IN RE: UNIVERSITY OF THE EAST

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

CID BN 19-067
(For violation of Data Privacy Act of 2012)

RESOLUTION

LIBORO, P.C:

Before this Commission is a breach case involving University of the East (UE) for the violation of Data Privacy Act of 2012 (DPA).

Facts

On April 14, 2019, S.B.N. - Dean of University of the East College of Computer Studies and Systems, received a message in his Facebook Messenger from username: C.D. that reads: *"Magandang umaga. Gsto namin ipaalam na hawak na naming ang libo libong data at mga MOA mula sa inyong mga web systems na gawa ng inyong research department. Hindi kami magdadalawang isip na ikalat ito sa publiko kapag ipinagpatuloy mo ang pag balewala sa hinain ng mga estudyante at ang pagkampi sa mga tao na umaapak sa mga karatapan nila".* A snapshot of the message was sent to Professor N.K.T., a CCSS faculty member designated as RnD Coordinator, who then informed RnD Team Leader and UE-CCSS student - D.G., and Assistant Team Leader – N.B.Z. D.G. and N.B.Z. both verified the claims of C.D. by checking the servers (Google Servers) maintained by the RnD Unit.

Their verification discovered unauthorized logs on the server maintained by N.B.Z. The said server sustained brute force attacks from more than 4,000 I.P. addresses, trying to get into the system's database. Notably, the server that was attacked contains the registration databases for UE school activities: "Pasiklaban 2019" and "CCSS Alumni Homecoming 2018". The same server includes databases for the "MOA Signing System" and "Research Archiving System."

On 17 April 2019, UE University Manila ("UE") notified the Commission on the incident involving unauthorized access to personal information stored in the database of the Research and Development ("RnD") unit of the UE College of Computer Studies and System ("CCSS"). According to incident report, the hacking involved a breach of personal data of 1,572 Senior High School Students and around 200 for CCSS Alumni.

In the same Data Breach Notification (Preliminary), UE requested for a postponement of notification to Data Subjects as the system hacking happened during the period of semestral break that is within the Holy Week, and this made it difficult for them to notify all affected data subjects, as well as to summon key persons for an interview concerning the incident.

On 9 September 2019, the Commission En Banc, denied[1] the request for postponement of UE. It emphasized the need of notification hence UE was ordered to notify the data subjects without further delay and to submit within fifteen (15) days a complete breach report, including details of notification and assistance provided to data subjects.

On 21 July 2020, due to UE's non-compliance with the Commission En Banc's directive on the Resolution dated 09 September 2019, the Commission sent an Enforcement Letter to UE which contains directive upon UE's Data Protection Officer to ensure immediate compliance with the Commission En Banc's directive on the said Resolution.

On 19 August 2020, Ms. T., responded to the Enforcement Letter explaining that they previously sent the complete breach report with details of notification (Final Report) on 09 October 2019 to complaints@privacy.gov.ph. However, this Division found deficiencies in the submitted Final Report. Thus, in the light of a thorough assessment, this Division further directed UE to submit the annexes and proofs of notification for a bona fide complete report.

[1] 09 September 2019, Resolution

On 16 September 2020, Ms. T. submitted the required annexes and proofs of notification, which finally cured the report's previously found deficiencies.

Discussion

This case before the Commission can now be considered closed.

Under circumstances where sensitive personal information or other information are reasonably believed to have been acquired by an unauthorized person, Section 20(f) of the Data Privacy Act of 2012 (DPA) provides that:

> The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

Section 18 of NPC Circular No. 16-03 (Circular) provides for the procedure on which the personal information controller (PIC) must follow in notifying the affected data subjects affected by a personal breach.

As to the content of notification, the Circular[2] provides that the notification shall include, but not be limited to:

> nature of the breach;
> personal data possibly involved;
> measures taken to address the breach;

[2] Section 18 (c), NPC Circular 16-03 – Personal Data Breach Management

> measures taken to reduce the harm or negative consequences of the breach;
> 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
> 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, PIC may be provided in phases without undue delay.

The Circular[3] further provides that the PIC shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. Hence, the notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. Where individual notification is not possible or would require a disproportionate effort, the PIC may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner.

In this case, it is shown that UE received the Resolution on 24 September 2019. UE was given a fifteen (15) day period to notify the affected data subjects. Based on the submitted screenshot[4] of e-mail notifications, it shows that UE started notifying the affected data subjects on 1 October 2019, which was well within the period given to it comply with the order.

As to examination of the content and form of the Notification, the Commission found that the notification thoroughly outlined the nature of the breach, the personal data that was possibly affected, the measures UE had undertaken to address the breach, reduce harm or

[3] Section 18 (d) Form. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data. The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.

[4] Screenshot of Email Notifications to Affected Data Subjects from U.E. DPO.

negative consequences of the breach, and contact details of the DPO where an affected subject could reach out for clarifications and further assistance. In addition, the said notifications were electronically sent individually to the affected data subjects via e-mail.

Aside from UE's compliance with the notification requirement provided in the Circular, UE provided measures it took to address the breach, to wit: 1. An immediate shut down of its main server to prevent further data compromise; 2. Verification of the sample data/data portion showed by 'C.D.' and confirmed that such is a part of the database; 3. Checking of the integrity of the database existing on the main server vis-a-vis the sample data from C.D. From there, it was verified that the data was merely copied and not altered nor destroyed; and 4. Migration of the databases and systems to a highly protected/secured cloud storage/service provider, such as Google Cloud Platform that provides a higher and stricter security level.

In order to prevent the recurrence of the same incident, the RnD unit of UE had further undertaken to perform the following additional measures: 1. UE's Information Technology Department was tapped to act as an Administrator for any and all designed Information System in their official UE Server for any and all conduct of Student Council Voter Registration and Elections, as well as Registration Systems for various Conferences/Seminars; 2. Definition of 'turnover responsibilities' of the RnD Unit which comprised of students whose engagement to the said unit can be terminated anytime; 3. All new measures, such as but not limited to procedures related to the collection, storage, sharing, and disposal of data shall be put in writing and be incorporated in the Operations Manual of the RnD Unit.

UE further adopted measures for non-RnD Unit Activities and Student-led projects, to wit: a. Higher and Stricter level of security on Google Cloud Platform; b. Incorporation of Cost of Subscription to a More secure Cloud Service in the College Budget; c. Designation of RnD Unit as an Institutional Account Holder for the migration of all its system/database to a new server; d. Definition of Duties and Responsibilities of the members of the RnD Unit, especially to members who shall manage the server; and e. For every system developed and deployed, the following items will be defined to closely monitor access to data among the members of the unit: i. System Development: a. Composition and definition of responsibilities of the

Systems Development Team; b. Access permission to files and databases; c. Use of password, encryption, and other security measures; d. Use of Google Drive and other cloud storage facilities; e. Use of mobile devices to access e-mail, Google Drive, and other facilities necessary for systems development; and ii. System Deployment: a. Collection procedure for the actual/live data and the security protocol applied to its access; b. Access Permission requirement for each member of the team to the system. A set of procedures will be formulated to define awarding to access rights and removal of access rights. Hierarchy of Access (such as Viewing, Editing Privileges, etc.) will also be considered; and c. Access Permission for databases for the RnD coordinator, team leader, assistant team leader.

A careful examination of UE's complete breach report reveals the organization's judicious and suitable put-up of measures, steps, and policies to address the breach incident. However, the said breach report also stated that they "emphasize herein that the data was just copied, not altered or destroyed[5]". With this, the Commission underscores the importance of data protection. Hence, PICs is directed to take by heart the provision of Section 4[6] of the Circular which mandates the implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system, and mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach. It is not enough to conclude that the data were just copied and not altered or destroyed without the PIC's in-depth investigation of the matter. The PIC's investigation should have considered the possibility that the information may have been accessed and used by unauthorized persons, in an effort to mitigate the risks to the data subjects.

Nonetheless, with the twin notification made by UE to this Commission and upon the affected data subjects, this shows consonance with Section 20(f) of the Data Privacy Act, which requires

[5] Complete breach report (Final Report), page 4.

[6] "A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure, among others, the implementation of organizational, physical, and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident, implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system, and mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach."

prompt notification upon the National Privacy Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person (in this case by one under the guise of "C."), which may likely give rise to a real risk of serious harm to any affected data subject.

With the foregoing, the Commission deduced from the careful examination of the reports and other documents submitted by UE that there is a bona fide compliance with the directives of the Commission's Resolution and the Circular. The measures undertaken by UE are responsive to the required personal data management, which includes prevention, incident response, mitigation, and compliance with notification requirements. More so, preventive measures were also undertaken by UE in its effort to deter future breach. Accordingly, due to the apparent bona fide compliance of UE in this case, there is nothing more left for the Commission than to close the case.

WHEREFORE, premises considered, the case CID BN 19-067 In the Matter of University of the East Manila, is hereby considered CLOSED.

SO ORDERED.

Pasay City, Philippines.
22 October 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

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

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

Copy furnished:

F.B.H.
Head of the Organization
Office of the Chancellor, Manila

M.Q.T.
Data Protection Officer
Office of the Chancellor, Manila

S.B.N.
Process Owner
Office of the Chancellor, Manila

LEGAL DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission