IN RE: ACTIVE NETWORK, LLC. **NPC BN 18-035**

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

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is Active Network, LLC's (Active) breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Facts

On 19 March 2018, Active notified the National Privacy Commission (NPC) about a "security incident that may have involved unauthorized access to the personal information of 1,715 residents of the Philippines."[1]

In its Initial Report, Active narrated it identified suspicious activity on one of its systems.[2] The investigation conducted by Active and cybersecurity firms revealed that unauthorized third parties potentially accessed personal information provided by users between December 2016 and September 2017.[3] Active alleged that throughout this period, unauthorized third parties deployed codes designed to collect information manually entered by users on the checkout page of Active's website.[4] Consequently, personal details provided during the checkout process may have been accessed by these unauthorized third parties.[5]

[1] Initial Report, 19 March 2018, at 2, *in* In Re: Active Network, LLC. NPC BN 18-035 (NPC 2018).
[2] *Id.* at 4.
[3] *Id.* at 2.
[4] *Id.*
[5] *Id.*

Active explained that the personal information potentially accessed because of the incident includes names, addresses, email addresses, credit or debit card numbers, expiration dates, and cardholder verification codes.[6]

Upon discovering the "suspicious activity", Active stated that it "engaged leading cybersecurity firms to investigate the incident" and took measures "to enhance monitoring tools and security controls" to prevent similar activity in the future.[7]

Active also maintained that it reported the incident to "relevant payment card brands and related entities and to regulatory authorities in the United States and other jurisdictions.[8]

Active manifested that it had already notified the one thousand seven hundred fifteen (1,715) data subjects affected by the incident.[9] It also submitted a copy of the notification template in the Initial Report:

> Dear [NAME]:
>
> We are writing to inform you that we recently became aware of a security incident involving the ACTIVE Network, including ACTIVE Works and ACTIVE Endurance ("Active") which may have impacted your personal information.
>
> **What Happened**
>
> Active recently identified suspicious activity on one of its systems. We worked with leading cybersecurity firms to determine that the activity related to transactions manually keyed in by users while checking out on the Active website between December of 2016 and September of 2017. During this time period, unauthorized third parties distributed code that was designed to gather information manually keyed in by users on Active's checkout page, and personal information that you provided as part of the checkout process may have been accessed by these unauthorized third parties.
>
> **What Information Was Involved**
>
> The information may have included your name, address, email address, credit or debit card number, expiration date, and

[6] *Id.*
[7] Initial Report, 19 March 2018, at 2, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[8] *Id.*
[9] *Id.* at 3.

> cardholder verification code (the three- or four-digit value included on the front or back of payment cards and used for verification of certain transactions).
>
> **What We Are Doing**
>
> As soon as Active identified the suspicious activity, it engaged leading cybersecurity firms to investigate the incident and took steps to enhance its monitoring tools and security controls. Active has also taken steps to contain and remediate the incident and has notified regulatory authorities in the United States. Active is in the process of reporting the incident to the National Privacy Commission.
>
> **What You Can Do**
>
> We encourage you to be diligent in watching for unauthorized activity associated with your payment card accounts and to quickly report suspicious activity to your bank or credit card company. The phone number to call is usually on the back of the credit or debit card.
>
> **For More Information**
>
> We apologize for any inconvenience this incident may cause. You may contact us at [], between 8:00pm and 2:00pm (Manila time), Monday through Friday, if you have any questions or would like additional information about this incident.[10]

On 07 September 2018, the NPC, through the Complaints and Investigative Division (CID), directed Active to submit a Full Report on the incident within five (5) days from the receipt of the Memorandum.[11] In addition, the CID instructed Active to submit the following:

> 1. A copy of the report, within five (5) days of receipt of the Order, sent to the relevant payment card brands and related entities and to regulatory authorities in the United States and other jurisdictions;
> 2. Consolidated results of the investigation, within fifteen (15) days from receipt of the Order conducted by hired cybersecurity firms;
> 3. List of reported related incidents, within fifteen (15) days from receipt of the Order, from their data subjects in the Philippines.[12]

[10] *Id.* at 4-5.
[11] Memorandum, 07 September 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[12] *Id.*

On 19 September 2019, Active requested for an extension of time until 16 October 2018 or thirty (30) days from receipt of the Memorandum, to submit the Full Breach Report.[13] Active stated that it needed time to gather information and documents from different business units as well as third parties, thus, it will not be able to submit the Full Breach Report on the deadline.[14] Active, however, provided the following details in their request for extension:

- The investigation on the data breach has been completed.
- Philippine residents or citizens were affected by the data breach and such individuals have been notified on 19 March 2018.
- Third-party security experts have been engaged to investigate the data breach and they have since completed their investigation.[15]

On 15 October 2018, Active submitted its Compliance,[16] which included a Response to the Memorandum dated 07 September 2018, and the full report of the details of the incident as directed by the CID.[17] In its report, Active reiterated the chronology of the events that led to the alleged loss of control over the personal data.[18]

Active determined that an unauthorized individual utilized customer credentials to enter its network.[19] Active believes that the unauthorized individual took the credentials, initially designated for customer use to access specific sections of the system, from a customer rather than from Active, possibly through methods like phishing or social engineering.[20]

When it discovered the breach, Active implemented changes "to completely segment or airgap the point of entry of the unauthorized third party and customers from the remainder of Active's environment."[21] This measure ensures that neither the unauthorized

---

[13] Request for Extension, 19 September 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[14] *Id.*
[15] *Id.*
[16] Compliance, 15 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[17] Response to NPC's Memorandum dated 07 September 2018, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[18] *Id.*
[19] *Id.* at 2.
[20] *Id.*
[21] *Id.*

individual nor any other unapproved entity can use that specific point of entry for access.[22]

Active claimed that the investigation reveals that the unauthorized individual managed to gain additional access to Active's network and "the presentation layer of an application that is part of the checkout process."[23] Active believes that this access facilitated the injection of a malicious JavaScript code to overwrite the original JavaScript file associated with the entry of payment card data.[24] Although the malicious code has been removed from Active's systems, it operated on the browsers of customers, collecting information entered on the checkout page.[25]

Active noted that due to their regular release of new codes into production every three weeks, the malicious JavaScript code was eradicated with each new production release.[26] Based on Active's investigation, the attacker would then re-enter Active's systems and reintroduce the malicious code with each new release.[27] This pattern persisted until mid-September 2017, "resulting in a 'start/stop' cadence to the attacker activity,"[28] which posed challenges in identification, diagnosis, and investigation. Active has taken numerous steps to halt and address this activity.[29]

Active reaffirmed its belief that the unauthorized party inserted the malicious JavaScript between December 2016 and September 2017.[30] It stated that it initially found out about the concerns regarding transactions in October 2017.[31] Due to the complex nature of the incident, Active had to engage "multiple leading third-party forensics firms to determine what had occurred and who had been impacted."[32] Active enumerated the factors which complicated the incident:

---

[22] *Id.*
[23] Response to NPC's Memorandum dated 07 September 2018, at 2, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[24] *Id.* at 3.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] Response to NPC's Memorandum dated 07 September 2018, at 3, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[30] *Id.*
[31] *Id.*
[32] *Id.*

- Many of the initial reports of fraud were found to not be fraudulent activity. They were instead identified as normal chargebacks.
- The malicious JavaScript code was no longer present on Active's systems at the time of the investigation, and the unauthorized third party had undertaken extensive efforts to cover their tracks.[33]
- While the investigation was able to identify unauthorized access to the network, it was unable to identify data exfiltration from the network.
- As discussed above in response to question 1(a), the "start/ stop" cycle of attacker activity - whereby Active would release new production code that did not include the malicious JavaScript code every three weeks, after which the unauthorized third party would re-enter the systems and insert the malicious JavaScript code into the new code - made the situation difficult to investigate and diagnose.[34]

Active noted that this incident potentially impacted approximately 1,715 data subjects residing in the Philippines.[35] Active clarified, however, that it believes only a small subset of this total number was actually affected by the malicious JavaScript.[36] Active alleged that it chose to be cautious in its analysis by considering any data subject that could not be definitively excluded as potentially impacted.[37]

Active also stated that the personal data breach may result in payment card fraud[38] since the information involved includes the "name, address, email address, credit or debit card number, expiration date, and cardholder verification code (the three- or four-digit value included on the front or back of payment cards and used for verification of certain transactions).[39]

To address the breach, Active provided a list of primary remediation and containment measures that it took.[40] This includes enhanced endpoint protection technology and continuous 24x7 monitoring

---

[33] *Id.*
[34] *Id.* at 4.
[35] Response to NPC's Memorandum dated 07 September 2018, at 4, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.* at 5.
[40] *Id.*

through full system/network logging.[41] Active also strengthened both its access and authentication protocols with increased use of multifactor authentication alongside improvements in system audit policies, restricted service account use, and limited remote access.[42] Monitoring has been significantly heightened, incorporating File Integrity Monitoring to detect changes in production code and various forms of monitoring to analyze activity within the Active environment.[43] An enterprise-wide password reset has been executed, and segmentation in the Active environment has been enhanced, including specific "air gapping" or complete segmentation to isolate compromised areas.[44]

Lastly, Active notified the affected data subjects in the Philippines on 19 March 2018.[45] In its notification template, Active encouraged recipients to watch out for unauthorized activity and to quickly report any such activity to the relevant bank or payment card brand.[46] At the time of notification, Active claimed that it provided a toll-free call center which individuals could contact for questions or for additional information.[47] Active also mentioned that to their understanding, "any fraudulent activity in relation to the potentially compromised credit cards will be dealt with through the usual procedures of the issuing banks."[48]

Issue

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

Discussion

The Commission resolves to close the matter. Active's submissions show that it properly notified its affected data subjects, sufficiently

---

[41] Response to NPC's Memorandum dated 07 September 2018, at 5, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.* at 6.
[46] Initial Report, 19 March 2018, at 4, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[47] *Id.* at 5.
[48] Response to NPC's Memorandum dated 07 September 2018, at 6, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).

addressed the breach, and implemented measures to prevent its recurrence.

It is the obligation of a Personal Information Controller (PIC), such as Active, to ensure that affected data subjects of the breach are promptly and properly notified.[49] The Commission has consistently emphasized that the purpose of the required notification to the data subjects of a breach is to allow them to take the necessary precautions or other measures to protect themselves against its possible effects.[50]

Section 17 (D) (3) of NPC Circular 16-03 provides the obligation of a PIC to notify the NPC of a personal data breach and outlines the content of notification, specifically the measures that a PIC should take to address the breach:

> Section 17. *Notification of the Commission*. The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> . . .
>
> D. *Content of Notification*. The notification shall include, but not be limited to:
>
> . . .
>
> 3. Measures Taken to Address the Breach
>   a. description of the measures taken or proposed to be taken to address the breach;
>   b. actions being taken to secure or recover the personal data that were compromised;
>   c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
>   d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
>   e. the measures being taken to prevent a recurrence of the incident.[51]

[49] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[50] *Id*.
[51] NPC Circ. No. 16-03, § 17 (D) (3).

In this case, Active notified its affected data subjects through a letter sent through email.[52] Active informed the affected data subjects about the security incident involving Active, as seen in the notification template attached to the Initial Report.[53] It included an explanation on the nature of the incident revealing suspicious activity on its systems related to manually keyed transactions on the Active website between December 2016 and September 2017.[54]

Active informed the affected data subjects that unauthorized third parties accessed personal information, including names, addresses, email addresses, and payment card details.[55] It also explained how it responded to the security incident by engaging cybersecurity firms, enhancing security controls, and notifying regulatory authorities.[56] Active advised the data subjects to remain vigilant for unauthorized activity on their payment card accounts and provided a contact number for inquiries.[57]

Active took measures to sufficiently address the breach and adopted measures to prevent its recurrence. Active promptly informed affected data subjects about the breach, acknowledging the real risk of serious harm.[58] This immediate communication allowed data subjects to take necessary precautions against potential adverse effects. It also established a toll-free hotline to facilitate communication with potentially affected data subjects, making it easier for them to obtain information and have their questions addressed promptly.[59]

Active engaged the services of a third-party cybersecurity firm to investigate the breach incident and significantly bolstered its technical security measures to effectively address the breach and fortify its cybersecurity defenses against potential future threats.[60]

These measures include the enhancement of endpoint protection technology to strengthen security as well as continuous monitoring

---

[52] Initial Report, 19 March 2018, at 3, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[53] *Id.* at 2.
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] Initial Report, 19 March 2018, at 2-3, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[59] *Id.* at 3.
[60] *Id.* at 2.

and full system/network logging.[61] Active also improved its access and authentication protocols through the expanded usage of multifactor authentication.[62]

Active strengthened its system audit policies and imposed restrictions on the use of service accounts and limited remote access. Monitoring measures were significantly intensified, incorporating File Integrity Monitoring to detect and alert on changes to the production code.[63] Active also executed an enterprise-wide password reset to render compromised credentials ineffective.[64] Active also implemented enhanced segmentation, including specific "air gapping," effectively isolated the point of entry used by the unauthorized party, preventing further unauthorized access.[65]

Given the foregoing, the Commission finds that the measures undertaken by Active have sufficiently addressed the incident and prevents its recurrence.

WHEREFORE, premises considered, the Commission resolves that the matter of NPC BN 18-035 In re: Active Network, LLC is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

---

[61] Response to NPC's Memorandum dated 07 September 2018, at 5, 11 October 2018, *in* In Re: Active Network, LLC, NPC BN 18-035 (NPC 2018).
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.* at 5-6.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

PP
Compliance Officer
Active Network, LLC

JAH
Counsel for Active Network, LLC

ANGARA ABELLO CONCEPCION REGALA
& CRUZ LAW OFFICE
Counsel for Active Network, LLC

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