IN RE: WESTERN UNION SERVICES (PHILIPPINES), INC.

NPC BN 18-151

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is Western Union Services (Philippines), Inc.'s (WUSPI) breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Facts

On 8 August 2018, WUSPI notified the National Privacy Commission (NPC) about a data breach that took place on 5 August 2018.[1] It involved one data subject from the Philippines whose personal data was disclosed to twenty-seven (27) individuals overseas.[2] The information was in electronic format and consisted of the data subject's name, address, primary phone number, email address, date of birth, occupation, the names of transaction counterparties, the relationship to the data subject and the transaction purpose.[3]

In its initial notification, WUSPI, on behalf of Western Union (WU) indicated the names of the Head of the Organization and the Data Protection Officer (DPO) as the responsible officers.[4]

WUSPI stated that WU runs a call cent[er] in the Philippines known as the Asia Pacific Regional Operations Cent[er] (AROC).[5] AROC utilizes a template Reinstatement Form to request information from

[1] Mandatory Breach Notification Letter, 08 August 2018, at 1, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[2] *Id.*
[3] *Id.*
[4] *Id.* at 1-2.
[5] *Id.* at 2.

individuals regarding certain transactions.[6] The data subject, being one of the clients, completed this form and sent it to WU.[7] WUSPI's employee, however, mistakenly sent the completed form to twenty-seven (27) other individuals.[8]

In response to the breach, WUSPI claimed that it took the following measures:

> - [It] contacted the recipients to delete the email and [data subject's] personal data;
> - Internal measures were undertaken to address the issue with [its] staff to avoid recurrence of the incident; [and]
> - [It] contact[ed] the affected data subject to notify her of the incident.[9]

WUSPI concluded its initial notification by stating that it is conducting further investigations to determine if any other individuals were affected by the breach.[10]

WUSPI also noted in its notification that it was "in the process of registering with the NPC and is one of the entities subject of a pending Request for Group DPO filed with the NPC on 27 February 2018 and refiled on 14 May 2018."[11]

On 15 October 2020, the NPC, through the Complaints and Investigation Division (CID), directed WUSPI to "submit a post-breach report detailing the results of the investigation conducted as well as the remedial measures taken to notify the affected data subjects, address the incident and prevent its recurrence" within fifteen (15) days from the receipt of the Order.[12]

On 28 March 2022, the CID issued another Order directing WUSPI, pursuant to Section 17(D) of NPC Circular 16-03, to submit a Full

---

[6] *Id.*
[7] Mandatory Breach Notification Letter, 08 August 2018, at 2, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.* at 1.
[12] Order, 15 October 2020, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2020).

Report detailing the incident within fifteen (15) days from receipt of the Order.[13]

On 08 August 2022, WUSPI sent a letter requesting an extension of time to submit its response.[14] In this letter, WUSPI explained that there was a delay in receiving the Order because it had been sent to the previous DPO, who left WU near the end of 2018.[15] The DPO who succeeded him also left WU on 3 June 2022.[16] Consequently, the current DPO was only able to register on 4 August 2022.[17] Given these circumstances, WUSPI's DPO requested an extension of time to submit a response.[18] She also stated that a response to the Order would be submitted within fifteen (15) days of receiving a copy of the incident report that WU submitted to the NPC.[19]

On 30 August 2022, the CID granted the request for extension.[20]

On 07 September 2022, WUSPI submitted its Compliance, including a full report detailing the incident as directed by the CID.[21] In its Report, WUSPI reiterated the details indicated in its initial notification to the Commission.[22] In its Report, WUSPI reiterated the details indicated in its initial notification, stating that the breach was caused by human error.[23] It claimed that WU employees are trained to send the blank Reinstatement Form template, which is stored on WU's SharePoint site, to customers upon request.[24] In this particular incident, however, instead of following the standard procedure to access the shared storage site, the employee mistakenly sent the Completed Reinstatement Form.[25]

---

[13] Order, 28 March 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[14] Request for Extension, 08 August 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Order, 30 August 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[21] Compliance, 07 September 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[22] *Id.*
[23] *Id.* at 2.
[24] *Id.*
[25] *Id.*

WUSPI added a chronology of the events that led to the loss of control over the data subject's personal data:

> Prior to July 30, 2018: The Western Union customer the [sic] completed the Reinstatement Form and sent the Completed Reinstatement Form to AROC
>
> July 30, 2018: An AROC employee mistakenly sent the Completed Reinstatement Form to 27 other customers.
>
> Between July 30 and August 2, 2018: One of the 27 customers to whom the Completed Reinstatement Form was sent notified AROC that the Completed Reinstatement Form [of] the customer had received contained information about another customer.
>
> Between July 30 and August 2, 2018: Western Union determined that in addition to the customer that reported receiving the populated Restatement Form, 26 other customers had received the same populated Form. Western Union emailed each of the 27 customers and requested that they delete the email that contained the data subject's personal information.
>
> August 3, 2018: Western Union's Data Protection Officer, WLT, was notified that a potential data privacy incident had occurred.
>
> August 5, 2018: Western Union's Data Protection Officer, WLT, determined that a reportable privacy incident had occurred.
>
> August 8, 2018: Following investigation into the incident, WLT submitted the incident notification to the NPC and sent the customer notification letter to the affected data subject.[26]

WUSPI asserted that the scope of disclosed data was limited, as only the personal data of one customer was inadvertently disclosed, and the categories of personal data were minimal.[27] It also alleged that "the completed reinstatement form did not contain any sensitive personal data, banking or funds source information, or the affected individual's national identification number."[28]

WUSPI claimed that the number of recipients was also limited, with the form being shared with only twenty-seven (27) individuals.[29] WUSPI contacted these individuals and instructed them to delete the

---

[26] *Id.*
[27] Compliance, 07 September 2022, at 3, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[28] *Id.*
[29] *Id.*

form.[30] WUSPI maintained that the recipients were not malicious actors but were customers seeking reinstatement of their own accounts.[31] According to WUSPI, since it is aware which customers received the data, any illegitimate use of the personal data could be traced back to those customers.[32]

Further, WUSPI contended that no systems or databases were compromised due to this incident.[33] The breach was caused solely by human error, and no system vulnerabilities were identified during the investigation that required remediation.[34] Additionally, WUSPI alleged that this incident occurred in July 2018, and it "has no knowledge of any illegitimate uses of the data subject's information since that time."[35]

WUSPI alleged that several safeguards had been in place to minimize the impact of the personal data breach and to prevent future incidents.[36]

WUSPI stated that after discovering the breach, it promptly sent emails to the twenty-six (26) customers as well as the one customer who had notified WUSPI of receiving the Completed Reinstatement Form.[37] Through these emails, WUSPI informed the customers about the error and instructed them to delete the form from their email accounts immediately.[38] WUSPI also alleged that it notified the individual whose personal data had been inadvertently disclosed, even though they assessed that the risk of harm was low.[39]

As part of its Compliance, WUSPI submitted a copy of the letter notice sent to the affected data subject,[40] along with a copy of the airway bill from the courier as proof of notification:[41]

---

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] Compliance, 07 September 2022, at 3, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Compliance, 07 September 2022, at 3-4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[40] Notification to Affected Data Subject, 08 August 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[41] Courier Receipt, 08 August 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).

> Dear [ ],
>
> I write on behalf of WU, regarding an incident involving personal data you provided recently in your reinstatement request for transaction with money transfer control number (MTCN) – [ ] - 7823.
>
> We regret to inform you that your data was inadvertently exposed in this Incident. The exposure included your full name, primary phone number, address, date of birth, occupation, email address, 455 and the names of your blood relatives from whom you received or to whom you sent money (and purpose for those transactions).
>
> Nature of the Breach.
> - You completed a reinstatement form and sent this to WU. The completed reinstatement form containing your information was mistakenly sent to 27 other individuals.
>
> Measures taken to Address the Breach.
> - Internal measures were undertaken to address the issue with our staff to avoid a recurrence of the incident.
>
> Measures taken to reduce the harm or negative consequences of the breach.
> - We have contacted the recipients to delete the email and your personal data.
>
> Do not hesitate to contact me for further information:
>
> Data Protection Officer WLT
>
> [Contact details]

WUSPI also claimed that disciplinary action had been taken against the employee who did not follow standard procedures.[42] It reminded the employee of the correct processes and issued a written disciplinary warning to prevent similar incidents from occurring in the future.[43] WUSPI contended that following the incident, the team in charge of sending reinstatement forms was reminded of the importance of adhering to the established processes.[44]

---

[42] Compliance, 07 September 2022, at 4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[43] *Id.*
[44] *Id.*

WUSPI maintained that an internal privacy policy had been in force at the time of the incident, which contained several provisions on the protection of personal information.[45] The policy included clauses such as collecting only necessary personal information,[46] using personal information for specific pre-defined purposes,[47] maintaining a comprehensive privacy and data protection training program,[48] implementing appropriate administrative, technical, physical, and organizational measures to protect personal information,[49] sharing only the minimum necessary personal information in a secure manner,[50] and enforcing disciplinary action for policy violations.[51]

WUSPI also attached its Information Classification Policy in its Compliance, which classified customer information as confidential and required all employees to protect this information, including providing heightened protections for confidential information.[52] In accordance with this policy, WUSPI required employees and departments to provide necessary information to demonstrate adherence and compliance which will be verified and documented by the Chief Privacy Officer (CPO) and the Chief Information Security Officer through Privacy Impact Assessments or Information Security Assessments.[53] Any violation of this Policy must be reported to the CPO or the Privacy Office, which will investigate and coordinate with relevant departments like HR, Legal, and Information Security to address and resolve any allegations of non-compliance.[54]

WUSPI claimed that it conducts mandatory global privacy training for all employees annually.[55] The training covered various aspects of data privacy and security, including the importance of data privacy laws, key privacy concepts, defining personal data, and handling individual data rights.[56] According to WUSPI, employees were also trained to

---

[45] *Id.*
[46] 2018 Privacy Policy, 17 May 2018, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[47] *Id.*
[48] *Id.* at 7.
[49] *Id.* at 8.
[50] *Id.*
[51] *Id.* at 10.
[52] Information Classification Policy, 24 June 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[53] *Id.* at 14.
[54] *Id.*
[55] Compliance, 07 September 2022, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[56] Privacy Training Continuing Education Visual Aid, 07 September 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).

recognize and manage privacy incidents in order to ensure compliance with relevant privacy laws and regulations.[57]

In addition, WUSPI alleged that it has a mandatory Corporate Information Security Program applicable globally to WU and its subsidiaries.[58] The program provided a framework for risk-based IT security measures.[59] WUSPI claimed that this program was designed to maintain the confidentiality of organizational information, safeguard against potential threats and hazards, ensure the availability and integrity of WU's data, and prevent unauthorized or illegal access to or use of its information assets.[60]

Issue

Whether WUSPI notified the affected data subject, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. WUSPI's submissions show that it properly notified its affected data subject, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

It is the responsibility of a Personal Information Controller (PIC), such as WUSPI, to ensure that affected data subjects of the breach are promptly and properly notified about the breach.[61] The Commission has consistently emphasized that the purpose of notifying data subjects of a breach is to enable them to take necessary precautions or other actions to protect themselves from potential consequences.[62]

Section 18 of NPC Circular 16-03 provides the requirements on the content and form of the notification of data subjects:

---

[57] *Id.*
[58] Compliance, 07 September 2022, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[59] *Id.*
[60] *Id.*
[61] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[62] *Id.* § 18 (A).

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:

. . .

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
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.

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.[63]

[63] NPC Circ. No. 16-03, § 18 (C) & (D).

Here, WUSPI notified the affected data subject about the incident through a letter sent by courier.[64] This aligns with the requirements set forth in Section 18(D) since it provides a direct and secure way to inform the affected individual while taking necessary precautions to protect her personal data from further unnecessary disclosure.

On the content of the notification, WUSPI identified the nature of the breach by informing the affected data subject that the completed reinstatement form containing the data subject's information was mistakenly sent to twenty-seven (27) other individuals.[65]

The notification specified the types of personal data that may have been exposed, including the full name, primary phone number, address, date of birth, occupation, email address, and the names of blood relatives involved in money transactions.[66]

The notification also outlined the immediate actions taken to address the breach, such as implementing internal measures to prevent recurrence and contacting the recipients to delete the email and personal data.[67]

WUSPI provided the DPO's contact information, including an email address and phone numbers, allowing data subjects to obtain additional information regarding the breach.[68] This satisfied the requirement to include contact information of a representative from whom more information could be obtained.[69]

In addition, WUSPI took measures to sufficiently address the breach and adopted measures to prevent its recurrence.[70]

Section 20 of Republic Act No. 10173 or the Data Privacy Act (DPA) provides that PICs must implement reasonable and appropriate

---

[64] Notification to Affected Data Subject, 08 August 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] NPC Circ. No. 16-03, § 18 (C).
[70] Compliance, 07 September 2022, at 4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).

organizational, physical, and technical measures intended for the protection of personal information against any unlawful disclosure:

> Section 20. *Security of Personal Information.* (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[71]

Disciplinary action was taken against the employee who failed to follow standard procedures, including a reminder of the correct processes and a written disciplinary warning.[72] The team responsible for sending reinstatement forms was reminded of the importance of adhering to established procedures.[73]

Even prior to the incident, WUSPI had an internal privacy policy, which included provisions for the protection of personal information.[74] This policy outlined practices such as collecting only necessary personal information, using it for specific pre-defined purposes, maintaining comprehensive privacy and data protection training programs, and enforcing appropriate security measures.[75]

WUSPI also has an Information Classification Policy, which stated that customer information is confidential and required heightened protections.[76] Moreover, WUSPI claimed that it conducted mandatory global privacy training for all employees annually, covering various aspects of data privacy and security.[77] In addition, WUSPI's Corporate Information Security Program provided a framework for risk-based IT security measures to maintain confidentiality, safeguard data, and prevent unauthorized access.[78]

---

[71] 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 § 20 (a) (2012).
[72] Compliance, 07 September 2022, at 4, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[73] *Id.*
[74] *Id.*
[75] 2018 Privacy Policy, 17 May 2018, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2018).
[76] Information Classification Policy, 03 April 2007, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[77] Privacy Training Continuing Education Visual Aid, 07 September 2022, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).
[78] Compliance, 07 September 2022, at 6, *in* In re: Western Union Servies (Philippines), Inc., NPC BN 18-151 (NPC 2022).

Given the foregoing, the Commission finds that WUSPI properly notified its affected data subjects and implemented sufficient measures to address the breach and prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-151 In re: Western Union Services (Philippines), Inc. is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
05 June 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

APG
Data Protection Officer
Western Union Services (Philippines), Inc.

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