



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

JLB,

Complainant,

CID-18-D-009

*For: Violation of the Data
Privacy Act of 2012*

-versus-

SECURITY BANK CORPORATION,

Respondents.

x-----x

DECISION

NAGA, D.P.C.:

This case involves an alleged unauthorized disclosure by the Respondent of the Cash Advance Personal Identification Number (CA PIN) and other personal information of the Complainant to unknown persons.

The Facts

JLB (Complainant) is a Security Bank Mastercard credit card holder since 16 January 2018. Security Bank Corporation (Respondent) is a universal banking corporation duly organized and existing under the laws of the Philippines.

On 29 January 2018, Complainant requested the CA PIN of his credit card through the Customer Service Hotline of the Respondent.

On 03 February 2018, Respondent, through Safefreight Services, Inc. (Safefreight), delivered the requested CA PIN to the billing address of the Complainant, which was received by a certain LA who identified herself as the Complainant's maid/caretaker. However, in a phone call with the Respondent's representative, the Complainant denies knowing LA. The Complainant then conveyed

to the representative of the Respondent to deliver the subsequent requested CA PIN to CB, MNB, and JPB only.

Respondent then delivered the second CA PIN to the Complainant's billing address, which was received by CB on 23 February 2018.¹

On 26 February 2018, the courier service provider, Safefreight, investigated the complaint of the Complainant in relation with the first CA PIN. Safefreight visited Complainant's residence and was able to speak with LA. LA confirmed the receipt of the first CA PIN, which according to her was forwarded to the Complainant.²

On 04 April 2018, Respondent's Customer Contact Group received an email from Complainant alleging that the bank exposed his personal and banking information to unknown individuals.

On 07 April 2018 a regenerated third CA PIN was delivered to the billing address of the Complainant, which was received by CB.

On even date, the Commission, through its Complaints and Investigation Division (CID), received the Letter of Complaint dated 06 April 2018 from the Complainant.

The Complainant alleged that the Respondent exposed his personal and sensitive personal information (i.e., full name, address, CA PIN, and name of bank) to persons unknown to him and that it may bring potential risk to his finances and safety. Complainant thus, charges Respondent with violations of Sections 32 and 33 of the Data Privacy Act of 2012 (DPA).³

Respondent filed its Comment in compliance with the Commission's Order dated 04 July 2018. Respondent argues the following:

¹ Note that the Respondent's agent erroneously reported to the Complainant that it was delivered to a certain MC. Nevertheless, the Complainant acknowledged in his Reply to the Respondent's Comment that the second CA PIN was received by CB.

² Annex 3 of Respondent's Comment

³ Complaint dated 06 April 2018

1. The CA PIN documents were properly sealed and endorsed to the courier services and it was delivered to the billing address indicated in the Complainant's credit card application.
2. Upon the investigation of Safefreight, they were able to validate that LA is the Complainant's maid and that she was able to forward the CA PIN to the Complainant.
3. That the properly sealed second and third CA PIN was received by the Complainant's father, CB in the indicated billing address.⁴

In the Order dated 20 June 2018, the case was called for Discovery Conference on 04 July 2018.

On 04 July 2018, the Complainant and Respondent's counsel appeared before the Commission and signified that there is no need to secure evidence from each other to further their case.

Complainant filed his Reply to the Respondent's Comment on 05 August 2018. In the Reply, the Complainant restated the allegations in his Complaint. He also maintained that the proof of delivery signed by LA should not be considered proof of delivery to the correct address or that it was received by an authorized recipient. Further, he emphasized that he does not know LA.

On 19 February 2020, this Commission ordered the Respondent to submit Supplemental Comment with reference to item number 25 of their submitted Comment.⁵ Specifically, the Commission wants the Respondent to submit details on utilization of the three CA PINs that were issued to the Complainant herein. However, up to date, the Commission did not receive any submissions from the Respondent.

Issue

⁴ Respondent's Comment dated 04 July 2018

⁵ 25. Lastly, it should also be noted that Complainant JLB has already used the CA PIN he requested when he successfully availed a cash advance through his credit card on 09 April 2018. Prior to this, there were two (2) CA PIN transactions involving attempts to avail cash advance made on 03 April 2018 with reference to the credit card of Complainant JLB. This only goes to show that Complainant JLB received his CA PIN.

Whether the Respondent violated Sections 32 and 33 of the DPA.

Discussion

The Complaint lacks merit. The Commission finds that the Complainant herein failed to prove by substantial evidence violations of Section 32 and Section 33 of the DPA by the Respondent herein.

As already established in past rulings, in administrative proceedings such as in this Commission, the burden is on the Complainant to prove by substantial evidence the allegations in his Complaint are true.⁶ “Substantial evidence is more than a mere scintilla of evidence. It means such relevant evidence as a reasonable mind might accept as adequate to support a conclusion, even if other minds equally reasonable might conceivably opine otherwise.”⁷

Section 32 (Unauthorized Disclosure) and Section 33 (Combination or Series of Acts) of the DPA provide, *thus*:

SEC. 32. *Unauthorized Disclosure.* – (a) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(b) Any personal information controller or personal information processor or any of its officials, employees or agents, who discloses to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos

⁶ Montemayor v. Bundalian, 453 Phil. 158 167

⁷ *Ibid*

(Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

SEC. 33. *Combination or Series of Acts.* – Any combination or series of acts as defined in Sections 25 to 32 shall make the person subject to imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

Complainant alleges that unauthorized disclosure of personal and sensitive personal information was committed when the Respondent delivered the first CA PIN to LA, a person that the Complainant does not know. In the Comment provided by the Respondent, it was stated that the three (3) CA PINs were delivered in the billing address provided by the Complainant to the Respondent in his credit card application. The first CA PIN was received by LA, who upon the Courier Troubleshoot Investigation Report conducted by Safefreight,⁸ revealed that she was the Complainant's maid. It was later found out that the second and third CA PINs were received by CB, the father of the Complainant, in the same billing address. In fact, the second and third CA PINs were eventually used by the Complainant in two (2) instances on 03 April 2018 and on 09 April 2018.

Instead of presenting an evidence to counter the Respondent's contentions, the Complainant herein just reiterated in his Reply his allegation that LA is not known to him, *viz*:

"I can no longer count how many times I have advised Security Bank Corporation (SBC) that I do not know any person name LA."⁹

Section 1, Rule 131, of the Revised Rules on Evidence provides, *viz*:

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.

⁸ Annex 3 of Respondent's Comment

⁹ Reply of the Complainant to the Respondent's Comments

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)

At this point, the Complainant has now the burden of evidence to prove in his Reply that LA is not known to him and that there was improper delivery of the CA PIN despite the delivery of the Respondent in the billing address as stated in the Complainant's credit card application. However, in this case, the Complainant just reiterated and relied on his allegations to counter the defenses provided by the Respondent. Basic is the rule that mere allegation is not evidence and is not equivalent to proof.¹⁰

Having failed to prove the factual allegations contained in the Complaint by substantial evidence, the allegations for violation of Section 32 and Section 33 of the DPA should likewise fail.

On another matter, this Commission would like to respond to the Respondent's assumption that it already established reasonable and appropriate measures intended for the protection of personal information just because it sent to its clients a properly sealed document, *viz*:

"There is also no unauthorized disclosure of Complainant JLB's CA PIN. We invite the attention of the Honorable Commission that when a CA PIN requested by a certain client is delivered, **the same is contained in a properly sealed document which can only be opened by tearing the sides of perforated paper....** Thus, even if the properly sealed document containing the CA PIN was handed to LA by the courier, delivery alone to the latter of the same is not equivalent to unauthorized disclosure of his CA PIN."

This Commission does not agree with Respondent's assertion that properly sealing of the documents is all it takes to comply with the DPA in this case. Section 20 of the DPA provides:

¹⁰ Morales, Jr. v. Ombudsman Carpio-Morales, et. al., G.R. No. 20808627, July 2016

SEC. 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.

To fully comply with the DPA, delivery procedure must include the policy that a document shall only be given to authorized persons if the primary recipient is not present to receive such document and other policies that will ensure the proper disclosure of documents containing personal and sensitive personal information.

Further, even if the Respondent subcontracts its courier service, the DPA still puts the responsibility of complying with the requirements of said law on the Personal Information Controllers (PICs), *viz*:

SEC. 14. Subcontract of Personal Information. - A personal information controller may subcontract the processing of personal information: Provided, That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

Thus, even if the Complainant failed to establish his case by substantial evidence, this Commission would not be precluded to conduct Compliance Check to the Respondent herein as provided by NPC Circular No. 18-02. This is to ensure that its processes and procedures are compliant with the DPA and other issuances of the Commission.

WHEREFORE, all premises considered, this Commission resolves to **DISMISS** the instant Complaint filed by JLB against Security Bank Corporation for lack of merit.

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:

JLB
Complainant

LPMMDAF
Counsel for the Respondent

SECURITY BANK CORPORATION

Respondent

**COMPLAINTS AND INVESTIGATION DIVISION
COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission**