IN RE: UNIVERSITY OF THE PHILIPPINES - VISAYAS **NPC BN 18-045**

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

RESOLUTION

AGUIRRE*, D.P.C.;*

Before the Commission is the Compliance dated 29 December 2020 submitted by the University of the Philippines – Visayas (UP Visayas) in fulfillment of the Commission's directive in its Order dated 15 December 2020.

Facts

On 07 April 2018, UP Visayas submitted its Data Breach Incident Report dated 05 April 2018, informing the Commission of a confidentiality breach where unauthorized individuals gained access to its system using an existing username without administrative privileges:

> SQL Injection attempts in the University's Research, Creative Works, Public Service and Publication System (RCWPSPS). Hackers were able to gain access to the system by guessing the password of existing users with easy guess password.[1]

UP Visayas stated that the hackers logged in to the system on 29 March 2018 at around 10:02 PM and "lasted for only 15 seconds."[2] It claimed that the data was not compromised since the "attempts to

---

[1] Data Breach Incident Report, 05 April 2018, at 1 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).
[2] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

query data on the database were blocked by the firewall."[3] Further, it alleged that the hackers were not allowed access to the personal data since the username was not allowed for that kind of operation.[4]

According to UP Visayas, only one account was compromised, and based on the assessment of its system developer and system and network administrators, no data was copied or taken out of the system.[5]

Further, UP Visayas identified that the following personal data may have been involved:

> 1. Description of sensitive personal information involved
>
> The system contains records of research, creative work, and public service project, as well as publications and other outputs of faculty and researchers [sic] from the various units and colleges of the University of the Philippines Visayas. The system also records email address, phone numbers, high school degree, awards, general and specific experience, roles on project and image of personnel.
>
> 2. Description of other information involved that may be used to enable identity fraud
>
> Part of the records kept at the system is the list of private sectors and the government institution partners/collaborators of projects, certificates of projects and completion, certificates of participation in research, creative works, public service, and publications projects. Reports, documentations, and other relevant certificates are also recorded and stored by the system.[6]

To address the breach, UP Visayas shut down access to the database of the involved system and disabled all usernames with easy passwords.[7]

---

[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.* at 2.
[7] Data Breach Incident Report, 05 April 2018, at 2 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

On 25 October 2018, the Commission, through its Complaints and Investigations Division (CID), sent a letter inviting UP Visayas to a meeting on 03 December 2018 to discuss the breach.[8]

On 19 December 2018, along with additional documents, UP Visayas submitted a copy of the notification it sent to the affected data subject, DJB. The notification informed DJB of the SQL injection attempts in UP Visayas' RCWPPS, that her username and password were used to log into the system, and that "possible access to [her] name, address and research work titles were compromised."[9] Further, UP Visayas informed her that her username and password were disabled and subsequently modified after the incident.[10]

On 15 December 2020, the Commission issued an Order requiring UP Visayas to submit a Post-Breach Report within fifteen (15) days from receipt of the Order.[11]

In response, UP Visayas submitted its Post-Breach Report dated 29 December 2020.[12] It emphasized that in addition to the measurements it took regarding passwords, users must now connect to UP Visayas' internet connection in order to access the website.[13] UP Visayas claimed that, as a result, "there has been no recurrence of a similar incident after the University has undertaken the security measures and breach management."[14]

Issue

Whether UP Visayas has complied with the directives of the Commission in its 15 December 2020 Order.

---

[8] Breach Notification of UP Visayas, 25 October 2018, at 1 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).
[9] Unauthorized Access to RCWPPS dated March 29, 2018, 19 December 2018, at 1 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).
[10] *Id.*
[11] Order, 15 December 2020, at 1 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).
[12] Post-Breach Report, 29 December 2020 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).
[13] *Id.* at 2.
[14] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Discussion

The Commission resolves to close the case considering that UP Visayas has sufficiently complied with the Commission's directive in its 15 December 2020 Order.

In its Post-Breach Report dated 29 December 2020, it sufficiently explained the nature of the incident and the circumstances regarding its discovery.[15] It also enumerated and submitted proof of the security measures it executed as a response to the incident, such as conducting a system audit, automatically shutting down access to the database, disabling and re-setting the passwords, and making the site available only through its university intranet.[16] Lastly, in compliance with the notification requirements, it informed DJB of the unauthorized access to the RCWPPS through her account.[17]

More importantly, the Commission stresses that the SQL injection attempts were not subject to mandatory breach notification since it was a security incident. There is a distinction between a security incident and a personal data breach.

Section 3 (F) of NPC Circular 16-03 defines a personal data breach:

> Section 3. *Definition of Terms.*
>
> . . .
>
> F. "Personal Data Breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. It may be in the nature of:
>
> 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
> 2. Integrity breach resulting from alteration of personal data; and/or

[15] *Id.* at 1.
[16] *Id.*
[17] *Id.* at 2.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> 3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.[18]

On the other hand, Section 3 (J) of NPC Circular 16-03 defines a security incident:

> Section 3. *Definition of Terms.*
>
> . . .
>
> J. "Security Incident" is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place[.][19]

In this case, the SQL injection attempts are considered security incidents considering that there is no personal data that was compromised. As a matter of fact, attempts to query data and access personal data were not permitted and blocked by the firewall because the username DJB was not allowed to perform those kinds of operations.[20] Therefore, other than the access of DJB username, no other personal data was involved in the security incident. Given that there was no accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data in this case since access to personal data was not permitted through DJB username, it is not a personal data breach; rather, it is a security incident.

Moreover, UP Visayas' swift actions and security measures ensured that the security incident would not result into an eventual personal data breach. The actions and measures executed after the incident proved successful since there has been no recurrence of any similar incident up to this date.[21]

---

[18] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16- 03], § 3 (F) (15 December 2016).
[19] *Id.* § 3 (J).
[20] Data Breach Incident Report, 05 April 2018, at 1 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022); Post-Breach Report, 29 December 2020, at 1 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).
[21] *See* Post-Breach Report, 29 December 2020, at 2 *in* In re: University of the Philippines - Visayas, NPC BN 18-045 (NPC 2022).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Thus, UP Visayas faithfully complied with the procedures under NPC Circular 16-03 and successfully executed its obligations as a Personal Information Controller. Further, it has sufficiently complied with the Orders and immediately implemented security measures to protect its data subjects' personal information.

WHEREFORE, premises considered, Commission resolves that NPC BN 18-045 In re: University of the Philippines – Visayas is hereby **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
10 November 2022.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

WLP
Data Protection Officer
University of the Philippines - Visayas

NAT
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

GENERAL RECORDS UNIT
National Privacy Commission

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228