Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: TUITT PHILIPIINES, INC. **NPC BN NO. 17-038**

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

RESOLUTION

NAGA, D.P.C.:

This Order refers to a Security Incident Report submitted by Tuitt Philippines dated 21 November 2017 and the Full Breach Report dated 26 July 2019, involving a security incident that may have exposed its WIFI network to unauthorized persons.

The Facts

On 19 November 2017, during a meetup event, Tuitt became aware of a potential security incident when the WIFI login credentials of their training laboratory's network were shared by a staff member with the event participants.

On 21 November 2017, the Data Protection Officer (DPO) of Tuitt submitted to the Commission a Security Incident Report[1] via email detailing that the unauthorized disclosure of WIFI login credentials may have compromised their network's security and the information of data subjects who accessed their machines through the same network. Tuitt also described in the Incident Report the measures they implemented to address the incident.

[1]Security Incident Report dated 21 November 2017.

On 08 July 2019, the Commission, through the Complaints and Investigation Division (CID), informed Tuitt the initial report they submitted did not comply with the reportorial requirements provided under NPC Circular 16-03. TPI was then required to submit a Full Breach Report in accordance with said Circular.

On 26 July 2019, Tuitt submitted its Full Breach Report. In the Report, Tuitt claimed that upon review of the incident that occurred on 19 November 2017, such was not a personal data breach as initially reported, but a security incident. Tuitt based its assertion that the nature of the incident did not fit the definition of a personal data breach as defined in the same Circular considering that the network that was accessed contains no personal data.

Discussion

This Commission deems the incident as a Security Incident since it only affected the data protection aspect of Tuitt system and does not involve personal data. Section 3 (F) of the NPC Circular provides:

> "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:
>
> 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
> 2. Integrity breach resulting from alteration of personal data; and/or
> 3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.
>
> xxx
>
> "Security incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include

> incidents that would result to a personal data breach, if not for safeguards that have been put in place.

Tuitt stated on their Full Breach Report[2] (Report) that they store personal information and sensitive personal information on secure cloud servers (AWS), and not on the training laboratory's network which was the subject of the incident. Upon review of the incident, Tuitt stated that the lab network where any of their data subjects' information are stored is isolated from the rest of their staff's network which reduced the potential risk of any form of data breach.[3] Therefore, no personal data breach occurred.

This Commission emphasizes that for an incident to be considered a personal data breach it must involve unlawful loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed, among other factors defined under Section 3 (F) of the NPC Circular 16-03. The aforementioned factors were not present in this case. Thus, the incident does not fall under personal data breach.

However, as correctly pointed out by Tuitt, the unauthorized disclosure of the WIFI login credentials shall be treated as a Security Incident since it may affect data protection, including the availability, integrity, and confidentiality of personal data. Further, the distinction between the two is that a security incident may result to a personal data breach if not for the safeguards in place implemented by the Personal Information Controllers (PICs).

In terms of the measures implemented by Tuitt to address the incident, they stated that the network passwords were changed, and the machines have been reformatted. Tuitt issued a Standard Operating Procedure (SOP) to the staffs who interact with the lab daily which includes the prohibition of sharing any WIFI credentials to non-staff personnel. Also, Tuitt white-listed all authorized machines where access is denied to other unauthorized devices.[4]

---

[2]Full Breach Report dated 26 July 2019.
[3]Ibid. At p. 2.
[4] Ibid. At p. 3.

However, the Commission finds that there was no proof submitted showing the measures implemented by Tuitt to address the incident as mentioned in their Report. Although the incident is considered a Security Incident, it is part of the PICs obligation to provide proof of the security measures they have implemented to address the incident along with their Report.

Further, the PICs also have the responsibility to implement policies and procedures in managing security incidents under Section 4 of the NPC Circular 16-03 which provides, *viz*:

> **SECTION 4.** ***Security Incident Management Policy***. A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:
>
> A. Creation of a data breach response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
>
> B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
>
> C. Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
>
> D. Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
>
> E. Compliance with the Act, its IRR, and all related issuances by the Commission pertaining to personal data breach notification.

This Commission highlights that the submission of the proof of the security measures implemented by Tuitt and their Security Incident Management Policy is necessary in order for the Commission to ensure and confirm that the security measures

implemented are sufficient to prevent the security incident in resulting to personal data breach.

WHEREFORE, premises considered, the Commission hereby **ORDER** Tuitt Philippines, Inc. to comply with the following within fifteen (15) days upon receipt of this Order:

(1) **SUBMIT** the proof of the security measures they have implemented as stated in their Full Breach Report dated 26 July 2019; and

(2) **SUBMIT** their Security Incident Management Policy pursuant to Section 4 of the NPC Circular 16-03.

SO ORDERED.

Pasay City, Philippines;
18 March 2021.

Sgd.

JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

AGCA
Data Protection Officer (Acting)
Tuitt Philippines, Inc.

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