Republic of the Philippines
NATIONAL PRIVACY COMMISSION

BGM

Complainant,

- versus -

NPC 19-653

(For violation of Data Privacy Act of 2012)

IPP.,

Respondent.

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

DECISION

LIBORO, P.C.:

Before this Commission is a Complaint filed by BGM (Complainant) against IPP. (Respondent) for the violation of her rights as a data subject under the Data Privacy Act of 2012 (DPA).

Facts

On 17 July 2019, Complainant filed her Complaint-Affidavit, alleging that respondent have violated her data privacy rights. In her Complaint-Affidavit, Complainant alleged that:

> Complainant's sister purchased online an iPad Pro from a certain seller named LQG (Seller) via an online platform CP. One of the mode of payments in said transaction was through respondent IPP., where payments can be made through its app or its designated physical payment centers. Hence, upon the request of her sister, Complainant paid the remaining balance of the purchase price, in the amount of Twenty Thousand pesos (P20,000.00) to the Seller through the medium provided by Respondent. Complainant then proceeded to the meet up place where the Seller promised to hand over the purchased product. However, after waiting for more than three (3) hours, the Seller was nowhere to be found. Complainant immediately called Respondent to have the Seller's account blocked and to get more information on the

> identity of the same for future legal actions. In the said phone call, Respondent told complainant that before they can disclose any information on the recipient of the payment, complainant must first secure a police blotter and a court order. On the same day, Complainant went to the MOA Police Community Precinct to file a police blotter of the incident. Thereafter, Complainant received a text message[1] from the seller's alleged mobile number saying that she used the money for her comatose son and that she will pay back Complainant when she receives the money from PCSO.

On 27 March 2019, Complainant sent Respondent an email informing them of the alleged incident and consequently requesting for the information of the account holder involved in the incident. Complainant invoked Section 16 (c) of the DPA [2] alleging that Respondent have violated the same for not providing them of the requested personal information of the seller/account holder who allegedly defrauded them thus prompting her to file the instant complaint.

On 12 September 2019, the parties were called for discovery conference. Both parties appeared, Atty. VTM, Mr. RCJ and Ms. UTM represented Respondent. During the scheduled discovery conference, Complainant asked from Respondent the information of the person she had the transaction with using Respondent's facility as alleged in the Complaint. However, since said information is involved in the issue of the case, Respondent was not required by the investigating

---

[1] Records at page 10 Fact-Finding Report NPC Case No. 19-653 Page 2
"Hi good evening. I'm sorry for what happened. Thank you so much sa tulong mo malaking tulong 2 para sa anak kong comatose ngaun dito sa davao. Ibabablik q agad to pagkakuha ko sa psco. Pinapangako ko yan sau. At dodoblehin pa 2 ni lord. Ung binayadm kc kinuha ko lang din sa remittance center. Salamat ulit. God bless."

[2] Section 16 (c) of DPA provides:
(c) Reasonable access to, upon demand, the following:
(1) Contents of his or her personal information that were processed;
(2) Sources from which personal information were obtained;
(3) Names and addresses of recipients of the personal information;
(4) Manner by which such data were processed;
(5) Reasons for the disclosure of the personal information to recipients;
(6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;
(7) Date when his or her personal information concerning the data subject were last accessed and modified; and
(8) The designation, or name or identity and address of the personal information controller;

officer to divulge the same. Respondent and Complainant were then ordered to submit their Responsive Comment within ten (10) days from the date of the discovery conference and Reply, respectively.

On 14 October 2019, Respondent filed its Responsive Comment praying for the dismissal of the instant complaint because it does not involve a violation under the DPA. Further, Respondent argued that the provision under Section 16 (c) (3) of the DPA does not apply when the data subject prompted the sharing of information to the receiver due to a transaction between them. Accordingly, it cannot give the personal information requested by the Complainant without the risk of violating the data privacy rights of the data subject involved as well as violating the numerous obligations mandated by the same law to personal information controllers.

Respondent further contended that their imposition of requiring Complainant to first obtain a police blotter and a court order are mere safeguards that they have to enforce as custodians of the personal information disclosed to them.

On 24 October 2019, Complainant then filed her Reply to Respondent's Responsive Comment. In her Reply, Complainant anchored her claims on the following: Complainant contended that the act of Respondent requiring her to first secure a court order manifests the latter's disinterest in protecting its subscribers from fraudulent behavior in the usage of their online application. More so, that such acts would embolden scammers from using their service, knowing that Respondent would not divulge any information. To disclose only on the basis of a court order before Respondent divulges the information she is requesting defeats the purpose of the right of access granted to data subjects under the DPA. Further, Complainant assumes that by the time that a court order is released, the case involving said fraudulent acts would have gone stale and would also cause the complaining party great cause, expense, and effort. She argued that she has no other means to verify the name given to her by the alleged scammer aside from the information that Respondent have in their custody. Complainant believes that it is essential for her to obtain the subject information from Respondent because the scammer may have used or assumed a different identity, which might cause failure on her part to protect her property from fraud. Complainant reiterated that to

allow Respondent to decline from disclosing information needed, such as in the instant Complaint, would effectively prevent other similarly situated victim of fraud to have concrete legal recourse against the scammer.

On 20 November 2019, Respondent filed its Rejoinder restating their prayer for the dismissal of the instant Complaint.

Issue

Whether or not Respondent's act of requiring Complainant to secure a court order prior to its release of the requested personal information violated the latter's data privacy rights.

Discussion

The Commission posits that the instant Complaint should prosper.

The crux of the Complaint involves the data subject's right to access, which is one of the rights conferred by the DPA under Section 16, paragraph (c) of the DPA, as follows:

> SEC. 16. *Rights of the Data Subject.* – The data subject is entitled to:
>
> x x x
>
> (c) Reasonable access to, upon demand, the following:
>
> (1) Contents of his or her personal information that were processed;
> (2) Sources from which personal information were obtained;
> **(3) Names and addresses of recipients of the personal information;**
> (4) Manner by which such data were processed;
> (5) Reasons for the disclosure of the personal information to recipients;
> (6) Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

> (7) Date when his or her personal information concerning the data subject were last accessed and modified; and
> (8) The designation, or name or identity and address of the personal information controller; x x x

In the instant case, in the exercise of her right to access, Complainant merely seeks to obtain the information of the recipient of her personal information.

Section 16 (c) (3) of the DPA is clear which has no room for interpretation and should therefore be applied in its literal meaning.

Complainant, as data subject, should be entitled to access the information of the recipient of her personal information considering that the money transfer receipts of Respondent only contains a transaction number and does not contain the name of the recipient of Complainant's personal information to enable her to identify as to whom a criminal case should be filed against.

In sum, Respondent's excessive or stringent requirement to complainant, with regard to the Complainant's request for the information of the account holder of the Respondent involved in the subject incident of alleged scam, violated the latter's right to access.

Moreover, Respondent as an entity considered as personal information controller (PIC), it is duty bound to observe and uphold the data privacy rights of Complainant, which thereby includes her right to access.

The Respondent herein should not have denied outright the request of the Complainant for the exercise of her right to access and using the DPA as a shield. Its requirement of compelling Complainant to produce a court order prior to the release of the requested information creates a high barrier that effectively impedes the rights vested by the DPA to the latter as a data subject.

Further, Respondent's assertion that the information within its custody can only be disclosed upon data subject's consent or on the basis of a lawful order is misplaced.

Section 12 of the DPA provides for the following criteria for lawful processing:

> SEC. 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:
>
> x x x
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution

In order for Complainant to secure a court order, there must necessarily first be a court proceeding. However, before there can be any court proceeding or in order for Complainant to initiate a criminal case against the Seller, the Complainant needs the information as to whom her personal data was disclosed in order to know against whom she should file a criminal case against.

Section 13 of the DPA expressly prohibits the processing of sensitive personal information, except in the following cases:

> "xxx f. The processing concerns such personal information as is **necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims,** or when provided to government or public authority (Emphasis supplied)."

In the case of NPC 17-018 dated 15 July 2019, this Commission held that "processing as necessary for the establishment of legal claims" does not require an existing court proceeding. To require a court proceeding for the application of Section 13(f) to this instance would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of "establishment … of legal claims" presupposes that there is still no

pending case since a case will only be filed once the required legal claims have already been established."

This Commission in the same case went on further and held that:

> The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is "necessary" or may or may not be collected by lawyers for purposes of building a case, applying the qualifier "necessary" to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of "establishment of legal claims" consistent with the general principles of legitimate purpose and proportionality.
>
> As regards legitimate purpose, the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.18 This means that the processing done for the establishment of a legal claim should not in any manner be outside the limitations provided by law. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.

Based on the foregoing, the disclosure to be made by the Respondent of the information of the recipient of Complainant's personal information, for purposes of identification of the person liable for the alleged fraud, *sans* the latter's consent, is necessary for the protection of the lawful rights and interests of the Complainant as contemplated by Section 13 (f) of the DPA.

Although Section 13(f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13(f) by the Respondent is considered as legitimate interest pursuant to Section 12(f) of the DPA.[3] This section provides that it is lawful to process personal information if it is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of

[3] CID Case No. 17-K-003 dated 19 November 2019 and NPC 18-135 dated 06 August 2020

the data subject which require protection under the Philippine Constitution.[4]

By application in the instant case, Respondent may not be held liable for unauthorized processing should it disclose the requested information to Complainant as its disclosure would be in pursuance of the latter's legitimate interest as the same cannot be fulfilled by other means.

It should be stressed, however, that having a legitimate purpose or some other lawful criteria to process does not result in the PIC granting all request to access by the data subjects. Such requests should be evaluated on a case to case basis and must always be subject to the PIC's guidelines for the release of such information.

Aside from legitimate purpose, the qualifier "necessary" also pertains to the general privacy principle of proportionality. Under the IRR, the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. The proportionality principle, as manifested in the qualifier "necessary" serves as a sufficient test in determining whether the processing is justified in relation to the declared purpose.[5]

Lastly, this Commission finds that the award of nominal damages to Complainant is warranted.

The Data Privacy Act provides that restitution for any aggrieved party shall be governed by the provisions of the New Civil Code.[6] The relevant provision in this Code states:

> Art. 2221. Nominal damages are adjudicated in order that a right of the plaintiff, which has been violated or invaded by the defendant, may be vindicated or recognized, and not for

[4] R.A. 10173, Section 12(f); *Ibid.*
[5] *Ibid.*
[6] *Id.*, §37.

> the purpose of indemnifying the plaintiff for any loss suffered by him.

As provided by the Supreme Court, in *Santos B. Arreola v. Court of Appeals.:*

> Nominal damage is recoverable where a legal right is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind, or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown.[7]

As established above, the Respondent violated the Complainant's right to access which is considered as a violation of the DPA[8]. The Supreme Court has also clarified that no actual present loss is required to warrant the award of nominal damages, thus:

> Nominal damages are recoverable where a legal right is technically violated and must be vindicated against an invasion that has produced no actual present loss of any kind or where there has been a breach of contract and no substantial injury or actual damages whatsoever have been or can be shown.[9]

As a recognition and vindication of Complainant's right that was violated by Respondent, the Commission awards nominal damages to the Complainant in the total amount of Forty Thousand (P40,000) Pesos.

WHEREFORE, all premises considered, Respondent IPP. is hereby **ORDERED** to furnish the Complainant BGM the name of the recipient of her personal information in compliance with Section 16 (c) (3) of the Data Privacy Act and pay the Complainant the amount of Forty Thousand (P40,000) Pesos as nominal damages to vindicate Complainant's right to access, which was violated by Respondent. Further, Respondent is mandated by this Commission to submit proof

---

[7] G.R. No. 95641, 22 September 1994.
[8] SEC. 16. *Rights of the Data Subject,* Republic Act 10173 – Data Privacy Act of 2012
[9] Seven Brothers Shipping Corporation v. DMC-Construction Resources, Inc. G.R. No. 193914. November 26 2014.

of compliance that it complied with the orders of the Commission **within ten (10) days from the receipt of this Resolution.**

SO ORDERED.

Pasay City, Philippines;
17 December 2020.

(Sgd)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

(Sgd)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

BGM
Complainant

IPP.
Respondent

LEGAL DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission