



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: ASIA UNITED
BANK CORPORATION

NPC BN 22-107

X-----X

RESOLUTION

NAGA, P.C.;

Before the Commission are the requests for exemption from the requirement of notification of affected data subjects and extension to submit full report submitted by Asia United Bank Corporation (AUB) dated 25 July 2022.

Facts

On 25 July 2022, AUB submitted to the Commission an initial report of a data breach through the Data Breach Notification Management System (DBNMS).¹

Based on the initial report, AUB stated that during the onset of the pandemic, delays in the handover of delivery receipts occurred due to the minimal workforce of Entrego, its service provider.² AUB made continuous follow-ups with Entrego to surrender the required delivery receipts, but to no avail.³ It was only on 18 July 2022 that Entrego reported to AUB that certain delivery receipts that serve as proof of delivery of credit cards were lost.⁴

¹ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Date of Notification of Asia United Bank Corporation (25 July 2022).

² *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology.

³ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.b Chronology.

⁴ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.a How breach occurred + DPS Vulnerability.

AUB reported that there are two hundred sixteen (216) recorded affected data subjects.⁵ However, AUB added that “the recipients of the two hundred sixteen (216) delivered credit cards are not the cardholders themselves.”⁶ AUB stated that:

However, if it is to be assumed that the recipients of the 216 delivered credit cards are not the cardholders themselves, then a maximum of 432 (i.e., 216 x 2) data subjects may expected (*sic*) to be affected - however, this number is highly speculative. It must be stressed that there are no copies of government-issued identification documents collected by Entrego - delivery receipts only state type of identification card and corresponding identification card number of the recipient of delivery.⁷

As for the personal data involved, AUB reported that the “[g]overnment-issued ID number unique to cardholder (*sic*) authorized representative; the fact that an AUB credit card was issued to a specific person” is information that may enable identity fraud.⁸

For the measures taken to address the breach, AUB stated that:

While it does not seem to be possible to recover/locate the lost delivery receipts, the affected delivered credit cards are in the process of being verified as having been successfully delivered to the correct cardholders. Based on initial investigation results, credit cards successfully reached the cardholders and have not been involved in fraud.⁹

Moreover, AUB reported that the security or recovery of personal data is “not possible under the circumstances.”¹⁰ In mitigating the harm, AUB also declared that an investigation was undertaken to determine

⁵*In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS/Records.

⁶ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS/Records

⁷ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.c Number of DS/Records.

⁸ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 2.b. Other info that may enable identity fraud.

⁹ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.a Measures to address the breach.

¹⁰ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.b. Measures to secure/recover personal data?

if any of the delivered credit cards had been involved in fraud.¹¹ AUB reported that based on the investigation, the credit cards were successfully delivered to the cardholders, and no fraud had occurred.¹²

AUB is then requesting for exemption from the requirement of notification of the affected data subjects.¹³ It stated that the request is “being made because it is unlikely that the breach will give rise to a real risk to the rights and freedoms of data subjects; rather, notification may cause unnecessary panic to cardholders.”¹⁴ AUB also mentioned that:

[I]t is not possible to trace who the actual delivery recipients had been other than to confirm whether the cardholders in fact eventually received the delivered credit cards. As such, it is not possible to undertake notification if the delivery recipient (whose name, signature and ID details are printed on a delivery receipt) is a person other than the cardholder.¹⁵

AUB is also requesting a fifteen-day extension “to submit full report in order to give time for the completion of the investigation. Progress of investigation is dependent on response time/quality of feedback from Entrego.”¹⁶

In a Minute Resolution dated 07 November 2022, the Commission resolved the requests for exemption and extension with the following dispositive portion:

WHEREFORE, premises considered, the Commission hereby **ORDERS** Asia United Bank Corporation to **SUBMIT** within fifteen (15) days upon receipt of this Minute Resolution the following:

¹¹ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?

¹² *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?

¹³ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Exemption.

¹⁴ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Exemption.

¹⁵ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Justification for Exemption.

¹⁶ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), in Explain the reason for the request for extension of time to submit.

- (1) Proof to substantiate the request for Exemption and Extension;
- (2) Further details and evidence of the security measures that have been implemented in response to the breach; and
- (3) Full Breach Report.

Should Asia United Bank Corporation fail to provide the foregoing documents, this case shall be submitted for resolution based on the records before the Commission.

SO ORDERED.¹⁷

Subsequently, AUB submitted its Compliance dated 22 November 2022 which contains the “full report of security incident,”¹⁸ attaching thereto a “Certificate of Delivery of Parcel” from Entrego,¹⁹ and a Certification from MVS, the incumbent Senior Vice President and Cards Business Group Head of AUB.²⁰

Further, AUB attached in its full report copies of the Certificates of Delivery Parcel issued by Entrego and clarified that “there are two hundred eighty-seven (287) individuals affected by the alleged breach” consisting of the “cardholders and/or the credit card recipients.”²¹

Issue

Whether to grant AUB’s requests for (1) exemption from notification of affected data subjects and (2) extension to submit its full report.

Discussion

The Commission resolves to deny the requests for (1) exemption from notification of data subjects and (2) a fifteen-day extension to submit its full report.

¹⁷ *In re: Asia United Bank Corporation*, NPC BN 22-107, Minute Resolution dated 07 November 2022, at p. 1.

¹⁸ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation.

¹⁹ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, Annexes “A” and “B”.

²⁰ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, Annex “C”.

²¹ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, in p. 2.

I. *The incident falls under the mandatory notification requirements.*

The Commission finds that the incident falls within the scope of mandatory breach notification requirement, thus, notification of the affected data subjects is necessary to protect them from the risk of serious harm.

Rule V, Section 11 of NPC Circular No. 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**. 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**.²² (Emphasis supplied.)

Based on the records, all the abovementioned requirements for mandatory breach notification are present.

First, AUB listed government-issued identification (ID) numbers as sensitive personal information.²³ AUB also reported that the

²² NPC Circular No. 16-03, Rule V, § 11.

²³ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 3.

cardholder's full name, delivery address, as well as the credit card recipient's name, and signature are information that may be used to enable identity fraud.²⁴

To note, government-issued IDs with peculiar information pertaining to an individual are considered sensitive personal information.²⁵ As regards the cardholder's full name, delivery address, credit card recipient's name, and signature, such information may be used to enable identity fraud. Further, these can be obtained wrongfully by another person and may be used by them to perpetuate fraud or deception, usually for economic gain. Here, the fact that the lost proofs of delivery pertain to credit cards, the data about the financial situation of the data subjects are also involved.

The second requirement is also present in this case. AUB mentioned in its initial report that:

In case certain lost delivery receipts were lost/misplaced outside the premises of Entrego, **there is a possibility that said delivery receipts would find their way to malicious persons.** However, malicious/unauthorized usage may be limited given the breadth of information involved.²⁶

Accordingly, AUB undertook an investigation to determine if the "delivered cards had been involved in fraud."²⁷ AUB reported that the credit cards had "successfully reached the cardholders and have not been involved in fraud."²⁸ However, AUB failed to sufficiently prove that indeed, no fraud has occurred. In its full report dated 22 November 2022, AUB failed to discuss the likely consequences of the lost delivery receipts.²⁹ Rather, AUB emphasized that the incident is attributable to Entrego.³⁰

²⁴ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 3.

²⁵ 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)(3) (2012).

²⁶ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 1.e Likely Consequences

²⁷ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?

²⁸ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.c Actions to mitigate harm?

²⁹ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 2.

³⁰ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 2.

Lastly, since AUB failed to sufficiently show that no fraud has occurred due to the lost of delivery receipts, the Commission finds that the personal and sensitive personal information involved can lead to potential harm or negative consequences to the credit cardholders or their authorized representatives. Thus, Section 11(C) of NPC Circular No. 16-03 applies.

It is noteworthy that AUB, as Personal Information Controller (PIC) has the obligation to notify the affected data subjects in case of breach which is within the scope of mandatory notification requirement. Thus, AUB is required to notify the affected data subjects in order to allow them to take the necessary steps or other measures to protect themselves against the negative effects of the breach.

II. Exemption from notification may be authorized by the Commission if such notification would not be in the public interest or in the interest of the affected data subjects.

AUB justifies its request for exemption by stating that the “notification may cause unnecessary panic to cardholders.”³¹ AUB also stated that “it is not possible to trace who the actual delivery recipients had been other than to confirm whether the cardholders in fact eventually received the delivered credit cards.”³² The Commission finds this justification unwarranted since in its full report, AUB was able to furnish this Commission copies of certificates of delivery of the credit cards showing the names of the recipients.³³

Rule V, Sections 18 (A) and (B) of NPC Circular No. 16-03 provide:

*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.*³⁴ (Emphasis supplied)

³¹ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for Exemption.

³² *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for Exemption.

³³ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 2.

³⁴ NPC Circular 16-03, Rule V, § 18(A).

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. **A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.** 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.³⁵ (Emphasis supplied)

In this case, AUB requested for exemption from notifying the data subjects since “it is unlikely that the breach will give rise to a real risk to the rights and freedoms of data subjects; rather, notification may cause unnecessary panic to cardholders.”³⁶ Section 18(A) of NPC Circular No. 16-03 requires the PIC to notify the affected data subjects within seventy- two (72) hours upon knowledge or reasonable belief that a breach has occurred. Section 18(B) thereof provides that exemption from notifying the data subjects may be granted if the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.

AUB failed to show proof that such notification would not be in the public interest or in the interest of the affected data subjects to warrant the exemption from notifying the affected data subjects. Even though this Commission has ordered AUB to submit proof substantiating its requests for exemption, AUB still failed to do so.³⁷

Thus, for failure to notify the affected data subjects within seventy-two (72) hours upon knowledge or reasonable belief of the occurrence of the breach, the Commission deems it proper for AUB to notify the two hundred eighty-seven (287) individuals affected. This is for them to take the necessary measures to protect themselves against the potential negative consequences resulting from the breach.

³⁵ NPC Circular 16-03, Rule V, § 18(B).

³⁶ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), Justification for Exemption.

³⁷ *In re: Asia United Bank Corporation*, NPC BN 22-107, Minute Resolution dated 07 November 2022, at p. 1.

III. AUB is required to submit its Full Breach Report

In its Initial Report, AUB reported that based on its investigation, the credit cards were successfully delivered to the cardholders and no incident of fraud has occurred.³⁸ However, AUB failed to make a report on the actions taken to inform the data subjects regarding the breach.³⁹

On the other hand, the full incident report of AUB dated 22 November 2022 does not mention any actions taken to inform the affected data subjects. Rather, it emphasized on Entrego's responsibility to deliver the credit cards to the cardholders and AUB's direct control is limited only to the issuance of credit cards.⁴⁰ AUB also stated that:

On the viewpoint of AUB, all credit cards subject of delivery by Entrego are in inactive/blocked status, and upon receipt by the relevant cardholders, require activation by each cardholder through a standard verification process.

...

As such, while unfortunate, AUB deems it unnecessary at this time to inform the Data Subjects on the loss of the delivery receipts. Notifying the Data Subjects of this incident may cause unnecessary panic on the part of the Data Subjects and blow the matter out of proportion, making it appear that the security measures of AUB are lax – although the loss of delivery receipts was accidental and purely attributable on the part of Entrego, a reputable courier. This reputational risk on the part of AUB will cause AUB irreparable harm as a financial institution with good standing, outweighing whatever imagined benefits there are to notifying the Data Subjects on such loss.⁴¹

However, this Commission finds that AUB shall submit its Full Breach Report containing the complete information required provided in Section 17(D) of the NPC Circular No. 16-03, including but not limited to the measures to secure/recover personal data and actions

³⁸ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.a Measures to address the breach; see 3.c Actions to mitigate harm?

³⁹ *In re: Asia United Bank Corporation*, NPC BN 22-107, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS), 3.d. Actions to inform data subjects.

⁴⁰ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 4.

⁴¹ DPO-Report NPC dated 22 November 2022 of Asia United Bank Corporation, at p. 4.

performed or proposed to mitigate possible harm, among others.⁴² In addition, the Commission also finds that AUB must submit proof of security measures it implemented as reported in its Initial Report dated 25 July 2022 and Full Incident Report dated 22 November 2022.

WHEREFORE, premises considered, this Commission resolves that the request for exemption and extension from the requirement of notification of the two hundred eighty-seven (287) affected data subjects of Asia United Bank Corporation (AUB) is hereby **DENIED**.

AUB is **ORDERED**, within fifteen (15) days from receipt of this Resolution, to comply with the following:

1. **NOTIFY** the affected data subjects including the proof receipt of the data subjects of such notification;
2. **SUBMIT** its Full Breach Report; and
3. **SUBMIT** proof of security measures to address the breach.

SO ORDERED.

City of Pasay, Philippines.
01 December 2022.

JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

⁴² NPC Circular 16-03, Rule V, § 17(D).

Copy furnished:

EMC
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission