IN RE: CARDINAL HEALTH INTERNATIONAL PHILIPPINES INC.

NPC BN 18-200

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the breach notification submitted by Cardinal Health International Philippines, Inc.'s (CHI Philippines) involving the disclosure of the home phone numbers of its employees to the Cardinal Health Inc. (Cardinal Health) group of companies as a result of a system glitch.[1]

Facts

Cardinal Health, the parent company of CHI Philippines, is responsible for managing the information security system of its international conglomerates, which includes CHI Philippines.[2] It also manages its directory services where its employees' information is stored.[3]

On 21 October 2018, Cardinal Health retired its single-sign on system and transitioned its directory service protocol from Lightweight Directory Access Protocol (LDAP) to Active Directory (AD).[4] To migrate information from LDAP to AD, one must export the contents

[1] Notification to the Commission, 27 October 2018, at 3, *in* In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).
[2] *Id.*
[3] *Id.*
[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

of the LDAP from the current environment, configure the directory server to use AD, and finally, import the exported file.[5]

During the process, Cardinal Health reported system errors.[6] The employees' home phone numbers stored in Workday, Cardinal Health's human resource management system, became available on Skype, Outlook, and global address book of the Cardinal Health group of companies.[7]

On 22 October 2018, two of its employees notified Cardinal Health that their home phone numbers were visible on Skype.[8]

On 26 October 2018, Cardinal Health identified that one thousand four hundred sixty-five (1,465) employees of CHI Philippines were affected by the incident.[9]

On 27 October 2018, Cardinal Health notified the National Privacy Commission of the breach.[10] On the same day, it notified CHI Philippines' employees by email.[11]

As a subsequent measure to address the incident, Cardinal Health declared that it took immediate steps by removing the script that triggered the internal disclosure of employees' home phone numbers.[12] It averred that it "implemented an internal communications protocol requiring coordination between its Identity Management (IDM) and Human Resource (HR) Data Compliance Departments when personal data will be processed to transferred to ensure [that] risks of inadvertent disclosures are identified, and safeguards against potential inadvertent disclosures are put in

---

[5] How to Migrate from LDAP to Active Directory, *available at* https://www.ibm.com/support/pages/how-migrate-ldap-active-directory (last accessed 31 January 2023).
[6] Notification to the Commission, 27 October 2018, at 3, *in* In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.* at 1.
[11] *Id.* at 5.
[12] Notification to the Commission, 27 October 2018, at 3, *in* In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).

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

place."[13] Cardinal Health also maintains that it will require its IT Team to undergo further training to ensure observance of data protection compliance protocols and take the necessary disciplinary actions against the IT Team.[14]

Cardinal Health specified that the exposure is only limited to the employees' home phone numbers.[15] It also maintained that neither sensitive personal information nor information that may be used to enable identity fraud were involved in the incident.[16] It assured that employees' private phone numbers are no longer visible to the best of its knowledge.[17]

Issue

Whether the matter requires mandatory breach notification.

Discussion

The Commission finds that this matter does not fall under mandatory breach notification. Thus, the Commission resolves to close the matter.

Section 11 of NPC Circular 16-03 (Personal Data Breach Management) provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> A. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud.

[13] *Id.*
[14] *Id.* at 4.
[15] *Id.*
[16] *Id.* at 3.
[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

> For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> B. There is reason to believe that the information may have been acquired by an unauthorized person; and
>
> C. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[18]

Given this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or other information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[19]

For the first requisite the personal data involved is the employees' phone numbers.[20] This, however, cannot be considered as sensitive personal information.[21] Section 3 (l) of the Data Privacy Act of 2012 defines sensitive personal information as:

> Section 3. *Definition of Terms*.
>
> . . .

[18] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §11 (15 December 2016).
[19] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2023).
[20] Notification to the Commission, 27 October 2018, at 4, *in* In re: Cardinal Health International Philippines Inc., NPC BN 18-200 (NPC 2018).

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

> (l) Sensitive personal information refers to personal information:
>
> > (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
> >
> > (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
> >
> > (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
> >
> > (4) Specifically established by an executive order or an act of Congress to be kept classified.[22]

A data subject's home phone number clearly does not fall within the definition of sensitive personal information. Also, given the circumstances, the data subjects' home phone number, by itself, cannot be considered as information that may be used to enable identity fraud.

For the second requisite, this matter involves a confidentiality breach where the employees' home phone numbers became temporarily visible to the entire organization. Because of this, the information could have been acquired by an unauthorized person. Thus, the second requisite is present.

The third requisite that the unauthorized acquisition is likely to give rise to a real risk of serious harm is not present in this case. Taking note of the nature and quantity of the personal data involved and the

---

[22] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 3 (l) (2012).

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

limited exposure within the confines of the organization, there is neither serious harm to the affected data subjects nor reason to believe that the employees' home phone numbers may have been likely resulted in a real risk to the data subjects.

Considering that the first and third requisites for mandatory breach notification are absent in this case, the Commission finds that the breach pertaining to employees' home phone numbers among the Cardinal Health group of companies does not require mandatory breach notification to the Commission.

Nevertheless, even if the incident is not subject to mandatory notification, Cardinal Health has fulfilled its obligations as a Personal Information Controller by taking immediate precautionary measures to minimize any possible harm or negative consequences to its data subjects.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-200 In re: Cardinal Health International Philippines Inc. is hereby **CLOSED.**

SO ORDERED.

Pasay City, Philippines.
19 January 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

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.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

JAS
Data Protection Officer
Cardinal Health International Philippines, Inc.,

COMPLAINTS AND INVESTIGATION 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