Republic of the Philippines
NATIONAL PRIVACY COMMISSION

CBI,

Complainant,

-versus-

XXX,

Respondent.

CID 17-K-004
For: Violation of the Data Privacy Act

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

DECISION

NAGA, D.P.C.:

This Resolution refers to the Urgent Motion for Reconsideration[1] dated 09 December 2019 filed by Complainant CBI in relation to his complaint against XXX for alleged violation of R.A. 10173 (Data Privacy Act).

The Facts

On 29 November 2019, this Commission issued a Decision[2] with the following dispositive portion, to wit:

> **WHEREFORE,** premises considered, the Commission resolves that this case be **DISMISSED** for failure to substantiate and prove the allegations in the Complaint, without prejudice to any action that may be filed to other appropriate agencies or institutions. The Commission, however, **ORDERS** XXX to act on the request for correction which has not yet been addressed, and to provide assistance to complainant to ensure that he is able to exercise his rights as data subject in accordance with law.

On 20 August 2020, the Complainant received a letter[3] from this Commission's Enforcement Division instructing him within

[1] Urgent Motion for Reconsideration dated 9 December 2019
[2] Decision dated 29 November 2019
[3] Letter dated 20 August 2020

ten (10) days from receipt to provide the Respondent a copy of his Urgent Motion for Reconsideration and explanation as to why the said Motion for Reconsideration was not served to the Respondent in the first instance.

On 28 August 2020, the Complainant filed a Compliance and Explanation[4] report before this Commission stating that he has sent copies of his Urgent Motion for Reconsideration to the Respondent, however, since the latter changed their office address they did not receive a copy of the said document. Accordingly, the Complainant provided a copy of his Urgent Motion for Reconsideration to the Respondent and attached a proof of the same. On the same day, Respondent received the Complainant's Compliance and Explanation together with a copy of his Urgent Motion for Reconsideration.

On 14 September 2020, this Commission received the Respondent's Comment[5] to the Complainant's Urgent Motion for Reconsideration.

In the Urgent Motion for Reconsideration, the Complainant consistently argued that there is substantial evidence to show that the Respondent failed to set up, institute and implement the necessary, appropriate, adequate security measures required under the DPA which resulted in the unauthorized and illegal use of Complainant's credit card. According to Complainant, the fact that the One-time Password (OTP) was compromised shows the Respondent's failure to adopt and institute an effective, reliable, and industry compliant security measures.

The Complainant added that the burden of proof has shifted to the Respondent considering that the obligation of implementing reasonable and appropriate organizational, physical, and technical measures are mandated to all Personal Information Controllers (PICs) under the DPA and its Implementing Rules and Regulations (IRR), *viz*:

> "The material and relevant fact is that OTP was compromised as a result of respondent's failure to adopt and institute an

[4] Compliance and Explanation dated 26 August 2020
[5] Comment to Complainant's Urgent Motion for Reconsideration dated 4 September 2020

> effective, reliable, and industry compliant security measures. The onus and burden of proof has shifted upon the respondent to show and prove that it was negligent and that it had complied with the law."[6]

On the other hand, the Respondent argued in its Comment that the Complainant failed to present new and material factual or legal arguments to support his allegations. Respondent maintains that it instituted reasonable and appropriate organizational, physical, and technical measures. Further, according to the Respondent, the phishing incident was caused by the Complainant's gross and inexcusable negligence, *viz*:

> As consistently argued by Respondent XXX, assuming arguendo that the Complainant was a victim of phishing attack, this conclusively proves that he was the one who knowingly and voluntarily disclosed his personal and confidential information to an unknown person or group. Instead of ignoring or deleting the suspicious email, and reporting the same, he accessed the malicious link provided therein, and disclosed information which were supposed to be known only to him, to wit:
>
> a. 16-digit credit card number printed on the face of the Complainant's card;
> b. Expiry date printed on the face of the card;
> c. 3-digit CVC printed on the back of the card; and
> d. Username and password of his registered email address.

Further, Respondent stated that Complainant cannot feign ignorance to phishing attacks as the Bangko Sentral ng Pilipinas (BSP) had been warning the public against it, and for that reason Respondent have also been regularly sending phishing advisories to its clients' registered email addresses and mobile addresses, which are also circulated through their social media platforms and posted on their website. Respondent then concluded that there is no factual and legal basis to prove that they violated the Data Privacy Act or its IRR.

[6] Urgent Motion for Reconsideration dated 9 December 2019

With regard to the Complainant's request for correction, Respondent stated that they have sent an e-mail to the Complainant dated 04 September 2020 reiterating their position that the additional disputed transactions referred to in the 04 August 2017 Cardholder's Statement of Disputed Item Form are deemed valid and shall remain chargeable against the Complainant's account.

Issue

Considering the representations made by both parties, the remaining issue to resolve is whether or not the Respondent failed to institute reasonable and appropriate organizational, physical, and technical measures that led to the unauthorize access of the Complainant's credit card.

Discussion

The Motion for Reconsideration lacks merit.

Settled is the rule that the party who alleges a fact has the burden of proving it. Section 1, Rule 131, of the Revised Rules on Evidence provides the difference between burden of proof and burden of evidence, *to wit*:

> Section 1. Burden of proof and burden of evidence.- Burden of proof is the duty of a party to present evidence on the facts in issue necessary to establish his or her claim or defense by the amount of evidence required by law. **Burden of proof never shifts**.
>
> Burden of evidence is the duty of a party to **present evidence sufficient to establish or rebut a fact in issue to establish a *prima facie* case**. Burden of evidence may shift from one party to the other in the course of the proceedings, depending on the exigencies of the case. (Emphasis supplied)

Complainant is mistaken for stating that the burden of proof has shifted to the Respondent, as provided in long line of jurisprudence, and as adopted in the current Rules on Evidence,

burden of proof never shifts. Further, the burden of evidence is on the side of the Complainant considering that this Commission had already ruled in its 29 November 2019 Decision that the Respondent have provided substantial evidence that it was not negligent in employing security measures. The relevant portion states:

> In summary, XXX's continuous awareness campaign and its verification process, through the use of OTP, provides substantial evidence that it was not negligent in employing security measures. The claim of CBI that it was the negligence of XXX that caused the phishing of his personal information is not meritorious.

The Complainant then must overcome the evidence presented by the Respondent that it had employed reasonable and appropriate organizational, physical, and technical measures. Specifically, the Complainant must show with substantial proof the causal link between the lack of reasonable and appropriate security measures of the Respondent and the phishing attack against him. In this case, the Complainant failed to do so.

The fact remains that the Respondent implemented adequate security measures including adopting dynamic consumer awareness program through the conduct of regular awareness campaigns against phishing by sending advisories to its clients' registered email addresses, mobile numbers and other platform circulations. Further, as an additional security measure against unauthorized access, Respondent enabled a multi-factor authentication for their online payments through the implementation of One-Time Password (OTP) to ensure the access or purchase is confirmed by the owner through his e-mail.

The aforementioned security measures are deemed sufficient to protect its data subjects from harm such as phishing and further proves that it is not negligent in instituting adequate security measures, as established in the earlier Decision[7] of this Commission. The allegations and suppositions in the Motion for Reconsideration failed to rebut these established findings. Further, security of personal information is a joint obligation of both the data subjects

[7] Decision dated 29 November 2019

and data controller or processor. Implementation of a "reasonable" security measure does not mean that the measure is a foolproof for any contributory negligence on the part of the data subject. Thus, this Commission sustains its 29 November 2019 ruling on the issue.

However, while Respondent proved that it has implemented sufficient security measures, this Commission notes that Respondent's inaction towards the Complainant's second request for correction has been excessively long. The order for Respondent to act on the Complainant's second request for correction was indicated in the 29 November 2019 Decision and was reiterated in the 18 June 2020 Resolution. This Commission then reminds the Respondent of its obligation to adopt and establish security measures that will allow it to "[take] preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach."[8]

Moreover, this Commission reiterates that the compliance to the Data Privacy Act is not only confined to general procedures such as registration of Data Protection Officers (DPO), conduct of privacy impact assessment, creation of data protection policy, or the exercise of breach reporting procedures, but also warrants PICs to act within a framework of amplifying the protection of the data subjects rights as aptly provided in the DPA.

WHEREFORE, premises considered, this Commission hereby **DENIES** Complainant CBI's Urgent Motion for Reconsideration. Furthermore, the case of CBI vs. XXX is hereby considered **CLOSED**. Furthermore, XXX is **ORDERED** to submit **within thirty (30) days** from receipt of this Decision a complete report on the measures it has undertaken or will undertake to address the issue of delayed response to their customers' request in relation to their rights as data subjects.

SO ORDERED.

Pasay City, Philippines;
21 September 2020.

[8] Implementing Rules and Regulations of the DPA, Section 28(d)

(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:

CBI
Complainant

XXX
Respondent

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