IN RE: POLYTECHNIC UNIVERSITY OF THE PHILIPPINES **NPC BN 18-222**

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

ORDER

Before the Commission is the Compliance submitted by Polytechnic University of the Philippines (PUP) dated 03 June 2022[1] in fulfillment of the Commission's directive in its Order dated 20 May 2022.[2]

In its letter dated 22 November 2018, the PUP notified the Commission of a breach in its information security.[3] It alleged that on 20 November 2018, it came across a post dated 18 November 2018 on the Facebook page of ZeroSecurity PH claiming that the latter was able to get three thousand eight hundred nine (3,809) emails from #PUPWebsite and #HalfofDatabaseEmails."[4] After seeing the post, the PUP Information and Communication Technology Office (PUP-ICTO) initiated a historical server activity audit and conducted a thorough review of the application and system logs:

1. PUP ICTO immediately checked the SIS database (DB) and cross checked the email addresses listed in the FB post in the database.
2. PUP ICTO checked unexpected query of records thru [sic] thorough review of SIS application logs and the DB system logs.
3. Changed the passwords of the admin user accounts that has [sic] registrar access to the system DB.

---

[1] In re: Polytechnic University of the Philippines, 03 June 2022, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[2] Order (To submit Post-Breach Report), 20 May 2022, at 2, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[3] Letter of Polytechnic University of the Philippines, 22 November 2018, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[4] *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

4. PUP ICTO discussed the current situation to PUP Executive Committee and informed the latter of the counter-measures done by the ICTO.[5]

It discovered that nine hundred ninety-one (991) email addresses of PUP Student Information System (SIS) users matched with the three thousand eight hundred nine (3,809) emails posted on the ZeroSecurity PH's Facebook page.[6]

After conducting its initial investigation, PUP concluded that:

1. The e-mail records might have come from an old copy of the database which is in possession of someone who had worked before with PUP SIS enhancement.
2. There is no direct access to the online database and the hackers simply compiled it from different sources.[7]

The Commission, through its Complaints and Investigation Division (CID), issued an Order dated 20 May 2022 directing PUP to submit its Post Breach Report within fifteen (15) days from its receipt of the Order.[8]

On 07 June 2022, PUP submitted its Compliance dated 03 June 2022.[9] It expounded that:

> The 991 email addresses that matched with the email addresses published by the 'hackers' are old records. The email addresses belong to student[s] who already graduated or have dropped out from the University." Further investigation conducted by ICTO on system logs reveals that there was no direct access to the system database and that the records were compiled from different source/s and not the Student Information System as claimed by the *'hackers'*. Technically, no hacking was done but

[5] *Id.* at 2.
[6] *Id.*
[7] *Id.*
[8] Order (To submit Post-Breach Report), 20 May 2022, at 1-2, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[9] In re: Polytechnic University of the Philippines, 03 June 2022, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (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

> mere exploitation of an old list (physical copy) of email addresses of students and some faculty members.[10]

Finally, PUP claimed that its "[a]ffected data subjects were prompted thru [sic] the Student Information System (SIS) to change their SIS passwords before they can access the SIS. They were also advised to take other important measures to ensure that their account is secured" and attached a screenshot of the notification prompt contained in the SIS page.[11]

NPC Circular 16-03 (Personal Data Breach Management) provides that a Personal Information Controller (PIC), upon knowledge of or when there is reasonable belief that a personal data breach requiring notification has occurred, is required to notify the affected data subjects within seventy-two (72) hours:

> 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:
>
> A. *When should notification be done*. The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.
>
> The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.[12]

Data subject notification is an essential obligation of a PIC.[13] Prompt notification is essential so that affected data subjects may have the

---

[10] *Id.* at 2.
[11] *Id.* at 3-4.
[12] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16- 03], § 18 (A) (15 December 2016).
[13] NPC BN 21-035, 01 June 2021, at 4 (NPC 2021) (unreported).

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

opportunity to take the necessary precautions or remedial measures to protect themselves and their own data.[14]

Although the personal information involved in the breach were only the data subjects' email addresses and names, there is still a potential risk. As previously held by the Commission:

> Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and **an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of 'Phishing' attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.[15]**

PUP claimed in its Compliance that it notified the affected data subjects by posting a prompt in the SIS before its users are able to access the SIS.[16] As evidence, it attached a screenshot of the notification prompt:

> Good day! In line with PUP Security Protocol, your PUP SIS password was reset.
>
> . . .
>
> Remember, all transactions recorded on your account are your accountability.
>
> Thank you for taking the time to read this. We sincerely apologize for the annoyance of having to change your password, but, ultimately, we believe this simple step will result in a more secure PUP SIS experience.[17]

This notice, however, does not conform with the requirements of notification of data subjects:

---

[14] NPC Circ. No. 16- 03, § 18 (A).
[15] NPC BN 20-124, 10 September 2020, at 3 (NPC 2020) (unreported). Emphasis supplied.
[16] In re: Polytechnic University of the Philippines, 03 June 2022, at 3-4, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[17] *Id.* at 4.

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

> 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:
>
> . . .
>
> 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.
>
> 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.[18]

The notification prompt of PUP in its SIS is inadequate because it lacks the contents required in an appropriate notification to the affected data subjects.

The notification prompt also does not sufficiently demonstrate that the PUP individually notified its nine hundred ninety-one (991) PUP SIS users. A prompt on the system does not suffice as proper individual notification. The prompt merely states that the password has been reset and suggests "several important steps that [one] can take to ensure that [one's] account is secure," which PUP believes

[18] NPC Circ. No. 16- 03, 18 (C) – (D).

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

"will result in a more secure PUP SIS experience."[19] PUP, as the PIC, should individually notify the affected nine hundred ninety-one (991) SIS users so that they may be informed of the incident and adequately protect themselves from the consequences of the breach.

Further, given PUP's claims that the breach is the result of an "old list (physical copy) of email addresses of students and some faculty members"[20] that is "in possession of someone who had worked before with PUP SIS enhancement,"[21] it should demonstrate that it has created and implemented systems in place to safeguard both physical and online data.

Thus, the Commission orders PUP to individually notify the nine hundred ninety-one (991) PUP SIS users whose email addresses matched with the three thousand eight hundred nine (3,809) emails posted on the ZeroSecurity PH's Facebook page[22] and to submit proof of the security measures it took to prevent the incident from recurring.

WHEREFORE, premises considered, Polytechnic University of the Philippines is hereby **ORDERED** to comply with the following **within fifteen (15) days** from the receipt of this Order:

1. **NOTIFY** its affected data subjects and **SUBMIT** proof that it individually and directly informed its affected data subjects; and

2. **SUBMIT** proof of the security measures it implemented.

SO ORDERED.

City of Pasay, Philippines.
10 November 2022.

---

[19] In re: Polytechnic University of the Philippines, 03 June 2022, at 4, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[20] *Id.* at 2.
[21] Letter of Polytechnic University of the Philippines, 22 November 2018, at 2, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[22] *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

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

I CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Copy furnished:

MMM
President
Polytechnic University of the Philippines

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
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