EDF,
Complainant,

\- versus -

BANK OF THE PHILIPPINE ISLANDS,
Respondent.
x----------x

NPC 21-016
For: Violation of the Data Privacy Act of 2012

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by EDF against the Bank of the Philippine Islands (BPI) for a violation of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Facts

On 11 November 2020, EDF received a call from a woman claiming to be a BPI employee who was supposedly conducting security enhancements on his BPI online account.[1] EDF alleges that the woman informed him of his full name and that she needed to log-in to his BPI online account to implement the security enhancements.[2] EDF maintains that the woman requested him to dictate several "number codes" that he received through text messages.[3] EDF admits that he cooperated with her requests only to belatedly realize that it was a scam.[4]

On the same day, EDF reported the incident to BPI – Zamboanga Main.[5] He asserts that a BPI customer representative informed him

[1] Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[2] *Id.*
[3] *Id.*
[4] *Id.*

[5] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

that his BPI Online account and BPI credit card were already blocked, that an online funds transfer to a GCash account amounting to Four Thousand Four Hundred Pesos (P4,400.00) could no longer be reversed, and that several transactions with Lazada amounting to Ninety Thousand Pesos (P90,000.00) were still floating.[6]

On 15 January 2021, EDF filed a complaint against BPI.[7] He alleges that BPI committed a "privacy violation" because the woman claiming to be its personnel had knowledge of his BPI online account.[8] He prays for the reversal of the Lazada transactions and the arrest of the woman purporting to be BPI's personnel.[9]

On 21 July 2021, the Commission issued an Order directing BPI to file a verified comment fifteen (15) calendar days from receipt of the Order and to appear for preliminary conferences on 25 August 2021 and 08 September 2021.[10]

On 25 August 2021, EDF appeared for the first preliminary conference and expressed his willingness to undergo mediation proceedings.[11] BPI did not appear due to a conflict of schedule.[12]

On 08 September 2021, both parties appeared for the second preliminary conference and manifested their willingness to undergo mediation proceedings.[13]

On 20 October 2021, BPI filed its Comment.[14] BPI explains that it investigated the disputed online funds transfer transaction to GCash and the disputed credit card transactions.[15] It maintains that the complaint should have been dismissed outright by the Commission according to Rule IV, Section 1 of NPC Circular No. 2021-01 (2021 NPC Rules of Procedure).[16] BPI argues that the cause of action neither pertains to a violation of the DPA nor involve a privacy violation or

[6] *Id.*
[7] Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[8] *Id.*
[9] *Id.* at 5.
[10] Order (To File Verified Comment and Appear Virtually for Preliminary Conference), 21 July 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[11] Fact-Finding Report, 17 September 2022, at 2, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[12] *Id.*
[13] *Id.*
[14] Comment, 20 October 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[15] *Id.* at 1-3.
[16] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

personal data breach, and that EDF presented insufficient information to substantiate the allegations in the complaint.[17]

It also alleges that EDF failed to establish by competent evidence that the disputed online funds transfer and credit card transactions were unauthorized.[18] It reiterates the validity of the transactions:

> Your Online Banking account was accessed using your nominated User Name and Password. Succeeding transactions were further authenticated by a One-Time PIN (OTP)/ Mobile Key.
>
> May we reiterate that the transactions done via the [sic] BPI Online can only be completed by undergoing several security measures:
>
> 1. Device binding – The device must be linked to client's online account to ensure that the account can only be accessed in client's trusted devices. One-Time PIN [OTP] (which is sent only to client's registered mobile number with the Bank) is required to link the device.
> 2. User Name and Password – The user is required to input his online credentials to access the account.
> 3. One-Time PIN (OTP) or Mobile Key for transactions – The user is required to input an OTP or Mobile key [sic] to execute financial transactions, except for transfer to own account.
>
> Given these security measures in place, the Bank had discharged its obligation in providing a safe and secure online banking platform. Since the personal banking information, which were under your control, were unfortunately compromised at your end, we regret to state that we are unable to grant reversal of your disputed transactions under the terms of use of the Internet Banking Service Agreement in place.[19]

It further explains that it implements a multi-factor authentication method to verify online fund transfers through BPI Online and online credit card transactions:

> 10. It must be emphasized that the Respondent implements a multi-factor authentication method to verify online funds transfers through BPI Online, and online credit card transactions. BPI Online transactions are authenticated through the concurrence of the following personal data conclusively presumed to be known only to the depositor:

[17] *Id.*
[18] *Id.*
[19] *Id.* at 2.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

1. BPI Online username;
2. BPI Online password; and
3. one-time-password ("OTP," for brevity) sent to the depositor's registered mobile number at the time of the transaction.

11. With regard to online credit card transactions, they are authenticated through the concurrence of the following personal data conclusively presumed to be known only to the depositor:
1. 16-digit credit card number printed on the face of the credit card;
2. expiry date printed on the face of the card;
3. 3-digit CVC printed on the back of the card; and
4. one-time-password ("OTP," for brevity) sent to the cardholder's registered mobile number, or his/her static 16-digit Customer Number.

12. In the present case, the disputed transactions would not have been made without the concurrence of the foregoing personal data. Therefore, the transactions are conclusively presumed to be made by the Complainant himself. He has the burden to present clear and convincing evidence to prove otherwise. Bare self-serving allegations do not equate to proof.[20]

On 19 October 2021, the parties conferred for mediation but failed to reach a settlement.[21] On 25 November 2021, the Commission issued an Order for the resumption of complaint proceedings and ordered the parties to submit their respective Memoranda within fifteen (15) calendar days from receipt of the Order.[22]

On 06 December 2021, EDF filed a Motion for Extension of Time to Submit Memoranda.[23] The Commission granted EDF until 26 December 2021 to submit his Memorandum.[24]

On 27 December 2021, EDF filed his Memorandum.[25] He alleges that he "never shared his mobile number to individuals not known to him, more so his BPI Accounts are only known to him and [BPI]."[26] He further argues that BPI failed to perform its mandatory obligations

[20] Comment, 20 October 2021, at 2-3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[21] Order to Mediate, 14 September 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[22] Order (Resumption of Complaints Proceedings and Submission of Memoranda), 25 November 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[23] Motion for Extension, 06 December 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[24] Order (Granting the Request for Extension of Time to Submit Memoranda filed by Complainant), 13 December 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021)..
[25] Memorandum for the Complainant, 27 December 2021, *in* EDF v. Bank of the Philippine Islands, NPC 21- 016 (NPC 2021).
[26] *Id*. at 6.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

under Section 20 of the DPA in implementing reasonable and appropriate organizational, physical, and technical measures for the protection of his personal information, particularly his personal mobile number, BPI Accounts, office address, date of birth, and mother's maiden name.[27]

He maintains that his confidential personal information was breached because BPI was remiss in its mandatory obligation to secure his personal information, which are "under the safekeeping of BPI."[28] He also avers that BPI did not exercise the necessary due diligence when it failed to inform him of the dubious Lazada transactions that were charged to his BPI credit card.[29]

Because of BPI's supposed failure to safeguard EDF's personal information, he prays that BPI should be held liable for Section 26 (Accessing of Personal Information and Sensitive Personal Information Due to Negligence), Section 27 (Improper Disposal of Personal Information and Sensitive Personal Information), and Section 32 (Unauthorized Disclosure) of the DPA.[30] He also prays that BPI should be ordered to reverse the Lazada transactions and all other related charges as damages.[31]

BPI did not file its Memorandum.

Issue

Whether BPI's supposed failure to safeguard EDF's personal information constitutes a violation of the DPA.

Discussion

The Commission dismisses the case for lack of substantial evidence.

[27] *Id.* at 6-7.
[28] *Id.* at 7.
[29] *Id.* at 10.
[30] *Id.* at 8-9.
[31] Memorandum for the Complainant, 27 December 2021, at 11, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

BPI argues that the case before the Commission should have been dismissed outright according to Rule IV, Section 1 of the 2021 NPC Rules of Procedure:[32]

> Section 1. *Outright dismissal, when allowed.* – Within thirty (30) calendar days from receipt of the complaint, the investigating officer may give the complaint due course or dismiss the complaint without prejudice, on any the following grounds:
>
> 1. The complaint is insufficient in form or did not comply with Section 3, Rule II of these Rules, unless failure to do so is justified or excused with good cause;
> 2. The complainant did not give the respondent an opportunity to address the complaint, unless failure to do so is justified;
> 3. **The complaint does not pertain to a violation of the Data Privacy Act of 2012 or does not involve a privacy violation or personal data breach;**
> 4. **There is insufficient information to substantiate the allegations in the complaint; or**
> 5. The parties, other than the responsible officers in case of juridical persons, cannot be identified or traced despite diligent effort to determine the same.[33]

BPI's contention is untenable. EDF's complaint should not have been dismissed outright. First, the complaint asserts a cause of action for a privacy violation, which requires the Commission's careful consideration. The mere allegation, however, that EDF's BPI Online Account, credit card, and other details are involved is not, by itself, sufficient. In this case, as stated in EDF's complaint, the unidentified caller knew of EDF's full name and other pieces of personal information, such as his office address, date of birth, and mother's maiden name.[34] This allegation, together with his allegations concerning the disputed transactions using his BPI Online Account and online credit card transactions, show that a cause of action is sufficiently stated in the complaint.

Second, an outright dismissal based on "insufficient information to substantiate the allegations in the complaint" would have been unfair to EDF.

[32] Comment, 20 October 2021, at 1-3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[33] National Privacy Commission, 2021 Rules of Procedure of the National Privacy Commission [NPC 2021 Rules of Procedure], rule IV, § 1 (28 January 2021). Emphasis supplied.
[34] Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

To substantiate his complaint, EDF submitted Statements of Account showing the supposedly unauthorized transactions on his BPI Online account and credit card, and an email containing the results of BPI's internal investigation.[35]The Commission, however, recognizes that EDF could not have had been able to submit other pieces of evidence to substantiate his claims apart from those that he submitted when the complaint was filed. As such, to dismiss the case outright without giving EDF the opportunity to confer for preliminary conference and avail himself of discovery proceedings would have been unfair to him.

In this case, the parties conferred for preliminary conference according to Rule V, Section 1 (2) of the 2021 NPC Rules of Procedure:

> Section 1. *Order to confer for preliminary conference.* – No later than thirty (30) calendar days from the lapse of the reglementary period to file the comment, the investigating officer shall hold a preliminary conference to determine:
>
> 1. whether alternative dispute resolution may be availed by the parties;
> 2. **whether discovery is reasonably likely to be sought in the proceeding;**
> 3. simplification of issues;
> 4. possibility of obtaining stipulations or admissions of facts and of documents to avoid unnecessary proof; or
> 5. such other matters as may aid in the prompt disposition of the action.[36]

The Supreme Court explained the purpose of discovery proceedings:

> What is chiefly contemplated is the discovery of every bit of information which may be useful in the preparation for trial, such as the identity and location of persons having knowledge of relevant facts; those relevant facts themselves; and the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things.[37] | | |

Discovery proceedings are essential, such as in this case, where the complainant cannot simply rely on the evidence it has to properly substantiate its allegations.[38] In this case, the evidence that EDF

[35] *Id.* Annex.
[36] NPC 2021 Rules of Procedure, rule V, § 1. Emphasis supplied.
[37] Producers Bank of the Philippines v. Court of Appeals, G.R. No. 11049 (1998).
[38] *See Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

could have presented to prove the existence of a privacy violation and BPI's supposed liability are most likely in the hands of BPI. Aside from the pieces of evidence that EDF submitted with his complaint, he could not have been able to produce other pieces of evidence to substantiate his allegations.

Following this, EDF could have availed himself of discovery proceedings to seek additional information and documents from BPI to substantiate his claims during the preliminary conference. Yet, he did not. Instead, he merely relied on the evidence that he submitted with his complaint.

Further, EDF himself admitted in his complaint that he received a call from an unverified person and gave several "number codes" that he received through text messages.[39] Although EDF never used the term one-time password (OTP), these "number codes" seemingly correspond to the OTP sent to the BPI depositor's registered mobile number at the time of the transaction in order to validate the BPI Online account and online credit card transactions.

By admitting that he dictated these "number codes" or OTP to the unverified person, the burden of evidence shifted to EDF requiring him to present evidence to support his claims against BPI. Section 1, Rule 131 of the 2019 Amendments to the Revised Rules on Evidence provides:

> 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.[40]

In his Memoranda, EDF asserts BPI's supposed failure to implement security measures and to safeguard his personal

[39] Complaints-Assisted Form, 15 January 2021, at 3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[40] 2019 AMENDMENT TO THE 1989 REVISED RULES ON EVIDENCE, A.M. No. 19-08-15-SC, Rule 131, §1 (1 May 2020). Emphasis supplied.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

information resulted in a breach of his confidential personal information following Section 20 of the DPA, which provides:

> Section 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.[41]

EDF claims that as a result of BPI's inaction, his BPI Online account and credit card were used for the disputed transactions.[42] EDF, however, failed to provide evidence to categorically substantiate his claim. Despite being given the opportunity to do so, EDF did not seek additional information and documents from BPI.

It is not sufficient for EDF to make allegations without substantial evidence to support his claims, considering that:

> The basic rule is that mere allegation is not evidence and is not equivalent to proof. Likewise, charges based on mere suspicion and speculation cannot be given credence.[43]

Contrary to EDF's assertions, BPI was not remiss in its obligation to implement security measures under the DPA. It maintains that it implements a multi-factor authentication method, which requires "personal data conclusively presumed to be known only to the depositor" to verify online fund transfers through BPI Online and online credit card transactions.[44] As explained in BPI's Comment, such transactions require a user-nominated user name and password, and an OTP that is sent only to the user's registered mobile number.[45] The fact that there was an OTP required in the supposedly unauthorized transactions shows that BPI implemented its multi-factor authentication.

---

[41] 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 § 20 (a) (2012).
[42] Memorandum for the Complainant, 27 December 2021, at 7, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).
[43] BSA Tower Condominium Corp. v. Reyes II, A.C. No. 11944 (2018).
[44] Comment, 20 October 2021, at 1-3, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021) .
[45] *See* Comment, 20 October 2021, at 2, *in* EDF v. Bank of the Philippine Islands, NPC 21-016 (NPC 2021).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

As admitted in his complaint, EDF's own actions directly resulted in the disputed transactions. To reiterate, it was EDF himself who dictated the "number codes" or OTP to the unverified caller.[46] The fact that the unverified caller allegedly knew EDF's personal information does not automatically mean that there was a breach or negligence on the part of BPI.

The Commission reminds data subjects that they should endeavor to protect their personal data, including bank account numbers, log-in credentials, credit card details, and OTP through email links, text messages or phone calls, to avoid possible risk or harm. As this Commission ruled in CID 17-K-004, "[the] security of personal information is a joint obligation of both the data subjects and data controller or processor. Implementation of a 'reasonable' security measure does not mean that the measure is a foolproof [sic] for any contributory negligence on the part of the data subject."[47]

EDF's admission, and the lack of substantial evidence to support his allegations cannot give rise to the conclusion that BPI's failed to implement security measures and that this supposed failure resulted in the unauthorized transactions. Given the foregoing, the Commission cannot find BPI liable for violating Section 26 (Accessing of Personal Information and Sensitive Personal Information Due to Negligence), Section 27 (Improper Disposal of Personal Information and Sensitive Personal Information), and Section 32 (Unauthorized Disclosure) of the DPA.

As to EDF's prayer on the reversal of the unauthorized transactions, such is beyond the jurisdiction of the Commission.

WHEREFORE, premises considered, the Commission resolves to **DISMISS** the Complaint of EDF against the Bank of the Philippine Islands.

SO ORDERED.

Pasay City, Philippines.

[46] *See* Complaints-Assisted Form, 15 January 2021, at 3-4, *in* EDF v. Bank of the Philippine Islands, NPC 21- 016 (NPC 2021).
[47] CBI v. XXX, CID 17-K-004, 29 September 2020, at 5-6, *available a*t https://www.privacy.gov.ph/wp-content/uploads/2020/12/CID-17-K-004-CBI-v-XXX-Decision-ADJU1.pdf (last accessed 04 April 2022).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

17 March 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

Copy furnished:

EDF
Complainant

BANK OF THE PHILIPPINE ISLANDS
Respondent

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT

National Privacy Commission

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228