Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: ABS-CBN CORPORATION **NPC BN NO. 18-179**

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

ORDER

AGUIRRE, D.P.C.:

This Order refers to a breach notification report sent by ABS-CBN Corporation (ABS-CBN) regarding possible unauthorized access and acquisition of personal data of customers of its online store.

The Facts

On 18 September 2018, ZDNet published an article[1] entitled "Broadcaster ABS-CBN customer data stolen, sent to Russian servers." According to the article, the payment skimmer, which intercepts the checkout process through an obfuscated malware hidden within a JavaScript file, has been in operation since 16 August of the same year. According to Dutch security researcher WDG, the malicious code scrapes the financial information of payment cards used by customers attempting to buy merchandise from the store. This information is then transferred to a payment collection server called adaptivecss.org, which is registered in Irkutsk, Russia.[2]

On 19 September 2018, the publication of the article was reported to ABS-CBN's Data Protection Officer (DPO), Mr. JCG, who contacted the company's Managed Security Service Provider (MSSP) - Symantec, to report the security incident and assist in the immediate investigation and containment procedures. Investigations conducted by the MSSP revealed that a file with a backdoor program was uploaded on ABS-CBN's website that created a form and submitted the information to the attacker. A total of two-hundred eight (208) unique customers were

---

[1] Charlie Osborne, Broadcaster ABS-CBN customer data stolen, sent to Russian servers, *available at* https://www.zdnet.com/article/broadcasting-giant-abs-cbn-customer-data-stolen-sent-to-russian-servers/ (Last accessed: 07 January 2021, 10:49PM)
[2] *Id.*

affected by the breach. Based on the investigation of the MSSP, the malicious code collected the name, complete address (including the city, state, country and zip code), email address, phone number, shop, and credit card details (including credit card name, number, expiration date and CVV) of ABS-CBN's online store customers. On the same day, ABS-CBN's DPO sent a formal notification to the Commission.

On 21 September 2018, the MSSP reported that based on the available evidence, Symantec Incident Response can state with high confidence that the attack is consistent with the so-called Magecart[3] campaign. Further, ABS-CBN claimed that the data breach incident is limited only to the ABS-CBN Store website and does not affect other ABSCBN digital properties.[4]

ABS-CBN reportedly took the following measures to address the incident upon knowledge of the compromise:

1. The publication of the article was immediately reported by an IT staff to the ABS-CBN DPO;

2. ABS-CBN engaged its MSSP to assist in the investigation, containment procedures and remediation activities;

3. ABS-CBN also invoked its Incident Response Retainer from the same MSSP;

4. The compromised ABS-CBN online store was taken down on 19 September 2018 at 09:28AM;

5. Upon receipt of additional information from internal Security Analysts, ABS-CBN has also taken down the UAAP Store (www.uaapstore.com) as a precautionary measure;

6. An informal notification was sent via SMS by the ABS-CBN DPO to NPC Commissioner Raymond Liboro who acknowledged receipt thereof;

---

[3] "Magecart, a threat group which has been active since 2015, specializes in compromising online stores and obfuscating malicious code in JavaScript in order to steal payment card information entered into store checkout pages." Charlie Osborne, Broadcaster ABS-CBN customer data stolen, sent to Russian servers, *available at* https://www.zdnet.com/article/broadcasting-giant-abs-cbn-customer-data-stolen-sent-to-russian-servers/ (Last accessed: 07 January 2021, 10:49PM)
[4] Email Notice: Personal Data Breach Incident dated 19 September 2018.

7. A Press Release was published by ABS-CBN Corporate Communications on the data breach;

8. The concerned personnel from IT, Retail and Infosec Head/DPO called for a meeting with the Third-Party Vendor to discuss technical details and remediation plans;

9. On 19 September 2018, the Head of Retail sent the list of affected customers to Head of iConn Operations (Customer Service) for email notification and callouts where two hundred two (202) affected data subjects were notified via email or contact number and six (6) customers were notified via postal mail;

10. ABS-CBN also advised the affected customers to immediately change their account passwords, inform their bank and credit card provider and follow their advice, refrain from providing personal and/or financial information to anyone claiming to be an ABS-CBN representative, and report to ABS-CBN if the aforementioned case was encountered;

11. On 20 September 2018, the MSSP found suspicious logins from one of the administrator accounts of the Third-Party Vendor, the Third-Party Vendor immediately reset administrator passwords and run virus scans on all personnel laptops.

To prevent the recurrence of the incident, ABS-CBN undertook the performance of the following measures:[5]

1. Magento Lockdown:
    a. Restriction of access to all administrative interfaces to specific systems only;
    b. Restriction of access to all administrative interfaces based on firewall policies;
    c. Application of multi-factor authentication for all administrative accounts;
    d. Removal of the Magento Connector Manager since this is a common target for malicious adversaries;

[5] Full Breach Report dated 24 September 2018.

e. Conduct regular vulnerability scanning of the site in order to detect any potential weakness;

2. For auditing, apply the company's log retention policies to services hosted by external providers;

3. Devise a backup strategy for the production website and store the backups in a safe location outside of an attacker's influence; and

4. Notify law Enforcement to take down the infrastructure 'adaptivecss.org' since the malicious code is designed to post customer payment card information on the said site.[6]

On 27 September 2018, the Commission, through the Complaints and Investigations Division (CID), met with the ABS-CBN DPO where the Commission requested for a copy of the logs, decoded malware and the basic Magento scanner used by ABS-CBN in addressing the incident. ABS-CBN provided the needed logs and malware samples via email to the NPC.

On 11 October 2018, another meeting was held between the CID and the ABS-CBN representatives, where ABS-CBN was required to submit a supplemental update on ABS-CBN's and its E-Commerce provider's additional mitigation and remediation activities.

On 16 October 2018, a supplemental update was sent via email by the ABS-CBN DPO.[7] The update stated that the two-factor authentication for super administrators, as part of its role-based access controls,[8] and an additional IP Whitelisting enabled on production environment on its jump server,[9] were already completed. On E-Commerce hosting, ABS-CBN explained that they will migrate to Sonassi Hosting provider from Nexcess to include additional features such as separate servers for web app and database, web application firewall, extended off-site

---

[6] Upon access, the website shows an article entitled "Semalt Expert: Visual Content Tips". Last accessed: 12:37AM, 08 January 2021.
[7] Supplemental update dated 16 October 2018.
[8] Role-based access control (RBAC) restricts network access based on a person's role within an organization.
[9] A jump server, jump host or jump box is a system on a network used to access and manage devices in a separate security zone.

back-ups and server logs. According to ABS-CBN, the signing of proposal was set on 05 November 2018.

Moreover, ABS-CBN already completed the disabling of Magento Connect and Magento Security Scanning (staging server), while the scanning and remediation of web application server on staging environment prior to restoration and the work with specific business unit and finalization of data retention for its online stores were expected to be completed by 26 October 2018. The scanning of web application server on new production environment pending the migration to new server was set to be completed on 05 November 2018.[10]

On 05 November 2018, another email was sent by the ABS-CBN DPO regarding minor updates on ABS-CBN's remediation activities. According to ABS-CBN, with regard to E-Commerce hosting, it has completed its migration to Sonassi Hosting provider from Nexcess on 29 October 2018 and that it has decided to host the web application server and Database in an Amazon Web Service (AWS) environment managed and monitored by ABS-CBN. The scanning and remediation of web application server on staging environment prior to restoration was completed on 26 October 2018. The scanning of web application server on new production environment 's completion was moved to 06 November 2018. ABS-CBN also informed this Commission of its target to go live for store website on 08 November 2018.

On 15 November 2018, ABS-CBN submitted their vulnerability scan report for the scenarios prior to restoration and after migration. In their submitted report, the number of vulnerabilities discovered on their web application after restoration and migration were reduced from sixty-one (61) to thirty-one (31). Moreover, of the thirty-one (31) vulnerabilities detected after migration, twenty-nine (29) of these vulnerabilities, which were classified as high risk by the scan, were found to be false positives[11]. ABS-CBN informed this Commission that they planned to relaunch the website on 16 November 2018.

Discussion

[10] Supplemental update dated 16 October 2018.
[11] A false positive state is when the IDS identifies an activity as an attack, but the activity is acceptable behavior.

Upon careful inspection of the reports and documents submitted by ABS-CBN, the Commission finds the absence of any proof of notification to the affected data subjects as well as proof of receipt of the said notification. NPC Circular 16-03[12] requires that all actions made by a personal information controller should be properly documented. This includes compliance with the notification requirements and assistance to affected data subjects:

> **SECTION 9.** ***Documentation.*** All actions taken by a personal information controller or personal information processor shall be properly documented. Reports should include:
>
> A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
> B. Actions and decisions of the incident response team;
> C. Outcome of the breach management, and difficulties encountered; and
> D. Compliance with notification requirements and assistance provided to affected data subjects.
>
> A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.

As to the manner of notification to the affected data subjects, Section 18(A) of NPC Circular No. 16-03 provides that:

> 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. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. **It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.** It may be supplemented with additional information at a later stage on the basis of further investigation.[13]

---

[12] National Privacy Commission, Personal Data Breach Management, Circular No. 16-03 (December 15, 2016).
[13] Emphasis supplied.

Moreover, Section 18(D) of same Circular provides that:

> 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.[14][15]

As stated by the Commission in its Resolution for NPC BN 20-161,

> 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.[16]

Notification to the affected data subjects in cases of personal data breach is an essential obligation in data privacy protection. Section 20 (f) of the DPA of 2012 states that:

> SEC. 20. *Security of Personal Information.* –
>
> xxx

---

[14] Emphasis supplied.
[15] Supra, Note 2.
[16] NPC BN 20-161, 17 December 2021.

> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

The Commission notes that ABS-CBN merely stated the following in its Incident Report:

> **REMEDIAL MEASURES**
>
> xxx
>
> b. The following security measures were advised to the affected customers:
> - Immediately change their account passwords.
> - Inform their bank and credit card provider immediately and follow the bank/credit card provider's advice.
> - Not provide any personal and/or financial information to anyone who may claim to be an ABS-CBN representative.
> - If the aforementioned case was encountered, report the incident to ABS-CBN by emailing abs-cbnstore@abs-cbn.com.

Pursuant to the requirements of Section 18(A) and Section (D) of NPC Circular 16-03, the Commission orders ABS-CBN to submit proof of notification to the two hundred eight (208) affected data subjects.

WHEREFORE, the Commission **ORDERS** ABS-CBN Corporation to submit proof of notification to the two-hundred eight (208) data subjects who were affected by the breach, **within fifteen (15) days** from receipt of this Order.

SO ORDERED.

City of Pasay, Philippines;
11 March 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JCG
Data Privacy Officer
ABS – CBN Corporation

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