IN RE: MEDICARD PHILIPPINES, INC. **NPC BN 21-192**

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

ORDER

Before this Commission is a Request for Extension and Alternative Means of Notification dated 29 December 2021, submitted by MediCard Philippines, Inc. (MediCard), through email, in relation to breach notification proceedings for a ransomware attack on its database servers.

The Facts

On 28 October 2021, the Commission issued a Resolution (Resolution) denying MediCard's request for exemption to notify the data subjects. It further ordered MediCard to notify the data subjects with corresponding proof of notification; submit its Full Breach Report; provide proof of its declaration that no company and data subject information was exposed and proof of security measures; and show cause in writing as to why it should not be subjected to contempt proceedings for failure to submit its Full Breach Report, *to quote*:

> **WHEREFORE,** premises considered, this Commission **DENIES** the request of MediCard Philippines, Inc. for the exemption or in notifying the data subjects affected by the breach.
>
> MediCard Philippines, Inc. is hereby **ORDERED** to comply with the following **within fifteen (15) days** from receipt of this Resolution:
>
> 1. **NOTIFY** the affected data affected subjects pursuant to Section 18 of the NPC Circular No. 16-03 and submit proof of compliance thereof, including the proof of receipt of the data subjects of such notification;

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

2. **SUBMIT** a Full Breach Report pursuant to Section 9 and 17 (D) of the NPC Circular No. 16-03;

3. **SUBMIT** proof of its declaration that no company and data subject information was exposed and proof of security measures indicated in the Forensic Report dated 12 October 2021; and

4. **SHOW CAUSE** in writing why it should not be held liable for its failure to submit its Full Breach Report within the prescribed period 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.

SO ORDERED. [1]

On 29 December 2021, MediCard sent an email to the Commission stating that it received the Resolution on 16 December 2021. Further, MediCard claims that it needs additional time of fifteen (15) days within which to comply with the given orders of the Commission. The reason cited for additional time needed is for the MediCard to further coordinate with its third-party cybersecurity service provider owing to logistical and communication challenges brought about by the COVID-19 pandemic and the intervening holidays.[2]

Aside from the request for additional time to comply, MediCard stated that it is considering notifying the affected data subjects through alternative means.[3] MediCard claims that it does not have the affected data subjects' contact information (e.g. current mobile number, email address, and residential address). MediCard further stressed that for company-sponsored accounts, the data subjects' employer or company directly coordinates with MediCard for the claims and benefits. Hence, MediCard would have no visibility on the personal contact details of the data subject who is the employee-beneficiary.[4]

---

[1] Resolution dated 28 October 2021.
[2] MediCard Email Request dated 29 December 2021.
[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

Thus, MediCard requests that the Commission allow it to notify the affected data subjects by: 1) sending a notification through the companies/employees of the affected data subjects; or 2) publication through its website.[5]

Issues

1. Whether MediCard's request for additional time to comply with the Commission's orders stated in its Resolution dated 28 October 2021 be granted; and
2. Whether MediCard's request for alternative means of notification be granted.

Discussion

The Commission grants MediCard's request for additional time to comply with its orders provided in the Resolution dated 28 October 2021. However, the Commission denies MediCard's request for the use of alternative means of notification.

The Commission grants the request for additional time to comply.

Section 17(C) of NPC Circular No. 16-03 (Personal Data Breach Management) provides:

> SECTION 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> xxx
>
> C. *When delay is prohibited.* There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the

[5] *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

> 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless the personal information controller is granted additional time by the Commission to comply."[6]

Further, Section 18(A) of the same Circular states:

> **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.[7]

As previously ruled by the Commission in its Resolution dated 28 October 2021, this case falls under the mandatory notification requirement.[8] Further, MediCard shall comply with the periods as provided in NPC Circular No. 16-03. The Full Breach Report must be submitted within five (5) days from filing the initial report.[9] While, the notification to the affected data subjects must be made on the basis of available information within the 72-hour period.[10]

However, MediCard asks for additional period to comply with the Commission's orders indicated in its Resolution dated 28 October 2021 because of the logistical and communications challenges in

---

[6] Section 17(C) of the NPC Circular No. 16-03
[7] Section 18(A) of the NPC Circular No. 16-03.
[8] Resolution dated 28 October 2021. At page 5.
[9] Section 17(C) of the NPC Circular No. 16-03.
[10] Section 18(A) of the NPC Circular No. 16-03.

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

coordinating with its third-party cybersecurity service provider due to the intervening holidays and the COVID-19 pandemic.[11]

The Commission emphasizes that in cases of data breach, especially cases that fall under the mandatory notification rule, personal information controllers (PICs) must ensure compliance with their obligations under the law including the prompt adherence with the periods provided in the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant issuances of the Commission such as NPC Circular No. 16-03.

However, in the interest of substantial justice and due process, the Commission exercises its authority to grant MediCard the additional non-extendible period of fifteen (15) days from receipt of this Resolution to comply with Commission's orders indicated in the Resolution dated 28 October 2021.

Individual notification has not been shown to be impossible or requires disproportionate effort as provided in Section 18(D) of the NPC Circular No. 16-03.

While the Commission grants MediCard additional period to comply with the Resolution, it denies Medicard's request to notify the affected data subjects through alternative means.

Section 18(D) of NPC Circular No. 16-03 provides the form of notification for affected data subjects, *thus:*

> **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:
>
> xxx
>
> *D. Form.* **Notification of affected data subjects shall be done individually, using secure means of communication, whether**

[11] MediCard Email Request dated 29 December 2021.

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

> **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.[12] (Emphases supplied)

Given that MediCard has yet to submit its Full Breach Report, and other crucial information regarding the data breach such as notification to the affected data subjects and proof of its security measures, there is insufficient information on whether the resort to alternative means of notification is proper.

MediCard has not proven that individual notification is not possible or would require disproportionate effort. According to MediCard the request for the alternative means in notifying the affected data subjects is due to the reason that it does have their contact information which includes their current mobile number, email address, and residential address.[13] However, a scrutiny of the record reveals that MediCard has the requisite contact details for the affected data subjects.[14]

In its Initial Report dated 22 September 2021, MediCard identified possible personal data that may have been subjected to the breach, which included email addresses of its MediCard Members or App users.[15] MediCard also identified that the possible personal data of its own employees may have been involved in the breach. Thus, given

[12] Section 18(D) of the NPC Circular No. 16-03.
[13] MediCard Email Request dated 29 December 2021.
[14] Initial Report dated 22 September 2021. At page 2.
[15] 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

that it has the email addresses of both members and employees, MediCard has no reason to use alternative means of notification. MediCard must then pursue individual notification as provided under Section 18(D) of NPC Circular No. 16-03.

As for MediCard's claim that for company-sponsored accounts, only the data subjects' company or employer directly coordinates with it, MediCard should be reminded that under the law, it is considered a PIC. A PIC is defined as one "who controls the processing of personal data, or instructs another to process personal data on its behalf."[16] Control is present when the entity "decides on what information is collected, or the purpose or extent of its processing."[17]

The nature of MediCard's business in processing claims and medical benefits for beneficiaries means that it has the requisite ability to decide on what information is collected, including its purpose and extent of processing.

Consequently, as the PIC and given that it controls the information given for processing, MediCard is responsible for complying with the notification requirements under NPC Circular No. 16-03 in case of data breach. It has the obligation to exert diligent efforts to coordinate with the relevant companies in order to provide information to the affected data subjects.

Hence, MediCard shall notify its affected data subject individually, using secure means of communication, whether written or electronic pursuant to Section 18(D) of the NPC Circular No. 16-03.

WHEREFORE, premises considered, Medicard Philippines, Inc.'s request for an additional period of time to comply with the Resolution dated 28 October 2021 is hereby **GRANTED.** Further, its request for the notification of the affected data subjects through alternative means is hereby **DENIED.**

---

[16] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 3(m).
[17] 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

MediCard is **ORDERED** to comply **within a non-extendible period of fifteen (15) days upon receipt of the Resolution,** with the orders of the Commission as stated in its Resolution dated 28 October 2021.

SO ORDERED.

City of Pasay, Philippines.
13 January 2022.

JOHN HENRY D. NAGA
Privacy Commissioner

I CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

RTM
Data Protection Officer

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