IN RE: METRO PACIFIC TOLLWAYS CORPORATION **NPC BN 23-015**

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

ORDER

Before the Commission is Metro Pacific Tollways Corporation's (MPTC) requests for postponement and exemption to notify affected data subjects.

On 26 January 2023, MPTC was informed of a suspicious user activity caused by an individual who created several accounts or via multiple referrals in the MPT DriveHub application.[1] The MPT DriveHub application is MPTC's travel companion application that offers mobility solutions such as RFID transaction, trip planning, and roadside assistance to its registered users.[2]

MPTC surmised that the several accounts were created in an attempt to earn more points or raffle entries to win prizes in MPTC's "Download, Drive, & Win" promotion, which ran from 11 November 2022 to 31 January 2023.[3]

In its investigation, MPTC confirmed that the multiple duplicate registrations used the same email address and mobile number to register.[4] MPTC believed that this indicated a potential breach of the MPT DriveHub application system with possible access to others' personal information such as name, username, and email address.[5]

---

[1] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[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

On 27 January 2023, MPTC notified the National Privacy Commission (NPC) of the breach through the Data Breach Notification Management System (DBNMS).[6]

In its initial report, MPTC stated that the number of data subjects affected is one hundred (100) but that the actual number is still to be determined.[7]

MPTC claimed that it was in the process of "conducting a comprehensive investigation to determine the details of the incident, [particularly] the potential exposure of personal information and the appropriate and necessary measures to be undertaken to address any vulnerabilities in its system."[8]

MPTC requested postponement to notify its affected data subjects.[9] It explained that it be allowed a reasonable period to notify its data subjects from the completion of the investigation in case its investigation determined that there was an actual breach.[10] It also argued that no notice to the data subjects is required at that point because its preliminary investigation indicated that there was no intrusion or access to personal information in its system.

On 06 February 2023, the Commission directed MPTC to submit proof to substantiate its request for postponement:

> **WHEREFORE,** premises considered, the Commission hereby **ORDERS** Metro Pacific Tollways Corporation to **SUBMIT** within five (5) days upon receipt of this Minute Resolution proof to substantiate the request for postponement to notify affected data subjects.
>
> Should Metro Pacific Tollways Corporation fail to provide the foregoing, this case shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED.**[11]

---

[6] *Id.*
[7] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Minute Resolution, 06 February 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).

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 09 February 2023, MPTC submitted its Compliance to the 06 February 2023 directive.[12]

MPTC requested the Commission to "instead grant an exemption to notify the affected data subjects."[13] It claimed that upon further investigation, there is "no evidence of personal information and sensitive personal information breach affecting data subjects."[14]

In its Compliance, MPTC reiterated that as a measure to address the breach, it conducted a comprehensive investigation to determine the details of the incident such as the mode of the attack, the vulnerabilities in its system, the identity of the hacker, and the potential exposure of personal information of other data subjects.[15]

MPTC maintained that the incident may have been done using a method called "Replay Attack", which permits the instant creation of several users.[16] MPTC defined Replay Attack as "an attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access."[17]

MPTC, however, claimed that the "attack was targeted more on inputting invalid raffle entries in an attempt to win, rather than on accessing personal data found in the MPT DriveHub databases."[18] Further, it firmly asserted that its investigation showed no evidence of leaked or extracted personal and sensitive personal information.[19]

MPTC's statements in its Compliance, however, is contrary to its prior representations in its initial report through the DBNMS. MPTC initially stated that there are one hundred (100) affected data subjects

---

[12] Compliance by Metro Pacific Tollways Corporation, 09 February 2023, at 1, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[13] *Id*.
[14] *Id*.
[15] *Id*. at 3.
[16] *Id*. at 2.
[17] *Id*.
[18] Compliance by Metro Pacific Tollways Corporation, 09 February 2023, at 2, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[19] *Id*. at 2-4.

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

although its actual number is still to be determined[20] and that there is possible access to personal information of others such as name, username, and email address.[21]

The Commission emphasizes that the notification requirement under NPC Circular 16-03 (Personal Data Breach Management) is for the protection and benefit of data subjects.[22] Section 11 of NPC Circular 16-03 requires a Personal Information Controller (PIC) to notify the Commission and the affected data subjects upon knowledge of or when there is reasonable belief by the PIC that a breach requiring notification occurred:

> 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.
>
> 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.[23]

---

[20] Initial Notification through the Personal Data Breach Notification Form, 27 January 2023, *in* In re: Metro Pacific Tollways Corporation, NPC BN 23-015 (NPC 2023).
[21] *Id*.
[22] In re: Breach Notification Report of Sun Life of Canada, CID BN 17-021, 10 September 2020, at 6, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-BN-17-020-_-029-09.22.2022-In-Re-Sun-Life-of-Canada_Resolution.pdf (last accessed 16 March 2023).
[23] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016). Emphasis supplied.

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

In addition, Section 13 of the same Circular provides that when the PIC is uncertain as to the need to notify, it shall take into account the likelihood of harm or negative consequences on the affected data subjects and how notification could reduce the risks arising from the data breach reasonably believed to have occurred.[24] The PIC shall also consider if the personal data reasonably believed to have been compromised involves at least one hundred (100) individuals:

> Section 13. *Determination of the Need to Notify*. Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred.
>
> The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:
>
> . . .
>
> B. **At least one hundred (100) individuals**[.][25]

The Commission previously held that a PIC must notify its affected data subjects to allow them to take the necessary measures to protect themselves against possible effects of the breach:

> It is noteworthy that the avowed purpose of the required notification to data subjects of a breach incident is for them to take the necessary precautions or other measures to protect themselves against possible effects of the breach. Moreover, personal information controllers (PICs) are required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach. It therefore follows that PICs should guarantee that the notification they sent to data subjects has been received. Otherwise, it defeats the very purpose of notification of data subjects.[26]

Given the inconsistencies in MPTC's submissions, however, the Commission cannot yet rule on MPTC's request for exemption to

---

[24] *Id*. § 13.
[25] *Id*. Emphasis supplied.
[26] In re: Batangas Bay Carriers, NPC BN 20-157, 17 December 2020, at 3, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Resolution-NPC-BN-20-157-In-re-Batangas-Bay_Dec-17.pdf (last accessed 16 March 2023).

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

notify the data subjects without sufficient details on the number of those affected and personal or sensitive personal information involved in the incident.

Thus, it directs MPTC to submit additional information, and explain the disparity between its statements in its initial report and in its compliance with the directive dated 06 February 2023, regarding the number of data subjects and the personal or sensitive personal information involved, if any, in the incident.

WHEREFORE, premises considered, the Commission **ORDERS** Metro Pacific Tollways Corporation (MPTC) within ten (10) days from receipt of this Order to:

1. **SUBMIT** additional details on the number of data subjects and personal and sensitive personal information involved in the incident, if any; and

2. **EXPLAIN** the disparity between the number of data subjects and the involved personal and sensitive personal information stated in the initial report submitted through the DBNMS dated 27 January 2023 with the Compliance dated 09 February 2023.

SO ORDERED.

City of Pasay, Philippines.
16 March 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:

CSM
Data Privacy 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