Republic of the Philippines

NATIONAL PRIVACY COMMISSION

IBC,
Complainant,

-versus-

CID No. 17-K-004
For: Violation of Data Privacy Act of 2012

PBI,
Respondent.

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

DECISION

PATDU, D.P.C.

This Commission is being asked to decide whether a bank may be made liable for claims that certain transactions charged against the credit card it issued was not authorized by the card holder. The card holder in this case is the data subject who requested for the bank to remove the charges in his account relevant to transactions which he claims were unauthorized.

Facts of the Case

From the records of the case, Complainant obtained a credit card from respondent PBI. Under the terms and obligations of obtaining the card, complainant is obliged to pay the purchases to be made and charges to be incurred.

On 09 July 2017, complainant received an email from PBI through email address <customercare@pbi.com.ph>. Said email required him to log-in as a card holder to verify his information on a link provided, under threat of having his card suspended. The email message stated that his credit card would be temporarily suspended until the verification process is complete with a separate reminder not to input any wrong information, otherwise, his account will be suspended.

Complainant, on the belief that it was a legitimate email coming from the respondent bank, felt obliged to comply with the instructions provided in the email.

When complainant tried to use his credit card on 19 July 2017, he was informed that he had already reached his credit limit. Complainant immediately called the Respondent's customer service hotline and was shocked to learn that several transactions were charged against his credit card to which he had no knowledge of.

During his inquiry with the Respondent's customer hotline, complainant learned that there were transactions done on 10 and 11 July 2017, amounting to a total of Php 203, 983. Complainant also received information about additional transactions done on 18 July 2017 amounting to Php 33, 000 pesos. According to the records of the case, all questioned charges were transacted online.

On 20 July 2017, complainant filed a protest on the first series of transactions alleging that it was not authorized. PBI instructed the complainant to fill out and file a "Cardholder's Statement of Disputed Item" (CSDI) form in order to pursue his protest. On the same date, Complainant filed his CSDI form for the first series of transactions and submitted it to the Respondent. On 04 August 2017, complainant filed another CSDI form for the second series of alleged unauthorized transactions as additional disputed items.

Through a letter dated 25 August 2017, respondent PBI sent a response to the complainant stating that after reviewing the complaint filed, the first series of transactions shall remain to be for complainant's account as a cardholder. Respondent stated that the transactions were made online using the cardholder's full credit card details. Furthermore, for security, a One-Time Password (OTP) was sent to the cardholder's registered email address ibc@yahoo.com and that the said transactions were properly authenticated using the OTP sent to the registered address.

Complainant then wrote his letter of protest dated 10 September 2017 to formally require Respondent to make and effect the necessary correction/removal and rectification of his account. However, complainant did not receive a reply on his letter of protest as well as a

response to the second Cardholder's Statement of Disputed Items Form.

Hence, Complainant instituted this complaint before the Commission for violations of the Data Privacy Act.

Allegations of Complainant

Complainant alleges that the Respondent failed to set-up, institute and implement the necessary, appropriate and adequate security measures required under the Data Privacy Act. He further alleges that this enabled unauthorized entities to obtain the personal information of the complainant which was illegally used to make unauthorized and fraudulent transactions charged to his credit card account. In addition, he further alleges that he had suffered sleepless nights, serious anxiety and mental stress which arose from the refusal of the respondent to correct the billing of the unauthorized or fraudulent transactions made on his credit card.

Responsive Comment

Respondent in its responsive Comment admits the following matters:

a. The issuance to the complainant of the above-described credit and the transactions that were charged to it;
b. The two protests of the complainant through the submission of Cardholder's Statement of Dispute Item Forms; and
c. The first protest of the complainant was denied through a letter dated 25 August 2017 while the second protest was received through their Card Fraud Control but was not responded to.

In their defense, Respondent asserts that their Card Fraud Control immediately acted on complainant's protests as evidenced by the denial letter furnished to the complainant.

Respondent maintains that the online transactions are deemed valid because they were properly authenticated through the One-Time Password (OTP) sent to the complainant's email address.

Respondent PBI further maintains that it did not violate the Data Privacy Act (DPA) requiring personal information controllers to take steps to ensure that personal data are legally and properly processed by natural persons under its authority.

They assert that the Complainant, assuming that he was a victim of phishing incident as he claims in his complaint, cannot feign ignorance about such because Respondent regularly sends phishing advisories to its clients' Registered email addresses and mobile numbers, in addition to the posting of said advisories on its website and conduct of periodic awareness campaign.

Respondent maintains that the Complainant was the proximate cause, if not the sole cause of the data breach and not the alleged failure of the respondent to ensure proper and legal processing of complainant's data because he voluntarily disclosed his personal and financial information without verifying the link provided in the email.

Respondent prays that the complaint be dismissed since the Complainant has no cause of action against the respondent under the DPA and its implementing rules and regulations as the data breach was a result of complainant's own acts and not from the failure of respondent to set up, institute and implement the necessary, appropriate and adequate security measures.

Issues

The sole issue to be resolved by this Commission is whether Respondent PBI is liable for unauthorized processing on the alleged illegal transactions charged to the Complainant.

Decision

Rights of Data Subjects

Before the discussion on the issue of unauthorized processing, the Commission deems it necessary to discuss rights accorded to data subjects relevant to this case.

Data subjects under the Data Privacy Act[1] are entitled to rights, including the right to rectification[2] of his or her records, to wit;

> (d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That the third parties who have previously received such processed personal information shall he informed of its inaccuracy and its rectification upon reasonable request of the data subject;
>
> € Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and
> (f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

Responsibility rests upon the Personal Information Controller (PIC) in establishing procedures and mechanisms for the exercise of these rights. In this case, the claim of the data subject is that the charges in his credit card are inaccurate or false. The complainant filed 2 protests with the Respondent bank on 20 July 2017 and 04 august 2017, respectively, through the submission of Cardholder's Statement of Disputed Item (CSDI) Form.

We note that while the first protest was addressed, the second protest and the subsequent letter of protest were not. In Respondent's Comment[3], they admitted receiving the CSDI form filed by the Complainant on 20 July 2017 and 04 August 2017. They also admitted to issuing a response denying the request for the first protest on 25

[1] 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, § 3(c) (2012) [hereinafter, DPA].
[2] DPA, §16(d)
[3] Comment, par. 6-8

August 2017. While they also admit to receiving the second CSDF abovementioned, and a subsequent letter of protest received on 10 September 2017, there was no mention of any response issued to these requests. Hence, evidence on record shows that the Respondent has not addressed all the concerns of the complainant regarding the rectification of his credit records.

Unauthorized Processing and lawful
Basis for processing of personal information

The Complainant anchors his right to have his records rectified and removed from the system of PBI on the claim that the transactions made on his credit card was unauthorized or illegal. Hence, since he did not give his authority to the disputed transactions, PBI should not have processed the same. Since PBI allowed the transaction to push through without his consent, Complainant asserts that the Respondent bank should be made liable for unauthorized processing of his information.

The Commission finds this argument devoid of merit.

For a person or a Personal Information Controller to be held liable for unauthorized processing, the following elements must be present:

1. There must be processing of personal information;
2. That such processing was without the consent of the data subject or that such was not authorized by the Data Privacy Act or any other existing law.

Under the DPA, there are criteria for lawful processing of personal information[4].

The same criteria is applied in this case in determining whether the processing of the alleged unauthorized transaction by the bank was indeed lawful.

[4] DPA, §12

In processing the personal information relevant to the transactions and charges made on the credit card, PBI may find support in section 12(b)[5]:

> "**Section 12.** *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> (a) The data subject has given his or her consent;
>
> (b)The processing of personal information is necessary **and is related to the fulfillment of a contract with the data subject** or in order to take steps at the request of the data subject prior to entering into a contract; xxx" (emphasis supplied)

The use of the credit card issued by PBI is governed by the terms and conditions which sets out the obligations of the issuer and recipient of the credit card. As held in the case of *Pantaleon vs American Express International* and in *BPI Express Card Corporation vs. Armovit*, the relationship between the credit card issuer and the credit card holder is a contractual one that is governed by the terms and conditions found in the card membership agreement.[6] Such terms and conditions constitute the law between the parties.[7]

In the complaint[8] filed by IBC, he admitted that at the time he obtained credit card from PBI, he obliged himself, as the borrower, to pay those purchases and charges which he incurred under the terms and conditions of the contract. This fact is not disputed by the Respondent. Since the same terms and conditions govern the contractual relationship between the parties, the processing of personal information done by PBI pursuant to its contractual obligation is deemed lawful, as provided under the law.

Therefore, the claim of IBC that PBI is liable for unauthorized processing for processing without his consent is misplaced. While IBC claims that he did not authorize the transaction, the basis of processing as discussed above is not simply the explicit consent of the Complainant, but rather, such processing that is related to the fulfillment of the contract that they entered. Online transactions using

[5] DPA, §12 (b)
[6] Pantaleon vs American Express International, G. R. No. 174269, February 23, 2011.
[7] BPI Express Card Corporation vs Armovit, G. R. No. 163654, October 8, 2014.
[8] Complaint, par 3.

credit cards do not proceed in the same way as transactions done offline, where the credit card holder affixes his signature to every transaction. In this situation, the manner by which consent will be given by the data subject for the transaction is governed by the agreement between the parties, as provided in the card membership agreement. Part of this are provisions for the use of a One Time Pin (OTP) as further verification.

The question now left for this Commission to decide is whether the Respondent bank should be held liable for processing the credit card transactions charged to Complainant IBC upon the latter's allegations that the same are without his authority and that he was a victim of phishing. Complainant claims that the security measures placed by PBI were insufficient and this resulted to the phishing of his personal information which eventually led to the unauthorized purchases.

Phishing and Access due to negligence

Phishing is defined as the fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication[9]. The responsibility for the avoidance of falling victim to phishing falls both on the Personal Information Controller and the data subject.

The PIC must be able to implement appropriate security measures[10] provided under the DPA to capture cases of phishing and be able to prevent it from happening for the protection of its data subjects.

In the case at bar, Complainant IBC argues that due to PBI's negligence in not employing security measures, his personal information was illegally obtained through phishing.

This claim has not been sufficiently proven.

While it is true that IBC was able to establish that he fell victim to phishing by presenting a copy of the email pretending to be a

[9] ISO/IEC 27032:2012 (en), §4 Terms and definitions
[10] DPA, §20.

legitimate email message from PBI, he was not able to prove that falling for the same email was due to the negligence of the latter. Complainant's claim that PBI did not employ security measures was not supported by any evidence aside from his bare allegations.

On the other hand, PBI presented before this Commission substantial evidence that it has employed security measures to protect its data subjects, including Complainant IBC, from falling for phishing emails.

In the submissions made by the Respondent bank, records show how it regularly sends advisories to its clients' registered email addresses and mobile numbers. They also posted advisories on their website to constantly remind their clients to ignore phishing emails and messages. These advisories were sent to its clients as early as 2014. Furthermore, respondent has shown that it was not remiss in its duties in adopting dynamic consumer awareness program against phishing by utilizing all the available channels to reach their clients[11], through advisories in its website, television commercials and email reminders. As to the sending of email advisories, Respondent also presented proof that the complainant's email address is included as recipient of their advisories on warnings against phishing[12].

The Commission notes that the regular campaigns of the respondent against phishing do not only raise awareness of their customers, but it also provides its clients with precautionary steps to be taken if and when they receive suspicious emails luring them to give their personal information, particularly financial information[13].
Furthermore, in support of Respondent's defense, it submitted evidence that they have enabled multi-factor authentication for their online payments through the implementation of One-Time Password (OTP) to ensure that any access or purchase would need a confirmation from the account owner through an email message before they process the purchase. In fact, in their letter dated 26 August 2017 in response to the Complainant's first protest, they stated that their Card Fraud Department determined that the transactions were deemed valid since the same were properly authenticated through OTP sent to the complainant's email address. To substantiate this, they

[11] Comment, Annex "5"
[12] Id. P. 67
[13] Ibid

presented screenshots from their system that the OTP was successfully sent to the card holder's email address, that their OTP logs showed that the OTP was successfully entered, and that the email address was the same one that the complainant submitted to the bank.

The alleged unauthorized purchases were authenticated using the OTP sent to IBC's email. Following authentication, PBI authorized the processing of the purchases[14] and charged the same against the Complainant.

In summary, PBI'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 IBC that it was the negligence of PBI that caused the phishing of his personal information is not meritorious.

Anent the issue on the determination of fraud in credit card transactions, the same falls within the ambit of the Central Bank. It has not been sufficiently established before this Commission that the said transactions are indeed illegal or unauthorized.

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** PBI 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.

SO ORDERED.

(Sgd.)

IVY D. PATDU
Deputy Privacy Commissioner

[14] Records, p. 10

WE CONCUR:

(Sgd.)

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

CBI
Complainant

PBI
Respondent

PBI CARDS
Respondent

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
NATIONAL PRIVACY COMMISSION