Republic of the Philippines
NATIONAL PRIVACY COMMISSION

JVA

Complainant,

-versus-

NPC Case No. 19-498
(Formerly CID Case No. 19-498)
For: Violation of the Data Privacy Act of 2012

U-PESO.PH LENDING CORPORATION (UPESO)

Respondent.

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

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by Complainant JVA against Respondent U-PESO.PH Lending Corporation ("UPESO") for an alleged violation of R.A. 10173 ("Data Privacy Act").

The Facts

Complainant is a borrower who obtained a loan from UPESO through their online lending application. Prior to this complaint, Complainant had settled three (3) previous obligations. On 11 April 2019, Complainant successfully obtained his fourth loan from respondent and has made several partial payments. However, Complainant was not able to fully settle his obligation and after several follow-ups, he could no longer be contacted.[1]

Complainant alleges harassment, threats, and damage to his reputation caused by the Respondent.[2] He alleges that he learned about the violation from his friends who received messages from Respondent, thus:

> Nagmessage po yung mga kasama ko na hinahanap ako at may warrant na daw ako at makukulong na daw po ako.[3]

---

[1] Comment dated 15 November 2019, p. 2.
[2] Complaints-Assisted Form dated 8 July 2019, p. 3.
[3] *Ibid.,* at p. 4.

Explaining how these messages affected him, the Complainant states:

> Apektado po ako ng sobra. Hindi po ako makatulog at hindi ako makapasok sa trabaho dahil sab anta nila na sasampahin ako ng warrant at ipihiya [sic] sa trabaho ko.[4]

The Complainant indicates in the Complaint that he is seeking an Order to temporarily stop the processing of his data, because "his life and his work is affected."[5]

The parties were ordered to appear on 19 August 2019 for a Discovery Conference.[6] During the Discovery Conference, both parties manifested their willingness to explore the possibility of amicable settlement through mediation. The investigating officer caused the parties to sign an application for mediation and issued an order to mediate. The parties were endorsed to the mediation officer to commence the mediation proceedings.

Since the Complaint included an application for a temporary ban on the processing of his personal information, an order for summary hearing was issued on the same date. The initial date of the summary hearing was, however, rescheduled due to the pendency of the mediation proceedings.

During mediation, Complainant failed to appear without prior notice and justifiable reason for two (2) consecutive conferences. Thus, mediation was terminated without the parties arriving at a settlement and the complaint proceedings were resumed.[7]

At the Discovery Conference held on 06 November 2019, only Respondent appeared. They manifested that they will not be requiring any document or evidence from Complainant. Respondent was thus ordered to submit their responsive comment.

On the same day, a second Order for Summary Hearing was issued requiring the parties to appear on 29 November 2019 in connection with Complainant's application for a temporary ban on the processing

---

[4] *Ibid*., at p. 6.
[5] *Ibid.,* at p. 7.
[6] Order to Confer for Discovery dated 23 July 2019.
[7] Order for Resumption of Complaint Proceedings dated 06 November 2019.

of his information. Despite this Order, none of the parties appeared. An Order was thereafter issued requiring Respondent to submit its memorandum stating why a temporary ban should not be issued but Respondent failed to submit. There being no other submissions made, the investigation of the case was terminated and all pending matters were endorsed for adjudication.

Arguments of the Parties

In their Comment, Respondent argues for the dismissal of the Complaint due to the repeated non-appearance of Complainant during mediation proceedings, applying the Rules of Court provisions on the dismissal of cases due to the fault of plaintiff.[8] Respondent also avers that Complainant has not exhausted administrative remedies prior to the filing of the Complaint, as required under NPC Circular 16-04.[9]

Respondent further argues that there is no violation of the Data Privacy Act of 2012. In their Comment, they state:

> The Step-by-Step Process in Loan Application of UPESO shows that it is the Complainant herself who entered the personal information required by UPESO in order to process the loan including the information of the Contact Person/s as the case may be. Furthermore, the said process flow also shows that the Complainant has consented for UPESO to have access to her contacts on her phone.[10]

The Respondent cites several portions of the Terms and Conditions and Loan Agreement to illustrate Complainant's consent as their lawful basis to process.[11] Among those they cite are the provisions on Waivers and Data Privacy:

> 38) Finally the Loan Agreement with UPESO provides:
>
> > 12. Waivers. The Borrower hereby willingly, voluntarily, and with full knowledge of his right under the law, waives the right to confidentiality of information and authorize the Lender to disclose, divulge and reveal any such information relating to

---

[8] Rules of Court, Rule 17, Section 3, Rule 17.
[9] NPC Circular 16-04 ("Rules of Procedure of the National Privacy Commission") dated 15 December 2016, Section 4.
[10] Comment dated 15 November 2019, p. 6.
[11] *Ibid.*, at pp. 6-11.

> Borrower's loan availment, including events of default, for the purpose of, among others, client evaluation, credit reporting or verification and recovery of the obligation due and payable to the Lender under the terms and conditions of this Loan Agreement.
>
> In view of the foregoing, **the Lender may disclose, divulge and reveal the aforementioned information to third parties, including but not limited to** the Borrower's employer, credit bureaus, the Lender's affiliates, subsidiaries, agents, service providers, as well as any prospective assignee or transferee, rating agency, insurer, any such person, entity or regulatory body that may be required by law or competent authority.
>
> **The Borrower holds the Lender free and harmless from any and all liabilities, claims and demands of whatever kind or nature in connection with or arising from the aforementioned disclosure or reporting.**
>
> xxx
>
> 14. Data Privacy. The Borrower hereby acknowledges, agrees and consents that the Lender or its authorized officer may collect, store, process and dispose data about the Borrower by the Lender. Any information and data received from the Borrower by the Lender may be used and utilized by the Lender, **either directly or indirectly** in the performance of the terms under this Agreement. The Lender shall take reasonable precautions to preserve the integrity and prevent any corruption or loss, damage, or destruction of the said data of the Borrower.…[12]

The Respondent also denies any liability for the alleged harassment and threats to Complainant stating that:

> 48) The text messages shown by Complainant as proof of the alleged harassment or threats cannot be said to have come from the Respondent because they are not from the Respondent and the Respondent does not authorize and even prohibits its collectors from using such collection methods. As discussed

[12] Comment dated 15 November 2019, pp. 8-9. Emphasis supplied.

> above, [Respondent] does not authorize and even prohibits its collecting agents from making threats and harassing customers

Despite this, they ultimately maintain their main argument that hinges on their Terms and Conditions, thus:

> 49) Furthermore the allegations that the Respondent contacted the contacts of the Complainant and other contacts to ask them to remind the Complainant of her loan which are all within the terms and conditions that the Complainant has agreed and consented to.

Issues

1. Whether Respondent committed a violation of the Data Privacy Act that warrants a recommendation for prosecution; and
2. Whether a temporary ban should be issued against Respondent's processing of personal data

Discussion

It is necessary for the Commission to delineate the two (2) issues alleged by Complainant in his Complaint. The first one relates to his claims of harassment and threats based on the text messages he received. Copies of these messages were attached to his Complaint as evidence.[13] The second issue is his claim that he was not the only one who received messages about his failure to pay, but that other people also learned about his loan and his corresponding default. He alleges that his contacts relayed to him that the messages said that he could be arrested.[14]

On the first issue, it bears stressing that the Commission is not the competent authority to determine the allowable practices in debt collection by financing companies and lending companies. These are governed by other laws and regulations and not the Data Privacy Act.

The second issue raised, however, falls squarely within the scope of the Data Privacy Act. The fact that Complainant was told by his acquaintances that he was being hunted to be arrested indicates that Complainant's name and fact of having obtained a loan were disclosed

---

[13] Complaints-Assisted Form dated 8 July 2019, pp. 9-18.
[14] *Supra* note 3.

by Respondent to third parties. This is considered processing of personal information under the Data Privacy Act.[15] The right to data privacy or informational privacy, after all, is the right of individuals to control information about themselves.[16] It is this control, exercised by persons and entities other than the data subject, that the Data Privacy Act seeks to regulate.

As Respondent recognizes in its Comment, there is a set of criteria provided in the Data Privacy Act for the lawful processing of personal information.[17] In justifying its contacting of Complainant's contacts, Respondent cites consent as its lawful basis to process, stating:

> 39) The above-quoted provisions of the Loan Agreement shows that the Complainant, by agreeing to loan from UPESO, has also waives (sic) the right to confidentiality of information and authorize the Lender to disclose, divulge and reveal any such information relating to Borrower's loan availment, including events of default, for the purpose of, among others, client evaluation, credit reporting or verification and recovery of the obligation due and payable to the Lender under the terms and conditions of this loan agreement. **This means that the Complaint has consented for UPESO to contact her (sic) contact references and her contacts in case she continues to fail to pay her obligations with UPESO and answer the calls and messages of UPESO.**
>
> 40) Furthermore, the Complainant has given her consent for UPESO to access her contacts especially the reference contacts. It was even the Complainant who provided her contact references. These information also help UPESO make sure that the Complainant can be contacted in case she fails to pay her obligation with UPESO and refuse to answer the calls or reminders of UPESO.[18]

To determine whether the consent given by the data subject is proper, an examination must be made whether such consent was freely given, specific, informed, and an indication of will.[19] Respondent points to the fact that it was Complainant himself who provided his personal information to UPESO as proof of consent. While this may show that there was a positive act showing an indication of will on the part of the Complainant and that such act was freely given, it is not enough to

---

[15] *See* Republic Act No. 10173, Section 3(j).
[16] Vivares v. STC, GR No. 202666, 737 SCRA 92, 29 September 2014.
[17] *See* Republic Act No. 10173, Section 12.
[18] Comment dated 15 November 2019, p. 10. Emphasis supplied.
[19] *See* Republic Act No. 10173, Section 3(b).

show that the given consent was specific or informed. These two (2) requirements relate to the obligation of personal information controllers such as UPESO to comply with the general privacy principle of transparency.

As the Implementing Rules and Regulations of the Data Privacy Act explains:

> The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.[20]

In this case, Respondent's Loan Agreement provides that the borrower "willingly, voluntarily, and with full knowledge of his right under the law, waives the right to confidentiality of information and authorizes the Lender to disclose, divulge and reveal any such information relating to Borrower's loan availment, including events of default, for the purpose of, among others, client evaluation, credit reporting or verification and recovery of the obligation due and payable to the Lender under the terms and conditions of this Loan Agreement."[21]

The Loan Agreement also provides that "[a]ny information and data received from the Borrower by the Lender may be used and utilized by the Lender, either directly or indirectly in the performance of the terms under this Agreement."[22]

The test to determine if the personal information controller has complied with the general privacy principle of transparency is to examine whether an average member of the target audience could have understood the information provided to them. This does not, however, mean that the requirement to use clear and plain language necessitates using layman's terms in place of technical words at the risk of not capturing the complex concepts they represent. Rather, this requirement means that the information required under Sections 18(a) and 34(a)(2) of the Implementing Rules and Regulations should be

---

[20] Implementing Rules and Regulations of the Data Privacy Act, Section 18(a).
[21] Comment dated 15 November 2019, p. 8.
[22] *Ibid.,* at p. 9.

provided in as simple a manner as possible, avoiding sentence or language structures that are complex.[23] The information provided should be concrete and definitive; it should not be phrased in "abstract or ambivalent terms or leave room for different interpretations."[24]

Applied to the present case, one is hard-pressed to identify the extent of what the Respondent is allowed to disclose and when. The cited provision not only allows Respondent to disclose any information relating to Complainant's loan availment but the purposes enumerated, which normally would limit the type of and the instances when information can be disclosed, are so different from each other and open ended that they cease to provide any meaningful limits.

This is all the more true when the provisions of the loan agreement are read together with the information provided in the application itself when it asks for permission to access and use the contacts of borrowers. The screenshot attached to Respondent's Comment states:

> Hello! Upeso needs to safely process your data so that you are qualified for loan… Upeso should be authorized for contact person and text message. We will process information for build your network with your financial record. Without your permission, we won't reach any of your contact.[25]

From this, access to the borrower's contacts seem to be only for client evaluation or verification and not for the purpose of debt collection which is what Complainant alleges.

This vague, overbroad, and confusing language cannot be said to comply with the requirements of the transparency principle and its objective of providing meaningful information to data subjects to enable them to understand the purpose, scope, nature, and extent of processing of their personal information. Taken plainly, what Respondent obtained was blanket consent to process the information they acquired from Complainant and not informed consent to process specific information for a specified and limited purpose.

---

[23] *See* Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party (2017).
[24] *Ibid.*
[25] Comment dated 15 November 2019, Annex "B".

Aside from this, the authorization given to the Respondent to disclose should be read in the context of related provisions in the Loan Agreement: the borrower's waiver of his right to the confidentiality of his information and the borrower holding Respondent "free and harmless from any and all liabilities, claims and demands of whatever kind or nature in connection with or arising from the aforementioned disclosure or reporting."[26]

Without being informed of their rights under the Data Privacy Act, borrowers are asked to not only waive their rights under the Act but also, as to them, the obligations of Respondent as a personal information controller to, among others, ensure that there is lawful basis for its disclosures and to comply with the general privacy principles. Read in this light, the extent of Respondent's authority to disclose becomes not just broader but seemingly without any legal consequence as well.

While the Commission recognizes the principle of autonomy of contracts which allow parties to stipulate the terms of their agreement, this doctrine, however, comes with a qualification. Such stipulations, clauses, terms and conditions may be agreed upon by parties, as they may deem appropriate, provided only that they are not contrary to law, morals, good customs, public order or public policy.[27] This is not met in this case.

The Data Privacy Act declares it the policy of the State to protect the fundamental human right of privacy.[28] This classification by law of privacy as a human right – as opposed to property rights, or civil and political rights – necessitates a corresponding treatment and protection in law. The 1987 Constitution includes as a State Policy that "the State values the dignity of every human person and guarantees full respect for human rights."[29] The very first premise of the Universal Declaration of Human Rights, to which the Philippines is a signatory to, characterizes such human rights to be "inalienable."[30] All of these indicate that no entity can subject an individual's right to privacy – a fundamental human right - to a contractual waiver. Similar to other human rights, such as the right to life, it cannot be treated as property

---

[26] *Ibid.,* at p. 9.
[27] Bricktown Development Corp. v. CA, G.R. No. 112182, 12 December 1994.
[28] Republic Act No. 10173, Section 2.
[29] CONST. art. II, § 11.
[30] United Nations, *Universal Declaration of Human Rights (nd)* available at https://www.un.org/en/universal-declaration-human-rights/

that is subject to the rules of ownership and trade. Respondent, in their Comment, manifest such misconceptions. It is the mandate of the Commission to clarify this issue and prevent the future commodification of this declared human right.

Hence, contrary to what Respondent claims, they cannot rely on consent as its lawful basis to process the names and mobile numbers of Complainant's contacts for purposes of disclosing to them the status of his loan.

Despite this, however, the Commission is constrained to rely on the facts proven by Complainant in determining whether there is sufficient basis to warrant a recommendation for criminal prosecution.

The Supreme Court has held that in administrative proceedings such as this case, it is the complainant who carries the burden of proving their allegations with substantial evidence or such "relevant evidence that a reasonable mind might accept as adequate to support a conclusion."[31]

In this case, an examination of the records shows that Complainant failed to sufficiently prove that Respondent processed and disclosed his personal information to his companions.

Although Complainant attached screenshots of his conversations with agents of Respondents showing how he was harassed as a result of his failure to pay his outstanding loan, as discussed previously, these go into the allowable practices in debt collection and are not under the jurisdiction of this Commission.

What is relevant to the discussion on disclosure is Complainant's allegation that he received messages from other people informing him that he is being hunted and that he has a pending warrant of arrest. In his Complaint, he said "*Nagmessage po yung mga kasama ko na hinahanap ako at may warrant na daw ako at makukulong na daw po ako*."[32] Aside from this statement, however, Complainant has not presented any other piece of evidence that would show much less prove the existence of the messages that he received from his companions, the contents of the messages, and, more importantly, the actions of Respondent in relation to them.

---

[31] Ombudsman v. Fetalvero, G.R. No. 211450, 23 July 2018.
[32] Complaints-Assisted Form dated 8 July 2019, p. 5.

From the records, it is unclear how Respondent disclosed Complainant's personal information to his companions and what personal information, if any, was disclosed to them, whether Respondent communicated with them through calls or messages, or whether an actual person came to his workplace or residence looking for him armed with a warrant. Complainant did not even identify his companions.

The Commission cannot rely on allegations that are unsupported by fact or by law. It is bound to adjudicate following its Rules of Procedure, which provides:

> **Section 22.** ***Rendition of decision.*** – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.[33]

As the Supreme Court held in *Government Service Insurance System v. Prudential Guarantee,* "it is basic in the rule of evidence that bare allegations, unsubstantiated by evidence, are not equivalent to proof. In short, mere allegations are not evidence."[34]

Despite being given several opportunities to provide additional information at the two mediation conferences and the Discovery Conference scheduled on 6 November 2019, Complainant failed to appear before the Commission without notice or justification.

Given this, in the absence of sufficient evidence to support Complainant's allegation that Respondent disclosed his personal information to his companions, it cannot be said that Respondent committed an act that would constitute unauthorized processing[35] or processing for an unauthorized purpose.[36]

As to Complainant's application for a temporary ban, the NPC Rules of Procedure provides:

> Section 19. SECTION 19. *Temporary Ban on Processing Personal Data*. – At the commencement of the complaint or at any time before the

---

[33] NPC Circular No. 16-04 dated 15 December 2016 ("NPC Rules of Procedure"), Section 22. Emphasis supplied.
[34] G.R. No. 165585, 20 November 2013, *citing* Real v. Belo, 542 Phil. 109 (2007).
[35] Republic Act No. 10173, Section 25.
[36] Id., at Section 28.

> decision of the National Privacy Commission becomes final, a complainant or any proper party may have the National Privacy Commission, acting through the investigating officer, impose a temporary ban on the processing of personal data, if on the basis of the evidence on record, such a ban is necessary in order to preserve the rights of the complainant or to protect national security or public interest.
>
> a. A temporary ban on processing personal data may be granted only when: (1) the application in the complaint is verified and shows facts entitling the complainant to the relief demanded, or the respondent or respondents fail to appear or submit a responsive pleading within the time specified for within these Rules; xxx

Considering the findings above, Complainant's application for the issuance of a temporary ban is denied.

WHEREFORE, all the above premises considered, the Complaint is hereby **DISMISSED**.

This is without prejudice to the filing of appropriate civil, criminal or administrative cases against the Respondent before any other forum or tribunal, if any.

SO ORDERED.
Pasay City, 9 June 2020.

(sgd)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(sgd)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(sgd)
JOHN HENRY DU NAGA
Deputy Privacy Commissioner