Republic of the Philippines
NATIONAL PRIVACY COMMISSION

JCR

Complainant,

-versus-

NPC Case No. 17 - K - 001
For: Violation of the provisions of the Data Privacy Act of 2012

GLOBE TELECOM, INC.

Respondent.

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

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by Complainant JCR against Respondent Globe Telecom, Inc. for supposed violations of R.A. 10173 ("Data Privacy Act").

The Facts

The facts of this case are not disputed.

On 03 November 2017, Complainant accidentally left her phone containing her Globe Subscriber Identity Module ("SIM") card in a taxi on her way to Makati. Her mobile number with Respondent served as her principal means of communication since its issuance. The next day, she went to Respondent's store in Greenbelt 3, Makati to request the deactivation of her lost SIM card and the issuance of a new SIM card with the same mobile number. An employee of Respondent named MCK assisted Complainant. She was given a blank inactive SIM card but they were unable to process the request. Complainant left her sister's mobile number so Respondent can communicate any development regarding her request.

After a couple of days, Complainant went home to Bacolod City without knowing whether her lost SIM card could be replaced or not. On 06 November 2017, MCK called Complainant's sister informing her that there was still no resolution regarding her request because

Respondent was still fixing the issue with her lost SIM card. Complainant went to the Respondent's store in SM Bacolod to check if her request was addressed. No update was given to her even after calling the hotline of Respondent.

On 10 November 2017, Complainant came back to the same store in SM Bacolod. The employee attending her request told her that the pendency of an incomplete/unspecific previous cancellation request on her account prevented any subsequent transaction on her account from pushing through. She was told to keep the blank SIM card she previously received and try to call the hotline to have it activated instead. On 11 November 2017, Complainant called Respondent's hotline. The agent who answered her said that Respondent's store in SM Bacolod could do nothing unless she returns to the Respondent's store in Greenbelt 3.

Thereafter, Complainant's sister went to Respondent's store in Greenbelt 3, but MCK was on leave and none of the agents could help her. Complainant then called to inquire how she can file a complaint and was referred to the supervisor. After waiting for more than twenty minutes over the phone, Complainant was told that her problem had been fixed and that she just needed to go back to the Respondent's store in SM Bacolod and look for the branch manager or assistant manager so she can get her SIM card replaced. On the same day, Complainant went back only to find that the personnel she was asked to look for were both not on duty on that day. The officer in charge asked for another 24 to 48 hours to once again try to address her concern.

After two weeks, Complainant inquired again about the status of her cancellation request because she did not receive any feedback for almost a week. However, there was still no resolution to her concern.

Arguments of the Parties

On 20 November 2017, Complainant filed her Complaint-Affidavit of even date before this Commission. According to her, she was worried about the integrity of her data and privacy because her primary means of communication and the repository of her personal data for six (6) years is now left uncertain in the hands of a stranger.

Complainant alleges that "the inability of Globe to deactivate my lost Globe SIM, re-issue the same and restore my possession of my Globe

number that belonged to me for the past six (6) years, qualify as a breach of its obligations under Republic Act No. 10173 or the Data Privacy Act of 2012 and its Implementing Rules and Regulations."[1]

Complainant further alleges that Respondent violated Sections 25 and 28(d) of the Implementing Rules and Regulations ("IRR") of the Data Privacy Act of 2012 for failure to implement reasonable and appropriate security measures to protect the availability, integrity and confidentiality of her personal data.

For their part, Respondent argues in their Comment[2] dated 28 August 2018 that there are no violations of the Data Privacy Act alleged in the Complaint. According to Respondent, the facts in the complaint discussed matters relating to a SIM replacement issue and/or customer service issue which was resolved when the replacement SIM card was issued to Complainant on 21 March 2018. As such, these are beyond the jurisdiction of this Commission.

Respondent also contends that there was no allegation that Respondent disclosed or caused the disclosure of Complainant's personal information. There is neither a privacy violation nor a personal data breach involved. Respondent argues that Complainant failed to state the alleged compromised or breached personal data. It explained that a SIM card does not store information or data. It is only a microchip inserted in a mobile phone that connects to a particular cellular network. It is the phone, not the SIM card, that stores information or data. The access to the data in the lost mobile phone may be gained with or without the SIM card except if the phone is protected or encrypted.

In addition, Respondent argues that the proximate cause of the alleged breach of complainant's data privacy, if any, was her own negligence when she lost her mobile phone with the SIM card in a cab. They contend that it is physically impossible for Respondent to protect and control the data or information that their data subjects store in their mobile devices. It is also impossible for Respondent to prevent the unauthorized disclosure of the data stored in one's device when the owner himself did not put the necessary measures to protect the data or information stored in it. Respondent explained that the personal data of subscribers stored in their devices and/or SIM card, if applicable, are physically and legally beyond the protection required by law from PICs and/or PIPs. It is the duty of the complainant, as a

---

[1] *Records*, p. 5.
[2] *Ibid.* at pp. 29-38.

reasonable and diligent owner, to protect the contents of her mobile. Respondent cannot be liable for any unauthorized disclosure of information stored in complainant's device because it is physically and legally beyond the protection of Respondent.

Respondent stated that as personal information controller ("PIC") and personal information processor ("PIP"), it is only required to protect the collected personal information in its possession and not the personal information of the subscribers contained in the devices and SIMs that are in the actual possession of its subscribers.

Respondent alleges that it has complied with the requirements under the Data Privacy Act, as well as its IRR. Respondent implements reasonable and appropriate organizational, physical and technical security measures for the protection of personal data. Respondent, as required by law, implements security measure for the protection of all the collected personal information stored in its designated data centers from any form of natural or human dangers.

Issue

The issue to be resolved in this case is whether Respondent violated Sections 25 and 28(d) of the IRR of the Data Privacy Act for its delayed action on Complainant's request to deactivate her lost SIM Card and issue another one with the same number.

Discussion

At the outset it should be stressed that there is no question that complainant's own negligence in leaving her mobile phone in the taxi was the proximate cause of her personal data being exposed to risks arising from possible unauthorized access and disclosure.

Respondent is therefore justified when it stated in its Comment that:

> Inasmuch as it is physically impossible for Globe, or this Honorable Commission despite repeated information campaign and reminder how to protect a person's personal information, to control the data or information that a subscriber stored in his mobile device, it is likewise to [sic] physically impossible for Globe, much less the Honorable Commission, to protect and/or prevent the unauthorized disclosure of data/information stored in such mobile device when owner thereof himself has not put the necessary measures to protect such data/information himself.[3]

---

[3] *Ibid* at p. 35.

Nevertheless, it is apparent that Respondent is only concerned with the personal data of Complainant stored in her mobile phone. As it explained in its Comment:

> … Respondent could only surmise that the "data" that she seeks to protect, which she claims to be in "the hands of a stranger whose intentions are demonstratively tainted" – refers to the data that are stored in her lost mobile phone – NOT in the Respondent SIM card. A SIM card is a microchip inserted in a mobile phone that connects it to a particular phone network – in this case to Globe's network. Clearly, a SIM it [sic] is not meant to be used to store information or data…[4]

In focusing only on the personal data stored in the mobile phone and characterizing the incident as a simple SIM card replacement and customer issue, Respondent ignores the very nature of Complainant's requests regarding the deactivation and reissuance of her SIM card and failed to take the necessary steps to protect the information stored in the SIM card that is associated with and used for the identification of the Complainant.

The United States of America's National Institute of Standards and Technology ("NIST") defined SIM cards as a removable smart card that "uniquely identifies the subscriber, determines the phone's number, and contains the algorithms needed to authenticate a subscriber to a network."[5]

While the SIM card itself does not contain the subscriber's mobile number, it contains, among others, the international mobile subscriber identity ("IMSI") number and integrated circuit card identifier ("ICCID")[6] that are used to uniquely identify the subscriber in the system of Respondent once it is activated. This allows that person to make and receive calls, send and receive SMS, use mobile data, and otherwise access and use the allocations of their account. Given this, in the same manner that a mobile number is considered personal information since it allows telecommunications companies such as Respondent to identify their subscribers, Complainant's activated SIM is also considered to contain personal information as far

---

[4] *Ibid.* at p. 32.
[5] Rick Ayers, et al., Cellphone Forensic Tools: An Overview and Analysis Update, NISTR 7387, United States of America National Institute of Standards and Technology, *available at* https://doi.org/10.6028/NIST.IR.7387, retrieved on 09 December 2019.
[6] *See* 3rd Generation Partnership Project: Technical Specification Group Terminals Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) Interface, 3GPP TS 11.11 v8.14.0 (2007-06) *available at* https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=419, retrieved on 09 December 2019.

as Respondent is considered and should therefore be protected in the same manner.

In its Comment, Respondent asserted that "the PIC and PIP could only implement reasonable and appropriate organizational, physical, procedural and technical security measures for the protection of personal data collected, and those that are within its control."[7] In this case, the deactivation of Complainant's SIM card to prevent further use and access by unauthorized persons is clearly within the control of Respondent especially since the matter had already been brought to its attention by Complainant several times.

Although the Complaint does not contain specific allegations relating to the misuse of Complainant's account, considering that the accidental loss of SIM cards is not an entirely uncommon occurrence, Respondent should have implemented the necessary mechanisms that will allow its data subjects, such as the complainant herein, to mitigate the potential damage resulting from their sim card being used by an unauthorized person.[8] This is all the more important given the risks that may result from a lost SIM card, ranging from unauthorized calls and texts being charged to the account of the subscriber to using the two-factor authentication codes sent to the mobile number, effectively allowing access the subscriber's accounts from social network accounts, bank accounts, and the like.

The fact that the proximate cause of these potential risks is the negligence of the complainant does not relieve Respondent of this obligation. After having been informed of the loss of Complainant's SIM card by complainant, the process for the deactivation of the SIM card was already entirely within the control of Respondent. Despite the diligent efforts Complainant took in following up her requests, her SIM card was only replaced on 21 March 2018 or more than four and a half months since the incident was first brought to the attention of Respondent on 04 November 2017.

While the records do not show the exact date when Complainant's old SIM card was deactivated, given the abovementioned risks, Respondent's inaction during the more than two weeks before the Complaint was filed is already too long. Respondent is reminded of its obligation to adopt and establish security measures that will allow it

---

[7] *Records*, p. 35.
[8] *See* Data Privacy Act, Sec. 20 (c)(3).

to "[take] preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach."[9]

For the reasons stated above, the Commission cannot agree with the Respondent that the issues raised regarding SIM card deactivation and replacement are merely in the nature of customer service.

Compliance with the Data Privacy Act entails more than simply ticking off boxes on a checklist such as the registration of a Data Protection Officer, conduct of a privacy impact assessment, creation of a data protection policy, or the exercise of breach reporting procedures. Companies must realize that compliance with the Data Privacy Act involves doing such activities within a framework of protecting the data subjects from very real risks, such as what Complainant faced in this case.

WHEREFORE, all the premises considered, the Commission finds no violation of the Data Privacy Act on the part of Respondent Globe Telecom, Inc. that is sufficient to warrant a recommendation for criminal prosecution. This Commission finds, however, that Respondent failed to adopt and implement the necessary policies and procedure relating to the prevention, correction, and mitigation against security incidents that can lead to a personal data breach.

The Commission hereby **ORDERS** Respondent Globe Telecom to submit a complete report on the measures it has undertaken or will undertake to address the issue of delayed SIM deactivation such as in this case, including the timeline for the implementation of such measures, within thirty (30) days from receipt of this Decision. Reference may be made to the requirements provided in the Implementing Rules and Regulations of the Data Privacy Act, particularly Section 28, paragraphs (c), (d), (e), and (f).

SO ORDERED.

Pasay City, 5 December 2019.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

---

[9] Implementing Rules and Regulations of DPA, Sec. 28 (d).

Concurring:

Sgd.	**Sgd.**
IVY D. PATDU	**RAYMUND ENRIQUEZ LIBORO**
Deputy Privacy Commissioner	*Privacy Commissioner*

COPY FURNISHED

JCR

CASTELO UNGOS CASIÑO & TUBAYAN
Counsel for Respondent Globe Telecom, Inc.

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission