Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: SAINT LOUIS UNIVERSITY **NPC BN 20-116**
x----------x

ORDER

LIBORO, P.C.:

Before this Commission is the Compliance and Motion for Reconsideration dated 24 March 2021 and 29 March 2021, respectively, which was submitted by Saint Louis University (SLU) to comply with the Resolution dated 21 January 2021 issued by this Commission.

Facts

On 21 January 2021, this Commission issued a Resolution with the following dispositive portion:

> **WHEREFORE**, premises considered, Saint Louis University is hereby **ORDERED** to comply with the following **within five (5) days from receipt of this Resolution**:
>
> (1) **SUBMIT** its full breach report with the contents required under NPC Circular No. 16-03 and the Resolutions dated 23 July 2020 and 21 September 2020;
>
> (2) **NOTIFY** the affected data subjects and **SUBMIT** proof of compliance thereof, including the proof of receipt of the data subjects of such notification; and
>
> (3) **SHOW CAUSE** in writing why it should not be held liable for failure to submit a full breach report and notify the affected data subjects within the required period under NPC Circular No.16-03 and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.

The Resolution dated 21 January 2021 containing a Show Cause Order was issued by the Commission because at that time, the reports submitted by SLU to NPC were not compliant with the previous

Resolutions dated 23 July 2020 and 21 September 2020 issued by this Commission and with NPC Circular No. 16-03 and SLU have not yet notified the affected data subjects despite previous orders from the Commission.

At that time, for SLU, there was no reason to believe that identity fraud could be perpetrated and that there is no reason to believe that the personal data involved have been acquired by an authorized person and that there is no real risk of serious harm to the data subjects. They have also implemented measures to address such incident and to prevent similar incidents from happening in the future. Thus, they considered the matter closed and for them, there is no more reason to inform any data subject.

In the said Resolution dated 21 January 2021, the Commission, in consideration with the likelihood of harm or negative consequences on the affected data subjects, and the number of data subjects involved, resolved that notification to the affected data subjects is necessary. This Commission emphasized that the exemption of notification to the affected data subject is not to be determined by the Personal Information Controller but by the Commission.

In compliance with the Resolution dated 21 January 2021, SLU conducted a reinvestigation of the breach and resubmitted a Final and more comprehensive breach report of the incident which is for evaluation of the Compliance and Monitoring Division.

The investigation revealed a Letter dated 02 July 2020 addressed to SLU by its Service Provider, PhilSmile, outlining the scope and the extent of the software malfunction, how to identify the data subjects affected, the data that was affected, and the recipients of the data

Based thereon, SLU was able to definitively identify those exposed and those who received the data. These were broken down into two categories: 1) The data subjects affected by the software malfunction whose data were exposed, consisting of fifty nine (59) individuals; and 2) The persons who were the recipients of the sensitive personal information who logged into the system between 22 to 25 June 2020, consisting of fifty four (54) individuals.

SLU's Data Protection Committee reached out to the affected data subjects and the recipients of the data and asked all fifty nine (59) and fifty four (54) of them to execute non-disclosure agreements in relation to the breach.

All fifty four (54) individuals who were the recipients of the sensitive personal information, have agreed to enter and have in fact entered into a non-disclosure agreement with SLU through a Google Forms site, whereby they expressed their assent to the terms and conditions of the Non-Disclosure Agreement (NDA) through a click-wrap mechanism.

Moreover, SLU has also recognized the right to indemnification of the affected data subjects whose data were exposed to the fifty four (54) persons and has granted them indemnification by waiving their registration and IT fees in the tuition fees for AY 2020-2021 of the data subjects, also through a click-wrapped NDA through Google Forms.

According to SLU, through the execution of the NDAs, it has already ensured that the risk of harm or negative consequence to the data subjects will not materialize and the breach is now under control.

SLU also stated that it has not returned to nor activated the PhilSmile student management platform since 25 June 2020. PhilSmile ceased operations on 14 December 2020. Thus, as far as the restart or use of the PhilSmile student management system is concerned, this has become a legal impossibility.[1] As a result, informing the students about the dangers of a system that is not only no longer in use but does not exist at all only heightens fear and mistrust for an event that is no longer possible.[2]

In its submitted Full Breach Report,[3] SLU also stated that its Data Protection Committee has also resolved to undergo a third-party audit of SLU's data privacy compliance, engaging the services of a reputable third-party provider for the same. The audit includes reviews of the policies and guidelines on data privacy; privacy impact assessments on all data processing systems within SLU; current organizational,

[1] NPC BN 20-116 In re: Saint Louis University Compliance and Motion for Reconsideration dated 29 March 2021
[2] *Ibid.*
[3] NPC BN 20-116 In re: Saint Louis University Attachment A Final Breach Report dated 29 March 2021

technical, and physical measures to ensure data protection; and training for SLU students, faculty, administrators, and personnel regarding SLU's data protection policies and guidelines.

SLU also stated in its Full Breach Report that based on the results of this audit, the Data Protection Committee will update SLU's fundamental data privacy documents, including but not limited to SLU's Privacy Notices, Data Privacy Manual, Data Privacy Policies and Guidelines, and other collaterals indicating a commitment to data privacy on the part of SLU.[4]

As to the reply to the Show Cause Order, SLU stated that it entertained a good faith belief that it had taken, implemented, and applied sufficient security measures to the personal data at the time the personal data breach was reasonably believed to have occurred.

The encryption of the data at rest and the taking of the system offline was part of a good faith belief that these measures prevented the use of the personal data by any person who had no rightful access to it. Upon receiving the Resolution dated 21 January 2021 of the Commission, it then took further steps to contain the data breach. SLU has since taken steps to completely prevent the likelihood of a real risk of serious harm unto the affected data subjects.

SLU prays for the Commission to reconsider its Resolution dated 21 January 2021 and finds that the disclosure of the nature and extent of the data breach to the affected data subjects is no longer necessary and should be exempt from notification under Section 19 of NPC Circular No. 16-03.

Discussion

As to the reply to the Show Cause Order, this Commission finds the explanation of SLU to be sufficient and wants to note the efforts executed by SLU to reinvestigate and to dig deeper into the breach and identify the affected data subjects.

[4] *Id* at pp. 7

As to the Compliance and Motion for Reconsideration, it mentions that the Data Protection Committee of SLU has reached out to the affected data subjects for them to execute NDAs and they have in fact executed the NDAs, but it failed to mention and give background to the Commission as to what SLU disclosed to the data subjects about the breach since they are still requesting for exemption to notify the data subjects.

The fact that the data subjects were made to execute NDAs, they necessarily should have informed them about the breach and the data subjects already should have knowledge of the breach.

As to the required contents of the notification to the affected data subjects, Section 18 (C) of NPC Circular No. 16-03 provides:

> **SECTION 18.** ***Notification of Data Subjects***. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> x x x
>
> C. *Content of Notification*. The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay. x x x

However, nowhere in the NDAs or in the other documents submitted revealed that the affected data subjects, before making them execute the NDAs, were properly apprised of the reason and consequences on why they were asked to execute them.

Furthermore, upon careful perusal of the NDAs, it shows that the NDAs did not comply with the notification requirements under Section 18 (C) of NPC Circular No. 16-03 indicated above.

This Commission would like to reiterate that SLU is not in the position to determine whether the notification to the affected data subjects is necessary or not. The determination of the aforesaid is within the ambit of the mandate of this Commission. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.[5]

In this case, the Commission did not exempt SLU from the notification of data subjects nor did SLU request for an exemption for the notification of data subjects only until now.

The Commission had already explicitly ruled on the said issue in the Resolution dated 21 January 2021 and will no longer entertain any requests from SLU regarding the matter. Thus, SLU is expected to strictly comply with the Resolution dated 21 January 2021 of this Commission to notify the affected data subjects and submit proof of compliance thereof, including the proof of receipt of the data subjects of such notification to this Commission.

WHEREFORE, premises considered, Saint Louis University is hereby **ORDERED** to **NOTIFY** the affected data subjects in pursuant to the requirements of Section 18 (C) of NPC Circular No. 16-03 and **SUBMIT** proof of compliance thereof, including the proof of receipt of the data subjects of such notification **within fifteen (15) days** from Receipt of this Resolution

This Commission gives a **STERN WARNING** to Saint Louis University that any deviation of compliance with the Order of this Commission will be dealt more severely.

SO ORDERED.

City of Pasay, Philippines.
15 April 2021.

[5] Section 18(B), NPC Circular 16-03.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

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

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

Copy furnished:

R.F.H.C.T
President
Saint Louis University

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission