Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: FLI OPERATING ABC ONLINE LENDING APPLICATION	**NPC 19-910** *For violation of the Data Privacy Act of 2012*

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

DECISION

AGUIRRE, D.P.C.

This concludes the investigation conducted by the Commission following the Fact-Finding Report prepared by the NPC Task Force on Online Lending Mobile Applications[1] (Task Force) dated 29 August 2019, which serves as the Complaint (Complaint) pursuant to Rule IV of NPC Circular 16-04.[2] The Complaint alleged violations of Republic Act (R.A.) 10173 or the Data Privacy Act of 2012 (DPA) by FLI, operating the ABC online lending application.

The Complaint summarized its findings with the following recommendations:

> On the basis of this fact finding report, there is sufficient ground to establish that FLI operating the ABC online lending application, as represented by their respective board of directors, committed acts in violation of the DPA, specifically:
>
> 1. Sections 11, 12, 13, 16, 20, and 21, for processing without complying with the requirements of the DPA and for failing to adhere to the principles of

[1] This Commission issued, on 14 May 2019, Privacy Commission Special Order Nos. 028 and 032-A, creating and reconstituting the NPC Task Force on Online Lending Mobile Applications. Said Special Orders explicitly named the seven (7) staff officers as members thereof. The Task Force is responsible to investigate the influx of complaints against several online lending companies for a potential violation of the DPA. The Task Force is also mandated to provide options and recommendations for the Commission to immediately address concerns of the public. In accomplishing this function, the Task Force submitted a fact-finding report on several online lending companies, one of which is the herein Respondents.

[2] NPC Circular 16-04. Rules of Procedure of the National Privacy Commission. Dated 15 December 2016.

Transparency, Legitimate Purpose and Proportionality;
2. Sections 25, for Unauthorized Processing;
3. Section 28, for Processing for Unauthorized Purposes;
4. Section 31, for Malicious Disclosure;
5. Section 32, for Unauthorized Disclosure.[3]

The Complaint

The Complaint made the following allegations:

> From 06 July 2018 to 31 July 2019, the NPC received a total of 689 complaints against several online lending applications. This constitutes around 55% of the total complaints filed before the NPC. This does not include around 2,666 similar concerns raised through email or social media which were not formally filed as complaints. These numbers are unprecedented, potentially qualifying any violation of the DPA as large scale processing. The complaints bring to focus online lending applications, which can be downloaded and installed in mobile phones. These applications are then used to facilitate loan transactions between companies and their clients, the data subjects. The applications provide a platform for the collection of all types of personal information from various device models, which information related not just to the clients of the company, but extends to persons in their contact lists. Evident from the complaints are common statements from data subjects conveying how downloading these applications lead to a disruption in the lives of others, in violation of individual rights and freedoms.
>
> Considering the number of data subjects involved, the seriousness of the allegations, and the risks of harm to data subjects, NPC, on its own initiative, investigated the circumstances surrounding the possible violations of ABC online lending application. Significantly, the number of complaints filed against this lending application have already reached a total of 113 complaints as of 31 July 2019.[4]

The Complaint provides that affidavits and sworn statements of the complainants against the company operating the ABC lending application were evaluated. It states that individual complainants

---

[3] Fact-Finding Report dated 29 August 2019, p. 23.
[4] *Id* at 1 .

relayed the incidents in the course of their transaction with the company based on their personal knowledge, own experiences, and supporting documents.[5] The Complaint found that the following statements about the company have been consistently made:

> 1. Personal information from complainants' mobile phonebook / directory/contact list were used by ABC to contact third persons, without their consent or authority;
> 2. Personal information about the data subjects, both unwarranted and false information were discussed to third persons, which included friends, relatives, co-workers and superior of the data subject. These persons were often told that the data subjects named them as co-makers or character references, and there were some reports that they were even asked to settle the loan in behalf of the data subjects;
> 3. Agents or representatives of ABC used personal information about data subjects and others in their contact list to damage the reputation of data subjects, or to harass, threaten or coerce them to settle their loans;
> 4. Methods used in processing personal information were unduly intrusive, including posting in social media of personal and sensitive personal information of data subjects or even subjecting their contacts to threats and harassment; the personal information processed were excessive or otherwise used for purposes beyond what is necessary or authorized under their agreement.[6]

The Complaint cites several specific allegations from various statements in different complaints, supported by screen captures by the complainants, such as:

> In CID Case No. 19-F-415, complainant reveals that prior to installing the ABC application, it required permissions to access her contact list and their phone numbers, Facebook and Google accounts, and others. Furthermore, Complainant in CID Case no. 19-G-522 alleges that ABC even hacked the photos in her phone, among other identifying information. Complainant also received the following text message:
>
> > *Before you sue us, we already send (sic) a text blast to all of your contacts. Posting your uploaded picture from Loan apps to social media.*

---

[5] *Id* at 2.
[6] *Id*, at 3.

> *We know your home address, office address, and your ugly face. But you never know us, that take times and you make effort and time for that. Right now we already send text blast with false information regarding you.*
>
> *We hacked your info, and we can send false information regarding this. All your contacts, messages, and in and outcall activity we have information. You're done due to swearing with us.*
>
> *Goodluck with your privacy law.*[7]

xxx

> While some agents make it appear that they are contacting the complainant's phone list to aid in collection, an ABC agent in CID Case No. 19-G-573 admitted that said "text blast" was for the purpose of ruining complainant's reputation:
>
> > *Hello Ma'am / Sir, your loan to ABC has been overdue. We will inform your relatives and friends to urge the repayment (overdue debts) when you has been overdue. Please cherish your reputation among friends and relatives, cherish your credibility and repay as soon as possible. Do reply if you don't want us to call of your contact references. This is the special collections team.*[8]

The Complaint included a Technical Report, prepared by the Information Technology Officers of the Task Force, in its Annexes to corroborate the statements of the various complainants, particularly those alleging that the application was able to access their contact lists. By extracting the AndroidManifest.xml, which describes the essential information about applications, Android build tools, the Android operating system, and Google Play, the Technical Report revealed that the ABC application required forty-four (44) permissions, seven (7) of which were classified as dangerous permissions.[9]

The Technical Report explained dangerous permissions as those that "cover areas where the app wants data or resources that involve the user's private information or could potentially affect the user's stored data or the operation of other apps. For example, the ability to read the

---

[7] *Ibid.*
[8] *Id at* p. 4.
[9] ABC App Preliminary Technical Report, 09 August 2019, P.4, citing https://developer.android/com/guide/topics/permissions/overview#dangerous_permissions

user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app. Until the user approves the permission, your app cannot provide functionality that depends on that permission. To use a dangerous permission, your app must prompt the user to grant the permission at runtime."[10]

On 30 August 2019, the Commission issued an Order to File an Answer pursuant to Section 24 of the NPC Rules of Procedure, directed to Respondent FLI and its responsible officers specifically ML, CW, KF, JG, HJL, and BSJ. with its dispositive as follows:

> WHEREFORE, premises considered FLI and its responsible officers specifically, ML, CW, KF, JG, HJL, and BSJ, are all instructed to file their respective Answers to the allegations in the Fact-Finding Report.
>
> The Answer should be filed no later than ten (10) days from receipt of this Order. In cases where the respondent or respondents fail without justification to submit an Answer or appear before the National Privacy Commission when so ordered, this Commission shall render its decision on the basis of available information.[11]

On 16 September 2019, an Appearance and Omnibus Motion was filed by the QG Law Offices for FLI and Respondents ML, CW, and BSJ., which prayed for the following:

> WHEREFORE, premises considered, it is prayed unto the Honorable Office, that an Order be issued:
>
> a) Upon receipt of the Motion, to suspend proceedings, pending resolution of the instant Omnibus Motion; and
> b) Initiating a Mediation Proceeding.
>
> As a matter of extreme prudence, it is also prayed for the Honorable Office to issue an Order giving the Respondents an additional time of fifteen (15) days or until 30 September 2019 within which to file their respective answer or such other responsive pleading.

---

[10] *Ibid.*
[11] Order to File an Answer, dated 30 August 2019.

On 17 September 2019, a Motion for Extension to File Answer with Entry of Appearance was filed by GNGA & Associates for Respondents KF, JG and HJL, likewise requesting for an extension, thus:

> WHEREFORE, premises considered, respondents most respectfully prays unto this Honorable Commission that the Motion for Extension of Time for a period of ten (10) days from 16 September 2019 or until 26 September 2019 within which to file the necessary pleading, BE GRANTED in the interest of substantial justice and the entry of appearance of the undersigned counsel be duly noted.

Thereafter, additional Motions for Extensions were filed by counsels for both parties.

On 26 September 2019, counsel for Respondents KF, JG and HJL prayed for an additional ten (10) days or until 6 October 2019 to file their Verified Answer.

On 27 September 2019, counsel for Respondent FLI, the QG Law Offices, filed their Withdrawal of Appearance.

On 30 September 2019 the law firm of DSBMR filed an Entry of Appearance with Motion for Further Extension of Time to File Answer for Respondent FLI. They moved for an additional period of fifteen (15) days or until 15 October 2019 within which to file their answer.

On 01 October 2019, the law firm of DSBMR entered its appearance as counsel for Respondents ML, CW, and BSJ and prayed for an additional period until 15 October 2019 within which to file its Answer.

On 07 October 2019, the Commission issued a Resolution that granted all the requests of the Respondents for additional time to file their Answers, finding that these were all duly filed within the allowable period of time.

As regards the prayer of Respondents ML, CW, and BSJ for the initiation of mediation proceedings, the Commission denied this and cited NPC Circular 16-04 which states thus:

> Section 26. Mediation officer. – The Commission shall assign a mediation officer to assist the complainant and respondent to reach a settlement agreement, **provided that no settlement is allowed for criminal acts.**

The Answers

On 11 October 2019, Commission received a Verified Answer from Respondents KF, JG, and HJL through their counsel.

On 15 October 2019, an Answer was filed by Respondents FLI, ML, CW, and BSJ, through their counsel.

On 08 January 2020, the Commission issued an Order stating that the Answer by Respondents FLI, ML, CW, and BSJ did not provide evidence to support the following arguments:

> 18. It is not true that FLI and its directors / officers have "knowledge of the practices of its agents or other people clothed with the authority to collect outstanding loans" because, in fact, the collection agents who committed debt-shaming practices did so without the knowledge of FLI and its directors/officers. It then follows that without any knowledge of FLI and its officers, the respondents could not have consented to the acts of the collection agents, whether expressly or impliedly.
>
> 19. FLI recognizes that even if the collection of loan repayments was outsourced to a third-party service provider, it was not amiss in its duty to ensure that the third-party service provider/processor and the collection agents under its employ comply with the DPA and the basic principles of personal data protection. In particular, collection agents are supposed to use only a provided computer software to contact the user/borrower of third parties. They were not allowed to use their personal phones to contact the user or other parties, which is what these collection agents did.[12]

[12] Order dated 8 January 2020.

The Commission thereafter ordered the Respondents to substantiate the allegations through the submission of documents such as :

> 1. The official company document containing the functional statements of each director and officer of the corporation; and
> 2. The outsourcing agreement with the third-party service provider / processor referred to in their Answer as of 29 August (the date of the Fact-Finding Report) containing the provisions they mentioned in Paragraph 19.[13]

On 10 February 2020, the Commission received a Motion for Extension of Time to File Compliance from Respondents FLI, ML, CW, and BSJ citing communication and logistics issues arising from the ongoing outbreak in China caused by the 2019 Novel Coronavirus.

On 20 February 2020, Respondents FLI, ML, CW, and BSJ filed their Compliance with the following Annexes:

4.1 Annex "A", a copy of the by-laws of FLI, as approved by the Securities and Exchange Commission.
4.2 Annex "B", an original copy of the Affidavit executed by the General HR manager at FLI, detailing the actual functions of the board of directors of FLI within the organization and how members of the board of directors of FLI were not privy to the manner and method of loan collection that was being adopted by the employees of CSA.
4.3 Annex "C", a copy of the Master Service Agreement executed by FLI and CSA, to whom FLI had outsourced the loan collection function on 12 October 2018.
4.4 Annex "D", the Code of Conduct of CSA, issued on May 2019, which identifies "bringing in and using mobile phones by unauthorized employee in the work area or while on while on duty" as an offense under the category "acts of inefficiency, negligence, and violation of work standards or company policies".

---

[13] *Ibid.*

> 4.5 Annex "E" is a copy of the presentation of FLI on its ongoing efforts for data collection and usage as well as optimization of data collection systems.
> 4.6 Annex "F", a copy of the certification issued by FLI' external legal counsel, QG Law Offices, which states that out of 69 complaints pending against FLI before the Honorable Commission, 25 complaints have already been settled.[14]

On 20 August 2020, the Commission noted this submission and stated in an Order:

> Under NPC Circular No. 16-04 or the NPC Rules of Procedure, the Commission may order the conduct of a clarificatory hearing if, in its discretion, additional information is needed to make a Decision.
>
> After due consideration of the evidence presented as of the date of this Order, the Commission finds that a clarificatory hearing is needed for the proper disposition of this case.
>
> **WHEREFORE,** in the interest of conducting an exhaustive investigation and pursuant to the NPC Rules of Procedure, the Commission hereby resolves to **ORDER** Respondents to appear for a clarificatory hearing on **24 SEPTEMBER 2020 at 2:00 PM**, in relation to its submissions for the case of NPC 19-910**.**

The Commission later received a Notice of Withdrawal filed by the law firm of DSBMR dated 21 September 2020, which stated:

> The law firm of SBMR respectfully manifests it is withdrawing as counsel for FLI, ML, CW, AND BSJ (collectively, the "Respondents") in the above-captioned case, pursuant to the instructions that it received from the RESPONDENTS.

The Commission likewise noted the Entry of Appearance with Urgent Motion to Reset Clarificatory Hearing filed by the QG Law Offices dated 22 September 2020.

Following these submissions, the Commission reset the clarificatory hearing to 01 October 2020, guided by NPC Advisory No. 2020-02 or "Guidelines on the Use of Videoconferencing Technology for the

[14] Compliance dated 20 February 2020.

Remote Appearance and Testimony of Parties Before the National Privacy Commission."

On 01 October 2020, the Commission conducted a Clarificatory Hearing (Hearing), pursuant to Section 21 of NPC Circular No. 16-04. Respondent FLI and the individual Respondents ML, CW, and BSJ were represented by Atty. QAL and Atty. ET from the QG Law Offices, while the individual Respondents KF, JG and HJA were represented by Atty. FG from the law firm of GNGA & Associates.

Following the commitments of the counsel for Respondent FLI, ML, CW, and BSJ to submit documents to substantiate their claims during the Hearing, the Commission issued an Order dated 01 October 2020 requiring them to submit the following:

1. The diagram of the organizational structure of FLI Lending, Inc. that was supposed to be attached as Annex "A" of the Affidavit of MTA, attached as Annex "B" of the Compliance filed by FLI Lending, Inc. on 20 February, 2020;
2. Board Resolutions, if any, discussing the following matters:
    - Authorizing ML, President, on behalf of FLI Lending, Inc., to enter into the Master Service Agreement with CSA dated 12 October 2018 ; and
    - Appointing the officers of FLI Lending, Inc. or authorizing the President to make appointments for the positions of General Manager, General HR Manager, and other officers of FLI Lending, Inc.
3. Documentation on the current status of the Master Service Agreement between FLI Lending, Inc. and CSA;
4. Details surrounding the presentation attached as Annex "E" of the Compliance filed by FLI Lending, Inc. on 20 February, 2020, such as: who delivered the presentation, to whom it was delivered, when it was delivered, etc.;
5. Documentation on the number of complaints filed with FLI Lending, Inc. in relation to the collection practices of CSA;
6. Documentation on the number of CSA employees terminated as a result of the complaints filed with FLI Lending, Inc.;
7. Details on the utilization, if any, by FLI Lending, Inc. of the following provisions in the Master Service Agreement dated 12 October 2018;

- Article VI, Section 2. *Unprofessional Practices in the Performance of the Service and Breach of the Contract; Penalties.*
- Article VIII, Section 3(d). *Duration of the Agreement and Termination; Termination; Performance evaluation yields an unsatisfactory result.*

8. Documentation of the issue relayed by FLI Lending, Inc. regarding alleged scammers who represent themselves to the public as agents of ABC, including any notices issued to the public informing them of this issue; and
9. Information on the background of individual respondents ML, CW, and Bernard BSJ.

On 16 October 2020, FLI filed a Partial Compliance with an attached Memo from CSA. dated 01 October 2019. FLI also requested for an extension of thirty (30) days or until 15 November 2020 to produce and submit the other documents required by the Commission.

Considering the circumstances raised by FLI and in the interest of an exhaustive investigation, the Commission granted the requested extension for submission of the required documents.

The Respondents filed their Compliance dated 26 November 2020, and submitted the following documents:

a. Disciplinary reports transmitted by CSA to FLI in relation with potential data privacy violations committed by CSA which proves that FLI mandated CSA to comply with their undertaking and obligation under the MSA;
b. Sample employment contract between CSA and its employees showing that the collection employees undertook to comply with CSA company policies specifically data privacy policies;
c. FLI and CSA Master Service Agreement with Confidentiality and Non-disclosure Agreement which proves that there is a contract between FLI and CSA pertaining to CSA's compliance with prevailing laws specifically data privacy laws;
d. A sample CSA employment contract with its employees; and
e. Master Service Agreement between FLI and CSA.[15]

[15] Compliance dated 26 November 2020.

Issues

The issues in this case are as follows:

1. Whether procedural due process was observed;
2. Whether the proceedings should be held in abeyance during the pendency of the other complaints;
3. Whether Respondent FLI violated Sections 11, 12, 13, 16, 20, and 21 of the DPA for processing without complying with the requirements of the DPA and for failing to adhere to the principles of Transparency, Legitimate Purpose, and Proportionality;
4. Whether Respondent FLI committed Unauthorized Processing of Personal Information and Sensitive Personal Information under Section 25 of the DPA;
5. Whether Respondent FLI committed Processing for Unauthorized Purposes under Section 28 of the DPA; and
6. Whether the penalty shall be imposed upon the Board of Directors, as responsible officers who by their gross negligence, allowed the commission of the crime.

Discussion

I. Procedural Due Process was Observed

In the Answer filed by Respondents FLI, ML, CW, and BSJ, they questioned the procedure in the *sua sponte* investigation, thus:

> 43. The Fact Finding Report admits that "[e]xaminations of publicly accessible information and the initial technical evaluation on FLI and their online lending application, ABC, show that the company has failed to demonstrate compliance with the DPA." This statement clearly shows that the Fact-Finding Report did not consider the side of FLI.[16]

The Commission takes the opportunity to discuss the nature of a *sua sponte* investigation.

[16] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019. Page 13.

The NPC is an independent body created to administer and implement the provisions of the DPA of 2012. As provided in Section 7 of the DPA, the NPC has Rule-Making, Advisory, Public Education, Compliance and Monitoring, Complaints and Investigation, and Enforcement powers[17] to enable it to protect the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth.[18]

Section 7(b) of the DPA specifically states that it is the mandate of the NPC to:

> (b) Receive complaints, **institute investigations**, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: Provided, That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act; (Emphasis supplied)

In the exercise of its rule-making power and to flesh out the provision above, the NPC issued NPC Circular 16-04[19] on 15 December 2016. Section 3 thereof provides who may file complaints with the Commission:

> SECTION 3. Who may file complaints. – The National Privacy Commission, *sua sponte,* or persons who are the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of the Data Privacy Act, may file complaints for violations of the Act.

Further, Section 23 of the NPC Circular 16-04 provides for the NPC's power of original inquiry:

---

[17] *See,* RA 10173, Section 7.
[18] *See, Id.,* Section 2.
[19] NPC Circular 16-04. NPC Rules of Procedure. Dated 15 December 2016.

> SECTION 23. Own initiative. – Depending on the nature of the incident, in cases of a possible serious privacy violation or personal data breach, taking into account the risks of harm to a data subject, the Commission may investigate on its own initiative the circumstances surrounding the possible violation. Investigations may include on-site examination of systems and procedures. If necessary, the Commission may use its enforcement powers to order cooperation of the personal information controller or other persons, with the investigation or to compel appropriate action to protect the interests of data subjects.

The NPC Circular 16-04 provides for the procedure in instances of *sua sponte* investigations, thus:

> SECTION 24. Uniform procedure. – The investigation shall be in accordance with Rule III of these Rules, provided that the respondent **shall be provided a copy of the fact-finding** report and given an opportunity to submit an answer. In cases where the respondent or respondents fail without justification to submit an answer or appear before the National Privacy Commission when so ordered, the Commission shall render its decision on the basis of available information.[20]

The Fact-Finding Report, therefore, serves as the Complaint in *sua sponte* investigations and is not yet a Decision by the Commission. Contrary to the claim of the Respondents that they were not afforded their right to due process, this Commission provided Respondents an opportunity to provide their side. This is precisely why the Commission, in an Order dated 30 August 2019, directed Respondents to file an Answer in response to the allegations in the Fact-Finding Report.

II. The proceedings should not be held in abeyance during the pendency of the other complaints.

In the Answer filed by Respondents FLI, ML, CW, and BSJ, they alleged that:

---

[20] I*bid,* Emphasis supplied.

> 46. The proceedings in the instant case also appear to be premature because there are, in fact, individual complaints involving actual, individual complainants which remain pending at various stages before the Honorable Commission.
>
> 47. The Fact-Finding Report mentions that there are a "total of 113 complainants as of 31 July 2019 which have been filed with the Honorable Commission against FLI.
>
> 48. First, out of the 113 complaints, FLI has been made aware only of 54 complaints and have received files, orders, and pleadings only for 54 complaints. These 54 complaints are in different stages of proceedings and some of them have already been subject to compromise agreement that was approved by the Honorable Commission while some of them are subject precisely to mediation proceedings.
>
> 49. Second, it is possible that the Honorable Commission could even lose the basis for the instant case, which was supposedly the 113 complaints, if for example, these individual complaints are eventually dismissed. In line with due process and fairness, the Honorable Commission should have first allowed the individual complaints against FLI [to] be threshed out by the Complaints and Investigation, before creating a fact-finding committee, also from within the Honorable Commission, which would investigate the same circumstances and cases. The Fact-Finding Report has effectively prejudged the pending individual complaints.
>
> xxx
>
> 51. Thus, the reasonable approach would be to let the individual complaints run their course and hold the instant case in abeyance.[21]

The Commission refers once more to the abovementioned Sections 3, 23, and 24 of NPC Circular 16-04 which provides the nature of a *sua sponte* investigation.

The fact that there exist hundreds of pending cases before the Commission against Respondent FLI is no bar to the filing of the present case. The Commission notes that the pending cases and the case on hand involve different parties, different causes of action with different prayers of relief.

---

[21] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019. Page 14.

The focus of this investigation is the functionality of the ABC application in relation to the categories of personal information collected upon its download and the extent of further processing vis-à-vis what is declared by Respondent FLI in their Credit Agreement and Privacy Policy. The citation of allegations from different pending cases illustrate that the effects of these functionalities coupled with the lack of transparency are not imagined but have seriously harmful effects in the lives of their borrowers, who are considered data subjects under the DPA.

III. Sections 11, 12, 13, 16, 20, and 21 of the DPA may be bases for determining violations under Chapter VIII of the DPA.

Respondents FLI, ML CW, and BSJ emphasized in their Answer that the violation of the above-captioned provisions does not give rise to criminal liability, thus:

> Sections 11, 12, 13, 16, 20, and 21 of the DPA cannot be the basis for criminal prosecution. The Honorable Commission could hold respondents liable only administratively for violations of the provisions, if any, based on the provision in the DPA that the Honorable Commission shall have the power to merely "receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matter affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report" (Section 7(b) of the DPA).
>
> Further, the DPA does not provide for any penalties, whether imprisonment or fine, for failure to comply with Sections 11, 12, 13, 16, 20, and 21 thereof.[22]

While it may be true that these provisions do not fall under Chapter VIII of the DPA, which provides for the prohibited acts, these

[22] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, page 2.

provisions notably cover the General Data Privacy Principles, Criteria for Lawful Processing of Personal Information, Sensitives Personal Information and Privileged Information, Rights of the Data Subject, Security of Personal Information, and Principle of Accountability. These consist of the principles and concepts in the DPA that serve as the substantive bases for determining violations under Chapter VIII which incur criminal liability.

IV. Respondent FLI committed Unauthorized Processing of Personal Information and Sensitive Personal Information under Section 25 of the DPA

In determining whether a violation of Section 25 of the Data Privacy Act occurred, three elements must be established with substantial evidence:

1. The accused processed the information of the data subject;
2. The information processed was personal information and sensitive personal information;
3. That the processing was done without the consent of the data subject, or without being authorized under this act or any existing law.[23]

A. The accused processed the personal information of the data subjects.

The first two elements for Unauthorized Processing are undisputed, as Respondent FLI admits to processing personal and sensitive personal information. In their Answer, they cite their Credit Agreement in claiming that it obtained it borrowers' consent to "collect, process, and retain" personal information such as, but not limited to, the name, address, phone number, mobile phone number, financial information, credit status information, phone contacts and other related

[23] NPC Case No. 17-018, Decision dated 15 July 2019.

information. [24] It further cites it Privacy Policy which states that ABC collects personal information provided to them which may include additional information about the borrower to help ABC get to know them better, such as "gender, age, date of birth, nationality, professional associations and registration numbers, information about how [they] use [their] products, and demographic information."[25]

The DPA defines personal information as, "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[26] Undeniably, the name, address, phone number, financial information, credit status information and phone contacts of the ABC borrowers, when put together, will serve to identify specific individuals. The gender, date of birth and nationality of the borrowers, on the other hand, are considered sensitive personal information under the enumeration provided in the DPA.[27]

The DPA enumerates a series of processing activities to emphasize that this covers the different stages of a data lifecycle. Processing is defined by the DPA as, "any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data."[28]

Respondent FLI, through the ABC application, processed the information of the borrowers when it accessed personal information

---

[24] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, at 6.
[25] *Ibid.*
[26] RA 10173, Section 3 (g)
[27] R.A. 10173, Section 3(l) *Sensitive personal information* refers to personal information:
(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
(4) Specifically established by an executive order or an act of Congress to be kept classified.
[28] R.A. 10173, Section 3(j).

through app permissions such as READ_CONTACTS and READ_EXTERNAL_STORAGE.[29] The processing, however, did not end there given the apparent retention of information which made it possible for Respondent FLI, through collection agents, to inform third parties about the borrower's outstanding debt. This will be discussed subsequently.

B. The processing was done without the consent of the data subject, or without being authorized under the DPA or any existing law.

The DPA provides for lawful criteria to process personal information. For the subject personal information in this case, the lawful criteria are found under Section 12[30] and 13[31] of the law.

---

[29] Pondo Peso App Preliminary Technical Report, 09 August 2019.

[30] 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:
(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;
(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
(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.

[31] SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
(b) The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

Respondent FLI claims the consent from the borrowers as its lawful criteria. In its Answer, it argued that it has obtained the consent of the borrowers prior to the collection and processing of the contact list, thus:

> 22. First of all, FLI obtains the prior consent of the borrowers to the collection and processing of their respective contacts list.
>
> 23. It provides a Credit Agreement and Privacy Policy which data subjects need to agree to:
>
> *Credit Agreement*
> *Part II (e)*
> *e) Subject to the provisions of the Privacy Policy, the User agrees, consents and authorizes ABC to collect, process and retain personal information of the User such as, but not limited to: name, address, phone number, mobile phone number, financial information, credit status information, phone contacts and other related information* ***in order to achieve the purpose of this Agreement.***
>
> *Part II(g)*
> *g) ABC ensures that personal information of the User shall be protected and secured from unauthorized access, breach, disclosure or sharing. The User agrees, consents and authorizes ABC to use, manage, disclose personal data, information, archives, data sources to Third Parties* ***in order to achieve the purpose of this Agreement*** *including but not limited to collection, data verification, use telecom operators, among others. Subject to the limitations as set forth under the Data Privacy Act and its Implementing Rules and Regulations.*[32]
>
> *Privacy Policy*
>
> *ABC collects personal information you* ***provide us****, which may include:*
> *(i) contact information, such as your name, company name, job title,*

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing;
(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or
(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.

[32] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019 at 7. Emphasis supplied.

> *address, e-mail address, and phone number; (ii) additional information about you to help us get to know you better, such as gender, age, date of birth, nationality, professional associations and registration numbers, information about how you use our products, and demographic information; (iii) comments, questions, requests and orders you make;*
>
> *(iv) financial information needed to process loans and payments, such as credit card or account information or other banking information; (log-in information, including, if applicable, social media account information for log-in purposes, if applicable; (vi) information about your preferences, such as your preferred methods of communication and product types in which you are interested (viii) phone contacts in your device needed* ***for collection purposes, if in case the information provided in the credit agreement is false, invalid or otherwise not responsive to our collection attempts.***
>
> 24. During user sign-up in the app, the user is required to click "Agree" to the Privacy Policy. Then, when the user decides to actually make a loan, the borrower is required to click "Agree" to the Credit Agreement and Disclosure Statement. Thus, the consent of the borrower to the collection and processing of his contacts list is obtained based on a specific purpose disclosed to the user. The consent is given expressly as well.[33]

According to Answer of Respondent FLI, the user is required to click "Agree" to the Privacy Policy during sign up in the application. Upon making a loan, the borrower is also required to click "Agree" to the Credit Agreement. In this regard, Respondent FLI states the consent of the user or borrower is expressly given and obtained based on a specific purpose disclosed to them.

At this juncture, the Commission takes the opportunity to emphasize the difference between a Privacy Policy and a Consent Form, considering the different requirements for these under the DPA.

This issue has been clarified in the Commission's Advisory Opinions, thus:

> [T]here is also a need to determine and clarify the distinction between a privacy policy and securing the consent of the data subject for the processing of his or her personal information. **Being a mere notice, it is emphasized that the privacy notice is**

[33] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019 at 7. Emphasis supplied.

> **not equivalent to consent.** This document is an embodiment of the observance of the data privacy principle of transparency and upholding the right to information of the data subjects.
>
> The principle of transparency mandated by the DPA dictates that 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 access and understand, using clear and plain language.
>
> On the other hand, obtaining consent from the data subject for the purposes of processing his or her personal data has different requirements altogether.
>
> Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information.
>
> When the processing of personal information is based on consent, the PIC must obtain the consent in relation to the declared purpose for processing. The consent must likewise be evidenced by written, electronic, or recorded means.
>
> **We reiterate that the mere posting of a PIC's privacy policy or notice and requiring the consumers to agree thereon via the online platform does not equate to obtaining the consent of the data subject for purposes of processing his or her personal information as required under the law.**
>
> [T]he fact that the data subject must agree to a privacy policy or notice fails to meet the requirement of meaningful consent. A "bundled" consent, for instance, will generally not suffice as the data subject is not empowered to make a true choice.[34]

In this case, Respondent FLI requires the borrowers to click "Agree" to the Privacy Policy, aside from the Credit Agreement, and subsequently relies on this as basis for the supposed consent obtained from the borrowers. Given this, the Commission evaluates both the Privacy Policy and Credit Agreement according to the requirements of the DPA for consent.

---

[34] Advisory Opinion 2018-013. Dated 18 April 2018. Emphasis supplied.

i.Respondent FLI committed unauthorized processing for its retention of contact lists beyond its declared purpose.

The Complaint included a Technical Report that examined the functionalities and permissions of the ABC application, in order to corroborate the collective allegations from the individual complaints.

> Based on the declared permission on Google Play Store, the extracted AndroidManifest.xml file and the Google Developer definition, the Examiners concluded that ABC app is:
>
> Capable of **COLLECTING USER'S PRIVATE INFORMATION** that potentially affect the user's stored data and the operation of other apps once installed on an Android device. Thru the android.permission.READ_CONTACTS permission, ABC app is capable in reading the user's contact data; thru the adroid.permission.READ_EXTERNAL_STORAGE, ABC app is capable in reading any data from the external storage of the device such as microSDs;

In its Answer, Respondent FLI gave its rationale behind all the Dangerous Permissions used in the ABC application, thus:

> 34. xxx
>
> c. READ_CONTACTS permission is necessary because reference contacts are populated during the loan application with a drop-down box. The reference contacts cannot be manually typed as this would potentially give way for users to provide bogus numbers. This also prevents instances wherein potential users would use a burner phone in order to have a loan application approved. One of the verification steps undertaken by FLI is the examination of the phone contact list to see if the phone is newly purchased or if there are no or next to minimal contacts presently registered in the phonebook. If the contacts list reviewed appears to be unscrupulous or is otherwise made up, the loan application will be denied outright.
>
> 37. It may also be noted that the access of FLI to the contacts of the user allows FLI to conduct its due diligence and credit investigation on potential customers. Thus, the processing of the

> contacts information of the user carries a legitimate purpose and is proportional to that purpose.[35]

The Commission finds this explanation to be insufficient and inconsistent with actual events that have led to the numerous complaints filed with the NPC.

Respondent FLI claimed that the READ_CONTACTS dangerous permission is justified by its need to determine, at the point of loan application, whether the mobile phone was newly purchased in the event of a few entries in the contact list. This is part of their verification process which is done prior to the approval of the loan. The issue remains, however, as to why these contacts were retained and kept in a form that allowed further processing even after the loan application's approval.

Such retention is considered as a processing activity under the DPA which must also be supported by consent or other lawful criteria.

The cited Credit Agreement shows that the declared purpose for retention and other processing activities was "in order to achieve the purpose of this Agreement." This cannot be a basis for consent.

Consent is defined as, "any freely given, specific, **informed** indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so."[36]

The declaration "in order to achieve the purposes of this Agreement" is circuitous and is an overbroad phrase that does not conform with the general privacy principle of transparency. This cannot support a claim of validly obtained consent, hence consent cannot be FLI' basis for lawful criteria. As held by the Commission in a decided case[37]:

---

[35] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019. Page 11.
[36] R.A. 10173, Section 3(b). Emphasis supplied.
[37] NPC Case 19-450. Dated 09 June 2020.

> [There is a need to] emphasize the need for personal information controllers, such as Respondent, to inform their data subjects of the purpose of the processing of their personal information in "clear and plain language." The requirement to use clear and plain language does not mean using layman's terms to substitute technical words at the risk of not capturing the complex concepts they represent….[38] The information provided should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different interpretations.[39]

The cited Privacy Policy in Respondent FLI' Answer also cannot be the basis for acquiring consent to retain the borrowers' entire contact lists. The Privacy Policy declared that its purpose for processing phone contacts was "for collection purposes."[40]

Regardless of whether Respondent FLI hinges on the purposes of verification, loan application, or debt collection, the retention of the borrowers' entire contacts lists far exceeds these purposes.

The Data Privacy Act of 2012 states thus:

> SEC. 11. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.
>
> Personal information must, be:
>
> xxx
>
> (d) Adequate and not excessive in relation to the purposes for which they are collected and processed;…[41]

This principle is further explained in the Implementing Rules and Regulations of the Data Privacy Act of 2012, which states, "personal

---

[38] *See,* Guidelines on transparency under Regulation 2016/679 of the Article 29 Working Party (2017).
[39] *Ibid.*
[40] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, at 7.
[41] R.A. 10173, Section 11(d).

data shall be processed **only if the purpose of the processing could not reasonably be fulfilled by other means**."[42]

The availability of far less intrusive measures, such as a reliance on a limited number of reference contacts provided by the borrower, demonstrates that the measures employed by Respondent FLI were disproportionate to the aim they sought to achieve.

Personal information that is processed in excess of what is proportional to the declared purpose amounts to Unauthorized Processing which is a punishable act under Section 25 of the DPA.

Lastly, the Commission notes that the Privacy Policy only refers to personal information "provided by the borrower" to the ABC application. It does not contemplate accessing the entire contact list stored in the mobile phone that was not specifically provided by the borrower. While the Privacy Policy refers to "collection purposes", this cannot be taken as a blanket authority for excessive collection and unauthorized retention of information.

ii. Respondent FLI committed unauthorized processing in its use of the borrowers' contacts for their debt collection.

The Complaint incorporates the findings of the Technical Report in its allegations, thus:

> The READ_CONTACTS permission make it possible for FLI and their agents to call and send messages to the people in the complainant' contacts lists.
>
> The fact that the ABC is also able to obtain access to storage devices of complainants through READ_EXTERNAL_STORAGE permission also confirms the allegations of some complainants about the reported threats made by agents that they can view complainants; photos and can post them anywhere they want.

[42] IRR, § 18(c), emphasis supplied.

> ABC is also capable of determining the approximate and precise geographical location of the users the Global Positioning System (GPS) through cellular network information and wi-fi connection. Again, this correlates with the allegations of some complainants that collection agents knew of their work and home addresses and exact locations.
>
> ABC is capable of manipulating information on the device through the WRITE_CALENDAR and WRITE_EXTERNAL_STORAGE dangerous permissions.
>
> Finally, ABC is capable of manipulating application will not fully function if any one of these dangerous permissions is not approved by the user.[43]

As summarized in the Complaint, the above dangerous permissions used by the ABC application translated into these actual experiences by data subjects:

> On 6 February 2019, NPC received a complaint docketed as CID Case No. 19-B-056 filed against ABC. Complainant alleges that ABC hacked her cellphone and obtained the details of her contacts. According to complainant, she received complaints from her people and clients that ABC have (sic) been disturbing them.
>
> xxx
>
> Complainant in CID Case No. 19-G-613 states that persons who called her phone, some of whom were not in her phone book, were even contacted by ABC.
>
> Complainant in CID Case No. 19-G-634 narrates that ABC contacted her team leader and sent the latter a photo of herself holding her Unified Multipurpose ID. [44]
>
> xxx
>
> While some agents make it appear that they are contacting the complainant's phone list to aid in collection, a ABC agent in CID Case No. 19-G-573 admitted that said "text blast" was for the purpose of ruining complainant's reputation:

---

[43] Fact-Finding Report, at 11.
[44] Fact-Finding Report, at 3.

> *Hello Ma'am / Sir, your loan to ABC has been overdue. We will inform your relatives and friends to urge the repayment (overdue debts) when you has been been overdue. Please cherish your reputation among friends and relatives, cherish your credibility and repay as soon as possible. Do reply if you don't want us to call of your contact references. This is the special collections team.*[45]

It is worth noting that Respondent FLI has never disputed the fact that the names of their borrowers and the fact of overdue payment have been disclosed to the people in their mobile contact lists.

Instead, Respondent FLI argues in its Answer that information on the use of the borrowers' personal information for loan collection purposes was provided to the borrowers in the Credit Agreement and Privacy Policy, thus:

> 25. The Credit Agreement and Privacy Policy expressly provide that the borrower's contacts list on his mobile phone will be obtained by FLI and such information will be used for purposes of loan collection, in case the borrower himself is unresponsive to FLI' collection attempts.
>
> 26. Even the Fact-Finding Report quotes the foregoing provisions. While the "third parties" to whom the personal information is disclosed is not specified, the user could reasonably assume that these third parties would be engaged in activities in line with the purposes stated for the disclosure to them – "collection services, background investigation, skip tracing, among others".
>
> **27. Based on these, a user of the app who reads and agrees to the Privacy Policy could reasonably conclude and expect that first, the app will be able to collect the details on his phone's contact list, and second, FLI could communicate with those contacts for collection purposes.**

The Commission disagrees. Borrowers would not have been able to reasonably expect Respondent FLI to use their phone contacts other than the reference contacts they submitted, especially because the Privacy Policy is worded this way:

> ABC collects **personal information you provide us,** which may include… (vii) phone contacts in your device needed for

[45] *Id. at* 4.

> collection purposes, if in case the information provided in the credit agreement is false, invalid or otherwise not responsive to our collection attempts.[46]

The Commission, in a previous Decision, has discussed the concept of reasonable expectation of privacy in relation to informational privacy:

> While the two-part test under *Katz* and *Ople* should now be construed taking into consideration the provisions of the Data Privacy Act, this concept of "reasonable expectation" may still be useful in addressing issues concerning informational privacy in relation to what controllers and processors may legitimately do. In this regard, this concept of "reasonable expectation" is considered to determine the legitimacy of the additional processing **by examining whether such further processing is compatible with the original business purpose communicated to the data subject and not beyond what the data subject may reasonably expect as to the purpose, scope, manner, and extent of the processing of their personal data**.[47]

Applying the foregoing concept to this case, the burden cannot be placed on the borrowers to have known what the ABC application was capable of, based on the information provided to them. The borrowers could have only expected that their entire contact lists will be utilized for collection purposes if they had known the scope, manner, and extent of Respondent FLI' processing of their information in the first place. This is all the more true considering the broad language used in the declared purposes of the Credit Agreement, i.e. "in order to achieve the purposes of this agreement." The declared purpose of "collection purposes" in the Privacy Policy likewise does not contemplate the indiscriminate messaging of family, friends, and acquaintances, considering the Policy referred to personal information "provided" by the borrowers. In the case of the ABC application, this pertains only to the reference contacts supplied upon the loan application.

This is bolstered by the fact that the Securities and Exchange Commission (SEC), in a Memorandum dated 19 August 2019, prohibited unfair debt collection practices of financing companies and

---

[46] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019, at 6-7. Emphasis supplied.
[47] *See*, EU General Data Protection Regulation, Recital 47, cited in NPC Case No. 17-047.

lending companies such as the disclosure of the names and other personal information of borrowers who allegedly refuse to pay debts,[48] except for circumstances provided in the same Memorandum. It also expressly provides for the confidentiality of information.[49] Given these, the Commission strongly disagrees with the claim that "the user of the app who reads and agrees to the Privacy Policy could reasonably conclude and expect that first, the app will be able to collect the details on his phone's contact list, and second, FLI could communicate with those contacts for collection purposes".

Respondent FLI, for good measure, states that even if there were acts of unauthorized processing, these cannot be attributed to Respondent FLI, thus:

> 28. If the collection agents who reach out to the borrowers' contacts, "damage the reputation of data subjects, or harass, threaten, or coerce them to settle their loans," as the Fact-Finding Report claims, then these acts are indeed unauthorized by the data subjects (i.e., beyond the consent they had given to FLI) but at the same time, these were neither authorized by FLI. Acts that damage the reputation of data subjects or coerce them to settle their loans are personal acts of the collection agents who, when they do these, act beyond the authority given to them by the data subjects and FLI.

Respondent FLI cannot be absolved of the violations of the DPA on the argument that the processing in relation to the collection was subcontracted to CSA.

In fact, during the Hearing, the Commission was able to elicit the actual arrangement between Respondent FLI and its collection agent, CSA. It sought clarification about one of the attachments in the Compliance submitted by FLI, specifically the slide about the "ABC Product Description."[50] It noted that there was a department in FLI for a "Collector," as described in their company organization structure:

> Part 1.1 Company Organizational Structure

---

[48] SEC Memorandum Circular No. 18. Prohibition of Unfair Debt Collection Practices of Financing Companies (FC) and Lending Companies (LC). Dated 19 August 2019. Section 1(d).
[49] *Ibid.,* at Section 2.
[50] Annex "E" is a copy of the presentation of FLI on its ongoing efforts for data collection and usage as well as optimization of data collection systems

- **COLLECTOR. Responsible for the collection of overdue users, sending reminders through calls and SMS.**
- QUALITY ASSURANCE. Enforces rules developed with aid from the Legal Department, by checking the call recordings of the collections, and imposing sanctions when warranted.
- LEGAL. Evaluates contracts and helps QA with inspections to determine collection rules. Handles customer complaints when it comes to questions of law.[51]

The counsel for Respondent FLI answered that the collector is an outsourced party, CSA.[52]

Even if it were true that the Collection Department was outsourced to a service provider, Respondent FLI' own Organizational Structure reveals that it considered debt collection as an integral part of its business, meriting its own department. During the Hearing, the counsel for Respondent FLI admitted to the Commission that the "Collector" department had a supervisor to whom reports were submitted. [53]

The DPA defines a Personal Information Controller as "a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf."
In this case, Respondent FLI is the corporation that operates the ABC online lending application, which is the service that collects and processes personal information of its borrowers. Thus, Respondent FLI is the Personal Information Controller. It cannot escape the fact that it was in the position to control and exercise discretion over what personal information is processed and the extent of its processing. It is likewise registered with the National Privacy Commission as a Personal Information Controller belonging to the Online Lending Sector.[54]

---

[51] *Ibid*. Emphasis supplied.
[52] *See*, Transcript p. 8.
[53] *See,* Transcript at 23-25.
[54] Fact-Finding Report, Annex B.

The DPA provides for the Principle of Accountability and concomitant obligations for Personal Information Controllers, thus:

> Section 21. Principle of Accountability. Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing. xxx
>
> (a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.
> (b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.[55]

The arguments of Respondent FLI, therefore, must fail for lack of basis in the law.

C. Respondent FLI did not violate Section 28 (Processing for Unauthorized Purposes) of the DPA.

Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes is committed when:

1. A person processed information of the data subject;
2. The information processed is classified as personal information or sensitive personal information; and
3. The processing of personal information is for purposes not authorized by the data subject, or otherwise authorized under this Act or under existing laws.

As discussed previously, the first and second elements are met in this case. The third element, which should differentiate Processing for

---

[55] R.A. 10173, Section 21.

Unauthorized Purposes under Section 28 from Unauthorized Processing under Section 25, does not apply in this case.

Although seemingly similar, the application of principles in statutory construction would require a differentiation between the two (2) provisions:

> Moreover, under the maxim *noscitur a sociis*, where a particular word or phrase is ambiguous in itself or is equally susceptible of various meanings, its correct construction may be made clear and specific by considering the company of words in which it is founded or with which it is associated. This is because a word or phrase in a statute is always used in association with other words or phrases, and its meaning may, thus, be modified or restricted by the latter. The particular words, clauses and phrases should not be studied as detached and isolated expressions, but the whole and every part of the statute must be considered in fixing the meaning of any of its parts and in order to produce a harmonious whole. **A statute must be so construed as to harmonize and give effect to all its provisions whenever possible.** In short, every meaning to be given to each word or phrase must be ascertained from the context of the body of the statute since a word or phrase in a statute is always used in association with other words or phrases and its meaning may be modified or restricted by the latter.[56]

Applying the foregoing principle in this case, the Commission notes that the qualifier "unauthorized" attaches to "processing" under Section 25, and to "purposes" under Section 28. Thus, Section 28 contemplates processing that was initially authorized either by consent of the data subject or some other lawful basis, but subsequently became invalid when the processing went beyond the consent given or the authority provided by law.

In this case, the dangerous permissions in the ABC application allowed it to retain information without consent or other lawful basis in the DPA. Since such processing activity was never authorized either by consent or some other authority in law, it was illegal from the beginning, hence the third element does not apply in this case.

---

[56] Chavez v. JBC, et. al. G.R. 202242. Dated 17 July 2012.

D. The penalty shall be imposed upon the Board of Directors, as responsible officers who by their gross negligence, allowed the commission of the crime.

Having established that Respondent FLI has committed Unauthorized Processing under Section 25 of the DPA, the Commission refers to Section 34 of the law:

> SEC. 34. *Extent of Liability.* – If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their **gross negligence**, allowed the commission of the crime. If the offender is a juridical person, the court may suspend or revoke any of its rights under this Act. If the offender is an alien, he or she shall, in addition to the penalties herein prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee and lie or she is found guilty of acts penalized under Sections 27 and 28 of this Act, he or she shall, in addition to the penalties prescribed herein, suffer perpetual or temporary absolute disqualification from office, as the case may be.[57]

Respondents FLI, CW, ML and BSJ, in their Answer, argue that they should not be liable for criminal acts unless their active participation can be proven, thus:

> 1. With respect to Sections 25, 28, 31, and 32 of the DPA, **a criminal offense will be committed only by individuals who actually committed the criminal act.**
>
> 2. FLI and its directors and officers such as ML, CW, and BSJ. could not be held liable for criminal violations of Sections 15, 28, 31, and 32 of the DPA because they did not at all engage or participate in, or consent to, (a) unauthorized processing; (b) unauthorized disclosure of personal information of the app users (collectively, the "Criminal Acts".)
>
> 3. If FLI, as a company, adopted policies that promoted and call for, or was aware of, the commission of the Criminal Acts, then the company and its responsible directors and officers would have been correctly impleaded as respondents.

[57] R.A. 10173, Section 34. Emphasis Supplied.

> 4. However, there is no showing by the Honorable Commission or the complainants that FLI observed or is observing a policy that promotes and calls for the commission of the Criminal Acts. Neither is there proof that FLI and its officers knew of the Criminal Acts;
>
> xxx
>
> 18. It is not true that FLI and its directors / officers have "knowledge of the practices of its agents or other people clothed with the authority to collect outstanding loans" because, in fact, the collection agents who committed debt-shaming practices did so without the knowledge of FLI and its directors / officers. It then follows that without any knowledge of FLI and its officers, the respondents could not have consented to the acts of the collection agents, whether expressly or impliedly.[58]

The DPA is clear, however, that the liability of the responsible officers in cases where the offender is a corporation does not rely on active participation alone. Gross negligence is explicitly stated in the DPA as a ground for criminal liability.

The Supreme Court has consistently defined gross negligence as "the negligence characterized by the want of even slight care, or by acting or omitting to act in a situation where there is a duty to act, not inadvertently but willfully and intentionally, with a conscious indifference to the consequences, insofar as other persons may be affected. It is the omission of that care that even inattentive and thoughtless men never fail to give to their own property."[59]

In this case, the Board of Directors of FLI did not deny the fact that a Master Service Agreement was entered into between Respondent FLI and CSA, with the President as the signatory. The Board of Directors should have been aware of the terms in this Agreement, considering that it concerns a vital aspect of their operations as a lending company.

Consequently, they should have been aware that the provisions of the Master Service Agreement contradicted the principles in the DPA. It

---

[58] Answer by Respondents FLI, ML, CW, and BSJ dated 15 October 2019 at p. 3.
[59] Fernandez v. Office of the Ombudsman, G.R. No. 193983. 14 March 2012.

included a provision that sought to surrender its accountability as a Personal Information Controller to CSA, thus:

> Article I
> Scope of Service
>
> Section 5. Methods of Work. **The service shall be performed by the Contractor in accordance with means and methods of work determined solely by it,** on the understanding that the company shall exercise control over the contractor only in regard to the results of the service.[60]

This provision is contrary to DPA which is very clear that the subcontracting of personal information by Personal Information Controllers cannot include the responsibility to prevent unauthorized processing, thus:

> Section 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.[61]

Despite this provision, Respondent FLI still was not entirely powerless under the Master Service Agreement. This responsibility under law could still have been exercised by Respondent FLI through certain provisions in the Master Service Agreement which contained remedies that they should have exercised as the Personal Information Controller after voluminous complaints were filed against it, such as:

> Article VI.
>
> **Unprofessional practices in the performance of the service and breach of contract.**
>
> xxx

[60] Compliance dated 20 February 2020, Annex "C". Emphasis supplied.
[61] R.A. 10173, Section 14. Emphasis Supplied.

> Section 2. PENALTIES. The CONTRACTOR acknowledges that the unprofessional performance on the SERVICE may compromise and damage the goodwill and public reputation of the COMPANY. In addition to the COMPANY's remedies under this Agreement or under the general civil law for unprofessional performance of the SERVICE, the COMPANY shall likewise be entitled to be compensated for the damages caused thereby whether committed by the CONTRACTOR itself or any of its representatives, agents, or employees.
>
> In case of suit by the COMPANY against the CONTRACTOR arising from such unprofessional practices, or any other breach or violation of any provision of this Agreement, the COMPANY shall be entitled to recover from the CONTRACTOR any and all expenses incurred by the COMPANY in investigating the matter, recovering any amounts lost to the COMPANY, or completing or rectifying defective works or service.[62]

During the Hearing, however, the counsel for Respondent FLI stated that they were not aware of a specific instance of an action taken by FLI against CSA.[63]

In its Compliance dated 26 November 2020, the counsel for Respondent FLI submitted supposed Disciplinary reports from CSA in relation with potential data privacy violations committed by their collection agents.[64]

In the four (4) submitted Disciplinary Report Forms, however, the offenses cited were simply "using the phone" and "exploring the post loan system to get the number of the user." These do not describe the unprofessional debt collection practices that have led to the hundreds of complaints filed before the Commission. These Disciplinary Report Forms also do not state what action was taken by either CSA or FLI, either through reprimands, suspensions, or terminations. The Commission cannot consider these submissions as proof of FLI' responsibility in preventing unauthorized processing by its subcontractors.

---

[62] Fact-Finding Report, Annex "B". Emphasis in the original.
[63] *See,* Transcript at 39.
[64] Compliance dated 26 November 2020, Annex 1.

The Commission likewise notes the Verified Answer of Respondents KF, JG, and HJL which claims that they should be absolved based on the supposed the fact that they are nominal directors, thus:

> 3.1 On 19 June 2018, respondents acted as nominee stockholders for the incorporation of respondent FLI before the Securities Exchange Commission.
>
> xxx
>
> 3.3. Thereafter and until the present time, respondents were not involved directly or indirectly with respondent FLI management and the day to day operations of the company.
>
> xxx
>
> 4.1. Respondents did not participate in the management of respondent FLI as well as the operation of its ABC online lending business.
>
> xxx
>
> a. In the case at bar, respondents although listed as board of directors and office or respondent FLI, they did not participate directly or indirectly in the management and operation of the ABC online lending business.
>
> xxx
>
> b. Respondents cannot also be considered to have acted in gross negligence in allowing the alleged commission of the acts for, as already emphasized, they are not involved in the management and daily operations of FLI Hence, they could not have allowed the alleged commission of the acts complained of.[65]

The fact remains that all the directors were incumbent members of the Board of Directors of FLI during the date of the violations. Members of the Board are presumed to participate as such. While the individual Respondents were given opportunities to dispute this presumption, they never did so.

The Commission has formerly ruled in the NPC Case 19-605, thus:

---

[65] Verified Answer dated 4 October 2020, p. 2.

In the case of *Alfredo Ching vs. Secretary of Justice*[66], the Supreme Court held that the Board of Directors shall be held criminally liable for violations committed by the corporation when by reason of the latter's negligence to supervise its employees, it has caused the corporation to commit acts in violation of the law, *viz:*

> "Though the entrustee is a corporation, nevertheless, the law specifically makes the officers, employees or other officers or persons responsible for the offense, without prejudice to the civil liabilities of such corporation and/or board of directors, officers, or other officials or employees responsible for the offense. The rationale is that such officers or employees are vested with the authority and responsibility to devise means necessary to ensure compliance with the law and, if they fail to do so, are held criminally accountable; thus, they have a responsible share in the violations of the law.
>
> xxx xxx xxx
>
> A crime is the doing of that which the penal code forbids to be done, or omitting to do what it commands. A necessary part of the definition of every crime is the designation of the author of the crime upon whom the penalty is to be inflicted. When a criminal statute designates an act of a corporation or a crime and prescribes punishment therefor, it creates a criminal offense which, otherwise, would not exist and such can be committed only by the corporation. But when a penal statute does not expressly apply to corporations, it does not create an offense for which a corporation may be punished. On the other hand, if the State, by statute, defines a crime that may be committed by a corporation but prescribes the penalty therefor to be suffered by the officers, directors, or employees of such corporation or other persons responsible for the offense, only such individuals will suffer such penalty. Corporate officers or employees, through whose act,

[66] G.R. No. 164317, February 6, 2006.

> default or omission the corporation commits a crime, are themselves individually guilty of the crime.
>
> The principle applies whether or not the crime requires the consciousness of wrongdoing**. It applies to those corporate agents who themselves commit the crime and to those, who, by virtue of their managerial positions or other similar relation to the corporation, could be deemed responsible for its commission, if by virtue of their relationship to the corporation, they had the power to prevent the act.** Moreover, all parties active in promoting a crime, whether agents or not, are principals. Whether such officers or employees are benefited by their delictual acts is not a touchstone of their criminal liability. Benefit is not an operative fact."

> Further, the Board of Directors has the duty of diligence. As provided by the Supreme Court in one case, directors or officers of a corporation are expected to exercise reasonable care and prudence in the performance of their duties and responsibilities.[67]

It is the persons behind FLI who allowed the harassment of its borrowers through the Master Service Agreement that surrendered all accountability to its subcontractor. These persons provided the approvals for the ABC application's functionalities and dangerous permissions. They were the ones who lacked supervision over the representations it made to all of FLI' borrowers.

Had the ABC application confined itself to the purposes FLI itself declared in the Privacy Policy, the collection agents would have only had access to the reference contacts whom the borrowers willingly indicated in their application.

Time and again, the Commission emphasizes the role that Personal Information Controllers play in ensuring that the innovation and growth that happens in the Philippines continue to abide by the laws

---

[67] NPC Case No. 19-605.

and ethical practices, leading to products and services that are free from any doubt on their security and informational privacy.

WHEREFORE, all these premises considered, this Commission hereby:

1. **FINDS** that Respondent FLI and its Board of Directors, namely, ML, CW, KF, JG, HJL, as responsible officers, have violated Section 25 of the Data Privacy Act; and

2. **FORWARDS** this Decision and a copy of the pertinent case records to the Secretary of Justice, recommending the prosecution of the Respondents for the crimes of Unauthorized Processing under Section 25 of the Data Privacy Act, for its further actions.

SO ORDERED.

City of Pasay, Philippines;
17 December 2020.

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

QG LAW OFFICES
Counsel
Counsel for FLI, ML, CW, and BSJ

GNGA& ASSOCIATES
Counsel for Respondents KF, JG and HJL

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission