IN RE: ENCHANTED KINGDOM, INC. **NPC BN 21-180**

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

ORDER

Before the Commission is a request for postponement of notification of data subjects filed by Enchanted Kingdom, Inc. (EKI) regarding a security incident on its online payment gateway on its website, operated by AsiaPay Payment Technology Corporation (AsiaPay).

Facts

EKI runs a theme park which has an online store selling its products. Customers are able to settle online purchases through various modes, including credit card payments.[1] The credit card option will direct customers to an online payment gateway, PesoPay, which is operated by AsiaPay. To confirm credit card payments, customers must supply their names, credit card numbers, and card validation values.[2]

In its Initial Report dated 31 August 2021 (Initial Report), EKI reported a possible security incident in the system of its online payment gateway partner, AsiaPay. From the Initial Report, AsiaPay alerted EKI that its payment gateway had been compromised for the period from 04 August 2020 to 02 May 2021. The EKI online store transactions may have been among those affected.[3]

EKI met with AsiaPay's Chief Operating Officer and its Philippine Senior Accounts Manager on 25 August 2021.[4] In the meeting, EKI was informed that AsiaPay was still investigating the breach and was

[1] Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.
[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

not in the position to confirm whether EKI transactions, or any specific EKI transaction or customer, were affected.[5] AsiaPay would provide more information to EKI about the breach, and assured them during the meeting and via email that the vulnerability which facilitated the breach had already been addressed.[6]

AsiaPay posted updates on its website regarding the security incident[7] on 11 June 2021, 22 July 2021, and 20 August 2021. In its last update, AsiaPay stated that based on the findings of a forensic investigator, there was a cyberattack that happened between the periods of 04 August 2020 to 05 May 2021 which occurred after its data center migration.[8]

EKI, through its Initial Report, is requesting for the authority to withhold public notification of the breach until such time AsiaPay "renders an actionable report to EKI" given that the information supplied by AsiaPay is nonspecific.[9]

Issue

Whether EKI's request for postponement of notification of data subjects should be granted.

Discussion

The Commission denies EKI's request for the postponement of notification of affected data subjects.

EKI is a Personal Information Controller (PIC).

[5] Id.
[6] Id.
[7] *See* Security Incident, accessed at https://www.asiapay.com/2021.html, as provided in the Initial Report.
[8] Id.
[9] 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

A PIC is defined as one "who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf."[10] Control is present when the entity "decides on what information is collected, or the purpose or extent of its processing."[11]

EKI is the owner and administrator of its website which sells various goods, services and merchandise, and its website provides avenues for online payment.[12] Particularly, customers are required to provide personal information (name, credit card number, and validation value) to confirm credit card payments on its website. This makes EKI a PIC since it determines and requires customers to provide such personal information. EKI is a PIC regardless of having AsiaPay as its online gateway partner, since AsiaPay is processing the personal data for the benefit and on behalf of EKI.

As the PIC, EKI has clear obligations under NPC Circular No. 16-03 (Personal Data Breach Management) relating to the notification of affected data subjects and the Commission, as well as providing crucial information about the data breach to the Commission and to the affected data subjects.

The data breach falls under mandatory data subject notification.

Under Section 11 of NPC Circular No. 16-03, notification must be done by the PIC upon knowledge or reasonable belief of a personal data breach that meets particular conditions, *to quote*:

> **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:

[10] Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, Section 3(h).
[11] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 3(m).
[12] Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.

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

> 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.[13]

Here, EKI reported that confirming credit card payments would require customers to input their names, credit card numbers, and credit card validation values.[14] These types of information relate to the financial and economic situation of data subjects. The information could also be used to enable identity fraud.

The information may also have been acquired by an unauthorized person, as AsiaPay itself publicly stated, through its website announcement, that "it is with regret that the Company now informs stakeholders and supporters that a highly sophisticated cyberattack on our systems has been discovered."[15]

It is also reasonably apparent that EKI believed that such unauthorized acquisition would likely give rise to a real risk of serious harm for affected data subjects. From its Initial Report, EKI met with AsiaPay's top management, and were promised to be updated about the breach.[16] This reveals the clear gravity of the situation. In any case, the Commission finds that the possible

---

[13] Section 11 of the NPC Circular No. 16-03.
[14] Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.
[15] *See* Security Incident, accessed at https://www.asiapay.com/2021.html, as provided in the Initial Report.
[16] Initial Report dated 31 August 2021 of Enchanted Kingdom, Inc.

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

acquisition of the names, credit card numbers, and credit card validation values gives rise to serious harm for affected data subjects.

There are only specific instances where the Commission may allow the postponement of notification of affected data subjects. Section 18(B) of NPC Circular No. 16-03 provides:

> **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
>
> B. *Exemption or Postponement of Notification*. If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement, or the postponement of the notification.
>
> xxx
>
> The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.

In this case, EKI does not allege that there is a pending criminal investigation, and its only reason for seeking postponement is its claim that "the information supplied by AsiaPay is nonspecific", and therefore, public notification should be withheld "until such time as AsiaPay renders an actionable report to EKI".[17]

As shown by AsiaPay's public posts on its website, it has already concluded a forensic investigation and determined the method and period when its systems were breached. EKI need not wait for AsiaPay to provide an actionable report to EKI, and should have been more proactive in seeking information on how the data breach

[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

affected EKI's customers availing of the credit card option for payment during the period relevant to the data breach.

EKI has also not provided the particular security measures it has done after learning about the breach in order to secure the affected data subjects' personal information. Thus, the Commission finds that with the type of personal data involved and the factual circumstances of the case, EKI shall have to notify the affected data subjects. Such notification to the affected data subjects is urgent and necessary in order to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.[18]

EKI has the further obligation to comply with the seventy-two (72) hour period to notify the Commission, and submit its Full Breach Report within five (5) days from notification, as provided under the NPC Circular No. 16-03.

Under Section 17(A) and (C) of NPC Circular No. 16-03, PICs are required to notify the Commission within seventy-two (72) hours from knowledge or reasonable belief of the data breach, and to submit a Full Breach Report within five (5) days from notification, *to quote:*

> **SECTION 17.** ***Notification of the Commission.*** The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> A. *When Notification Should be Done***. The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.**
>
> xxx

[18] Section 18(A) of the NPC Circular 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

> 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 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.[19] (Emphases supplied)

Here, EKI knew about the breach since 20 August 2021. It notified the Commission only on 31 August 2021, or beyond the seventy-two (72) hour-period. Further, EKI has yet to provide its Full Breach Report to the Commission pursuant to Section 9 and Section 17(D) of NPC Circular No. 16-03.

WHEREFORE, premises considered, this Commission **DENIES** the request of Enchanted Kingdom, Inc. (EKI) to postpone the notification of affected data subjects.

EKI is hereby **ORDERED within fifteen (15) days** from receipt of this Order to comply with the following:

1. **NOTIFY** the affected data affected subjects pursuant to Section 18 of NPC Circular No. 16-03 and submit proof of compliance thereof, including the proof of receipt of the data subjects of such notification;

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

3. **SUBMIT** proof of security measures to address the breach pursuant to Section 17(D) of NPC Circular No. 16-03; 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

[19] Section 17(A) and (C) 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

law, before the appropriate court, and such other actions as may be available to the Commission.

SO ORDERED.

City of Pasay, Philippines.
27 January 2022.

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

I CONCUR:

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

BMM
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