



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: MEDICARD PHILIPPINES, INC.

NPC 18-205

x-----x

RESOLUTION

NAGA, P.C.:

This Resolution refers to the compliance of MediCard Philippines, Inc. (MediCard) to the Resolution dated 10 December 2021.

Facts

On 10 December 2021, the Commission issued a Resolution¹ to MediCard, *to wit*:

WHEREFORE, premises considered, the request of MediCard Philippines, Inc. for exemption of notifying the remaining one thousand two hundred forty-one (1,241) affected data subjects is hereby DENIED.

Further, MediCard Philippines, Inc. is **ORDERED** to notify the remaining affected data subjects that are not yet notified through e-mail based on the available e-mail addresses in MediCard's database and at the same time post the notice couched in general terms on its official website for faster dissemination of information.

Finally, MediCard Philippines, Inc. shall **submit** to the Commission within **fifteen (15) days from receipt** of this Resolution a compliance report, which shall include details of notification to the data subjects (i.e., proof of the email notifications, postings, and their respective links).

SO ORDERED.²

¹ In re: Medicard Philippines Inc., NPC BN 18-205, Resolution dated 10 December 2022, at p. 11.

² Id.

On 09 March 2022, in compliance with the Resolution of the Commission, MediCard posted on its website³ the notice to affected data subjects, *to wit*:

Unauthorized Disclosure
09 Mar 2022

We at MediCard Philippines, Inc. protect your privacy seriously and recognize our duty to take care of our customers whose data we hold. As such, we take every precaution to ensure that your personal information is protected at all times while maintaining our transparency to our customers.

Last October 2018, we reported a data breach to the National Privacy Commission (NPC) involving a billing statement that was unintentionally delivered to the wrong company. The notification was made pursuant to the mandatory data breach notification procedure of the NPC. Unfortunately, data of some AIG Shared Services employees, limited to: employee number, MediCard ID number, name, and age were exposed in this data breach.

To validate this, if you have been an active employee of AIG Shared Services – Business Processing Inc. in October 2018, please access the following link: <https://webportal.medicardphils.com/DataBreachNotice> and enter your Member ID and date of birth.

We sincerely apologize that this has happened, and we want to assure you, as our valued member, that we have taken steps to prevent a recurrence of the incident. Also, the company has been in close coordination with the National Privacy Commission (NPC) to address this.

Should you have clarifications, feel free to reach us by mail at privacy@medicardphils.com.⁴

On 15 March 2022, MediCard submitted screenshots of its webpage posting and its e-mail notifications.⁵

³ See <https://www.medicardphils.com/news-promos-announcements/article/35>

⁴ See Unauthorized Disclosure, available at <https://www.medicardphils.com/news-promos-announcements/article/35>, last accessed on 22 June 2022

⁵ Compliance Report of MediCard Philippines, at pp. 1-2.

In relation to the e-mail notifications, MediCard submitted its Compliance dated 15 March 2022 and 25 May 2022. Along with the 25 May 2022 Compliance are the sworn affidavits of FC and JM, the persons responsible for notifying the affected data subjects through e-mail.

In Mr. FC's affidavit, he attested that on 09 March 2022, the e-mail notification was sent via the email address, privacy@medicard.phils.com, with the subject: MANDATORY PERSONAL DATA BREACH NOTIFICATION to a total of three hundred (300) data subjects following the required e-mail settings: (a) request a read receipt and (b) request a delivery receipt.⁶ He was able to send the e-mail notification to the three hundred (300) e-mail addresses and the delivery receipts provided were **"Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server."**⁷ Among the three hundred (300) email notifications, three (3) were not delivered due to "E-mail wasn't found at gmail.com", "E-mail address you entered could not be found", and "Your message could not be delivered."⁸ Despite repeated attempts to contact the recipients e-mail system, it did not respond.⁹

While in Ms. JM's affidavit, she attested that on 09 March 2022, she sent an e-mail notification with subject: Mandatory Personal Data Breach Notification to a total of three hundred and one (301) data subjects via the email address, privacy@medicardphils.com.¹⁰ She was able to send the e-mail notifications to the three hundred and one (301) e-mail addresses.¹¹ Some of the delivery receipts stated, **"Delivery to these recipients or groups is complete, but no delivery notification was sent by the destination server,"** while only five (5) have **"read receipts"**.¹² Among the three hundred one (301) e-mail notifications, six (6) were identified as **"Undeliverable"** and with a **"Failure Notice"** due to **"E-mail wasn't found at**

⁶ Affidavit of FC, p. 2

⁷ Id.

⁸ Id.

⁹ Id.

¹⁰ Affidavit of JM, p. 2.

¹¹ Id.

¹² Id.

gmail.com” and “Delivery has failed to these recipients or groups”.¹³

MediCard was able to successfully deliver five hundred ninety-two (592) e-mail notifications out of the total six hundred and one (601) e-mail addresses available to it. Nine (9) e-mail addresses available were not delivered for reasons: **“E-mail wasn’t found at gmail.com”, “E-mail address you entered could not be found”, “Your message could not be delivered”, and “Delivery has failed to these recipients or groups”.**

Discussion

The Commission finds MediCard compliant with the Resolution dated 10 December 2021.

MediCard was able to notify the remaining one thousand two hundred forty one (1,241) affected data subjects by sending the notification to the available e-mail addresses of the data subjects¹⁴ and by posting the notice on its website.¹⁵

Section 18 (C) of NPC Circular 16-03, otherwise known as Personal Data Breach Management, provides:

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

¹³ Id.

¹⁴ Compliance Report dated 15 March 2022 and Compliance Report dated 25 May 2022

¹⁵ Unauthorized Disclosure, available at <https://www.medicardphils.com/news-promos-announcements/article/35>, last accessed on 22 June 2022

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.¹⁶

Medicaid's website notification¹⁷ contained the nature of the breach, the personal data possibly involved, measures taken to address the breach and reduce the harm or negative consequences of the breach, such as prevention of recurrence of the incident, and contact details of the personal information controller. Thus, the website notification of Medicaid sufficiently complied with Section 18(C) of NPC Circular 16-03.

With respect to the e-mail notifications sent to the available e-mail addresses in its records, Medicaid was able to submit its Compliance dated 15 March 2022¹⁸ and 25 May 2022.¹⁹

According to the Compliance Report dated 25 May 2022, the affidavits of Mr. FC and Ms. JM stated that nine (9) out of the six hundred one (601) e-mail address available to MediCard were not successfully delivered for reasons: **"E-mail wasn't found at gmail.com"**, **"E-mail address you entered could not be found"**, **"Your message could not be delivered"**, and **"Delivery has failed to these recipients or groups."**²⁰

The failure to send e-mail notifications to the remaining nine (9) data subjects, despite MediCard's repeated attempts, rendered the individual e-mail notification impossible.²¹

Even though there is an impossibility in sending e-mail notifications to these data subjects, the Commission provides for

¹⁶ National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18 (C) (15 December 2016) (NPC Circular 16-03).

¹⁷ Unauthorized Disclosure, available at <https://www.medicardphils.com/news-promos-announcements/article/35>, last accessed on 22 June 2022

¹⁸ Compliance Report dated 15 March 2022

¹⁹ Compliance Report dated 25 May 2022

²⁰ Affidavit of FC; Affidavit of JM

²¹ Final Enforcement Assessment Report, 23 June 2022, p. 6

alternative means of notifying them through NPC Circular No. 16-03 (Personal Data Breach Management).²²

Particularly, Section 18(D) of NPC Circular No. 16-03 allows for alternative means of notification in which data subjects would be informed about the personal data breach in an equally effective manner if individual notification is impossible or would require disproportionate effort, *to wit*:

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 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.***²³ (Emphasis supplied)

Based on the records, the nine (9) remaining data subjects still could not be reached despite repeated attempts, and the e-mails could not be delivered for various reasons.²⁴ Given these circumstances, the Commission finds that there is an impossibility in individually

²² National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18 (D) (15 December 2016) (NPC Circular 16-03).

²³ National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18 (15 December 2016) (NPC Circular 16-03).

²⁴ See Affidavit of FC and Affidavit of JM.

notifying these data subjects. Consequently, alternative notification is allowed for these data subjects.

The Commission notes that MediCard has already posted the notification on its official website, which was in compliance with the Resolution dated 10 December 2021. Thus, the Commission deems the alternative notification sufficient with regard to the nine (9) remaining data subjects who could not receive email notifications of the data breach.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC 18-205 “In re: MediCard Philippines, Inc.” is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
14 July 2022.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
DUG CHRISTOPER B. MAH
Deputy Privacy Commissioner

COPY FURNISHED:

RTM

Data Protection Officer

4th The World Center Building

330 Sen. Gil Puyat Ave., Makati City

COMPLAINTS AND INVESTIGATION DIVISION

ENFORCEMENT DIVISION

GENERAL RECORDS UNIT

National Privacy Commission