Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: FAMILYHAN CREDIT CORPORATION

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by Familyhan Credit Corporation

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

NPC SS 20-001
For: Violation of the Data Privacy Act (DPA) of 2012

ORDER

This resolves the Recommendations of the National Privacy Commission (NPC)'s Complaints and Investigation Division (CID)[1] which may be summarized as follows: 1) To initiate an investigation on Familyhan Credit Corporation (Familyhan) and its responsible officers and members of the board, MTR, VBV, JPV, AA, and MDA[2] for reported violations of Sections 26 and 30 of the Data Privacy Act of 2012 (DPA); 2) To subject Familyhan to the appropriate compliance and enforcement orders; and 3) In the interim, to order the immediate take down of its database from being accessible online.

The Facts

On 16 June 2020, the CID received notarized complaints from Global Migration Assistance alleging that the personal information of five (5) individuals was disclosed maliciously and without authority.[3]

On 23 July 2020, the CID received an email from a user account named familyhan.whisteblower (fhw@abcdef.com) with two (2) attached excel files named database1 and database2.

[1] Fact Finding Report dated 05 October 2020.
[2] Familyhan Credit Corporation General Information Sheet for the Year 2018, dated 14 March 2019 (latest on file with the SEC).
[3] Preliminary Report dated 03 September 2020.

According to CID's Fact Finding Report (Report), the file named database1.csv contained six thousand ninety two (6,092) records with the following personal information:

1. Full Name;
2. Passport Number; and
3. Current addresses of borrowers based in Hong Kong and Singapore.

While the file named database2.csv contained six thousand seventy (6,070) records with the following personal information:

1. Full Name;
2. Passport Number;
3. Email address;
4. Current addresses of borrowers based in Hong Kong and Singapore; and
5. Residential addresses of borrowers in the Philippines.[4]

On 07 August 2020, the CID received another email from the familyhan.whistleblower user account . The email message included a link which showed a proof-of-concept video to show that the database of Familyhan, as well as the steps to gain access to it, are publicly accessible.[5]

On 25 August 2020, the NPC's Legal and Enforcement Office (LEO) issued a Mission Order[6] for its personnel with the following actions to be taken:

1. Verify the alleged exposed Familyhan database and secure a copy, if possible;
2. Cross reference all acquired databases and evaluate number of data subjects affected; and
3. Prepare a preliminary report based on the findings.

On even date, the CID was able to secure a copy of the database believed to be that of Familyhan borrowers by following the steps provided in the video and the email. The database contained six

[4] *Supra,* note 1.
[5] *Ibid.*
[6] Mission Order CID 20-001 dated 25 August 2020.

thousand five hundred fifty three (6,553) records of individuals with the following personal information:

1. Full Name;
2. Passport Number; and
3. Current addresses of borrowers based in Hong Kong and Singapore.[7]

On 03 September 2020, the CID cross-referenced the databases acquired and found that the names of borrowers are identical across all three (3) database files. The names of the individuals who filed the notarized complaints with the Commission were also found in the abovementioned three (3) database files.[8]

On 17 September 2020, the CID found a post on the Facebook page of the Employers and Migrants Against Familyhan Credit Corp, dated 16 August 2020, showing a three (3)-minute and fifteen seconds (3:15) video guide on how easy it is to access Familyhan's database. The video guide was the same video that the anonymous tipster provided the Commission.[9]

Discussion

The NPC is an independent body created to administer and implement the provisions of the DPA. 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[10] to enable it to protect the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth.[11]

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,

[7] *Supra,* note 1.
[8] Preliminary Report dated 03 September 2020.
[9] *Supra,* note 1.
[10] *See,* RA 10173, Section 7.
[11] *See, Id.,* Section 2.

> 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, otherwise known as the Rules of Procedure of the National Privacy Commission (NPC Rules of Procedure) 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 Rules of Procedure provides for the NPC's power of original inquiry:

> "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."

In addition, the DPA explicitly provides for the Commission's power to issue Cease and Desist Orders:

> Section 7 (c). Issue cease and desist orders, impose a temporary or permanent ban on the processing personal information, upon finding that the processing will be detrimental to national security and public interest.

This was reiterated in the Implementing Rules and Regulations (IRR) of the DPA:

> Section 9. Functions. The National Privacy Commission shall have the following functions:
>
> xxx
>
> f. Enforcement. The Commission shall perform all acts as may be necessary to effectively implement the Act, these Rules, and its other issuances, and to enforce its Orders, Resolutions, or Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:
>
> xxx
>
> 4. Issuing cease and desist orders, or imposing a temporary or permanent ban on the processing of personal data, upon finding that the processing will be detrimental to national security or public interest, or if it is necessary to preserve and protect the rights of data subjects.

From these, it can be seen that three (3) elements are required for this Commission to validly exercise its power to issue a Cease and Desist order:

1. There must be a finding of a practice or act that an entity is doing, threatening, or about to do, which constitute a violation of the DPA, its IRR, or other related issuances;
2. Such act or practice is or will be detrimental to national security or public interest, or the issuance is necessary to preserve and protect the rights of the data subject; and
3. The commission or continuance of such act or practice, unless restrained, will cause grave and irreparable injury to a data subject.

The Report details how the personal and sensitive personal information of more than six thousand (6,000) data subjects was accessed by unauthorized persons using simple steps that can be done through a web browser. The CID was able to confirm the accessibility of the database by following the steps as indicated in the email and in the Facebook group. Based on these, the Report states:

> In sum, there is sufficient ground to support the finding that FamilyHan violated the following penal provisions of law:
>
> > Section 26 of the DPA. Accessing Personal Information and Sensitive Personal Information Due to Negligence – (a) Accessing personal information due to negligence shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than five hundred thousand pesos (Php 500,000.00) but not more than two million pesos (Php 2,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.
> >
> > (b) Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than five hundred thousand pesos (Php 500,000.00) but not more than four million pesos (4,000,000.00) shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under this Act or any existing law.
> >
> > xxx
> >
> > Section 30 of the DPA. Concealment of Security Breaches Involving Sensitive Personal Information – The penalty of imprisonment one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php 500,000.00) but not more than One million pesos (Php 1,000,000.00) shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach.

The Report finds that there is reason to believe that Familyhan should have known or had a reasonable belief that a security breach of their borrowers' personal information occurred; that it has not made the required notification under NPC Circular 16-03 (Personal Data Breach Management); that there is evidence to support a finding of possible negligence for failure to secure the database and prevent unauthorized access; and that it has not registered with this Commission, despite meeting the criteria for mandatory registration.

These findings clearly allege a privacy violation or personal data breach, with risks of harm to the data subjects, the situation contemplated in the provision for *sua sponte* investigation under the NPC Rules of Procedure.

These findings also exhibit that the entity is doing, threatening, or about to do, acts and practices which constitute a violation of the DPA. Furthermore, considering that, as of the date of the Report, the database remains to be accessible online, it is necessary for the Commission to preserve and protect the rights of the data subjects involved by restraining the continuing processing of personal data by Familyhan Credit Corporation on their database. The negative effects caused by the breach of more than six thousand (6,000) data subjects' records, as well as the real risks of injury from further processing, cannot be overlooked by this Commission.

WHEREFORE, premises considered, Familyhan Credit Corporation and its responsible officers and members of the board, MTR, VBV, JPV, AA, and MDA are hereby ordered to:

1) File a **COMMENT,** within ten (10) days from receipt of this Order, on the allegations in the attached Fact Finding Report, pursuant to Section 24 of the NPC Rules of Procedure; and

2) **CEASE AND DESIST** from the processing of personal data on their database until the Commission issues a decision on the submission of the Comment, which shall be made no more than thirty (30) days from the expiration of the period to file a Comment or of the termination of the clarificatory hearing if one is held, pursuant to NPC Circular No. 20-02.

SO ORDERED.

City of Pasay, Philippines;
15 October 2020.

(sgd)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

(On Official Business)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(sgd)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

FAMILYHAN CREDIT CORPORATION
Batangas

MTR
Rizal

VBV
Rizal

JPV
Rizal

AA
Rizal

MDA
Rizal

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