>
> . . .
>
> 2. The Company also conducted an inventory of other campaigns using Google forms to check that settings do not allow viewing of previous responses.
> 3. A refresher course on data privacy was conducted among members of the Marketing Operations team.
> 4. Disciplinary proceedings were also initiated for employees responsible for the error in the Google Forms settings.
> 5. As a long term remediation, Smart no longer uses Google Forms for campaigns requiring data submission (such as registration or surveys) from participants/customers. The Company uses Office 365 and requires previous clearance from our Cyber Security Operations Group.[10]

---

[6] *Id.*
[7] Order, 24 April 2020, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2020).
[8] Order, 15 November 2021, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[9] Compliance to Order dated 15 November 2021, 01 December 2021, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[10] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

SMART also reported that the incident concerned a total number of "three thousand tree hundred thirty-five (3535) [sic] affected data subjects, broken down as follows: (a) 3123 responses for the English Google Forms, (b) 153 responses for the Japanese Google Forms, (c) 100 responses for the Korean Google Forms, and (d) 69 responses for the Chinese Google Forms."[11] SMART revealed that it also addressed the settings for the Google Forms in other languages including Korean, Chinese, and Japanese.[12]

On 23 December 2021, the CID ordered SMART to submit a Post-Breach Report containing the proper documentation on the actions SMART has taken.[13]

On 11 January 2022, SMART submitted its Post-Breach Report in compliance with the directive dated 23 December 2021.[14] It attached proofs on the following: (1) how the data exposed were presented to those who will click the "*view summary of previous responses*" functionality, (2) that the information exposed were only names and email addresses, and (3) that no sensitive personal information was disclosed during the incident, (4) that SMART already uses Office 365 instead of Google forms in collecting data from customers requiring data submission and that the clearance from its Cyber Security Operations Group is required prior to collection.[15]

On 26 October 2022, the Commission ordered SMART to submit the Full Breach Report.[16]

On 11 November 2022, SMART submitted its compliance to the 26 October 2022 Order reiterating its own submissions in response to the previous Orders. [17]

---

[11] *Id.* Annex A.
[12] *Id.*
[13] Order, 23 December 2021, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[14] Compliance to Order dated 23 December 2021, 11 January 2022, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2022).
[15] *Id.* Annex A-D.
[16] Order (To Submit Full-Breach Report), 26 October 2022, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2022).
[17] Compliance, 11 November 2022, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2022).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Based on the CID's assessment dated 18 January 2023, the security measures adopted by SMART upon knowledge of the incident are sufficient to address the same and prevent or mitigate its recurrence.[18]

Issue

Whether SMART conducted proper breach management, including the implementation of reasonable and appropriate security measures.

Discussion

The Commission finds that SMART conducted proper breach management and implemented reasonable and appropriate security measures upon knowledge of the incident. Thus, the Commission resolves to close the case.

Section 20 (a) and (b) of the Data Privacy Act of 2012 (DPA) mandates a Personal Information Controller (PIC) to implement reasonable organizational, physical, and technical measures intended for the protection of personal information:

> Section. 20. *Security of Personal Information*. (a) **The personal information controller must implement reasonable and appropriate organizational, physical and technical measures** intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.
>
> (b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.[19]

---

[18] Final Breach Notification Evaluation Report, 18 January 2023, at 7, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2023).
[19] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (a) and (b) (2012). Emphasis supplied.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Further, SMART enumerated in its submissions the measures it took to address the breach following Section 17 (D) (3) of NPC Circular 16-03 (Personal Data Breach Management):

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification*. The notification shall include, but not be limited to:
>
> 3. Measures Taken to Address the Breach
>
> a. description of the measures taken or proposed to be taken to address the breach;
> b. actions being taken to secure or recover the personal data that were compromised;
> c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
> d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
> e. the measures being taken to prevent a recurrence of the incident.[20]

As an immediate response, it disabled the option in the Google Forms to prevent a recurrence of the same incident.[21] Additionally, SMART informed that it corrected the settings for Google Forms for the other languages.[22]

To immediately address possible concerns on the unintended disclosure, SMART also established an *ad hoc* team to monitor complaints from registered users that could have resulted from this incident.[23]

---

[20] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §17 (D) (3) (15 December 2016).
[21] Data Breach Notification – SMART LTE Tourist SIM Registration Matter, 01 August 2018, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2018).
[22] Compliance to Order dated 15 November 2021, 01 December 2021, Annex A (Full Report), *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[23] Data Breach Notification – SMART LTE Tourist SIM Registration Matter, 01 August 2018, at 1, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2018).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

According to SMART, it reviewed its campaigns that also used Google Forms to determine if its registration settings would still allow previous responses to be viewed by other users.[24]

As an organizational measure, SMART conducted a data privacy refresher course among the members of its Marketing Operations Team.[25] Similarly, SMART conducted annual data privacy e-learning courses for its employees.[26]

SMART also initiated disciplinary proceedings for the employees responsible for the error in setting up the Google Form that led to the incident.[27] SMART reported in its Post-Breach Report that the erring employee is no longer with SMART.[28]

As a technical measure, SMART conveyed that it transitioned from Google Forms to Office 365 for their future campaigns requiring data submission from participants or customers.[29] It averred that the latter platform requires previous clearance from its Cyber Security Operations Group prior to collection of data.[30] As proof of such, SMART attached an excerpt of its manual entitled "Company's Work Tools Security Standards" and "Company's Information Security Compliance Management Standards."[31] The manual specifically prohibited the use of public cloud-based services such as Google Drive and implemented the rule that all confidential information should be saved in the company-provided cloud storage.[32]

SMART also reported that its Marketing Team also implemented tracking and analytics on the website to enable tracking of views and

---

[24] Compliance to Order dated 15 November 2021, 1 December 2021, Annex A (Full Report), *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Compliance to the Order dated 23 December 2021, 11 January 2022, at 2, *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[29] Compliance to Order dated 15 November 2021, 1 December 2021, Annex A (Full Report), *in* In re: Smart Communications, Inc., NPC BN 18-142 (NPC 2021).
[30] *Id.*
[31] *Id.*
[32] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

downloads.[33] According to SMART, this will enable detection from the logs of views and downloads of information posted on their website.[34]

Based on the foregoing, the Commission finds that SMART as a PIC took sufficient steps to address the incident and mitigate any negative effects, if any. SMART implemented reasonable and appropriate organizational and technical measures to protect the personal data of its data subjects.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-142 In re: SMART Communications, Inc. is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
30 March 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

---

[33] *Id.*
[34] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Copy furnished:

LBJ
Chief Data Privacy Officer
Smart Communications, Inc.

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228