IN RE: EASYTRIP SERVICES CORPORATION

NPC BN 17-028
NPC BN 18-180

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is the breach notification submitted by Easytrip Services Corporation (ESC) involving the unauthorized access and manipulation of an ESC account by means of an illicit Structured Query Language (SQL) injection in a mobile application.

Facts

On 25 October 2017, an ESC sales personnel detected a post on the "Buy and Sell Philippines" Facebook group selling ESC load "at 30% off through the PayMaya mode of payment."[1] ESC reported that it did not authorize the post as a valid promotion during that time.[2]

The seller of the ESC load was named "CB" who is not an ESC employee, customer, or business partner.[3] Since this was not an official promotion, the sales personnel reported the matter to the ESC Operations Management for investigation.[4]

After further investigation, ESC discovered that the seller enticed potential customers to top-up an amount of One Thousand Pesos (Php 1,000.00) in their ESC accounts at the cost of only Seven Hundred Pesos (Php 700.00).[5] After the transaction, the buyer would have to pay the

---

[1] Full Report, 19 September 2018, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[2] *Id.*
[3] *Id.* at 2.
[4] *Id.*
[5] *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

seller in the latter's PayMaya account by paying through a 7-11 branch.[6]

Subsequently, ESC created a dummy account and contacted the seller through Facebook Messenger.[7] Thereafter, the dummy account asked the seller to reload One Thousand Pesos (Php 1,000.00) as a prerequisite to receiving the payment.[8]

ESC narrated that "it ran all auditing and logging tools on the system to capture the said reloading activity."[9] After the transaction, ESC stated that an additional One Thousand Pesos (Php 1,000.00) was added to the running balance.[10] ESC, however, discovered that there was no description, credited amount, or total amount added to the Statement of Account (SOA) to show that a legitimate reload transpired.[11]

ESC further stated that "the balance of the dummy account gained an additional One Thousand Pesos (Php 1,000.00) despite the fact that there was no actual monetary transaction with ESC."[12] ESC explained that there were "no traces of the typical logs" that is usually remarked in a legitimate transaction.[13]

On 03 November 2017, ESC notified the National Privacy Commission (NPC) of the incident.[14] ESC explained that an infiltrator with username "sa7" managed to perform a SQL injection on the account using an Android Balance Inquiry Application called "finandroid."[15] This enabled the seller to access and manipulate certain information in the ESC account.[16]

---

[6] Full Report, 19 September 2018, at 2, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Full Report, 19 September 2018, at 2, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[13] *Id.*
[14] Easytrip Breach Report, 03 November 2017, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2017).
[15] *Id.*
[16] Full Report, 19 September 2018, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).

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

ESC identified that SQL injection was performed in a specific part of a mobile application dedicated to ESC customer inquiries.[17] This part of the application was specifically related to information on the account balance of ESC customers.[18]

ESC stated this specific system covers the following information: (1) balance of the account; (2) name of account holder; (3) account number; (4) last reload of account; and (5) the on-board unit number.[19] ESC's investigation reveals that the compromised data include the balance of the dummy account.[20]

To address the issue, ESC's third party company, Egis Projects Philippines Incorporated Software Development Center (EPPI SDC) reported that ESC adopted the following measures:

a. Disabled identified Web Service and Applications possibly used by perpetrator;
b. Created a new secured web service;
c. Updated and secured ESC Android Mobile POS Reloading;
d. Updated and secured ESC Android Mobile POS Balance Inquiry for POS;
e. Disabled Online Reloading facility for GP, upgrade Work in Progress;
f. Pending update and deployment of Android Mobile balance inquiry for ESC Customer;
g. Investigation and audit of other web services.[21]

ESC reported that it "adjusted sensitivity and adaptability of *PFsense firewall* to block additional IP threats on the firewall" to reduce the harm or negative consequences of the breach.[22]

Specifically, ESC's measures include "caching of Web Server content to lessen server load, creating page rules for Hypertext Transfer Protocol Secured (HTTPS), twenty-four (24) hours reporting on all passing through web traffic, Internet Protocol (IP) white listing and

---

[17] Full Report, 19 September 2018, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] Easytrip Breach Report, 03 November 2017, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2017).
[22] *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

block listing, and checking of all incoming web browser for possible threats."[23]

ESC hired a security expert for additional mitigation and resolution to prevent a recurrence of the incident,.[24] It also subscribed to "Anti Distributed DenialofService (DDoS) Attack" which aims to filter network traffic for threats and other suspicious activities.[25] It created a "DdoS Playbook" to protect and provide alerts to the organization for imminent threats in similar future scenarios.[26] It implemented an infrastructure upgrade to gather "recent patches and upgrades regarding newly upgraded cyber threats."[27] Lastly, ESC subscribed to Cloudflare, an IT service management company, to further strengthen its security.[28]

ESC narrated that apart from the dummy account that the seller accessed, there were no indications that other accounts were accessed.[29] ESC also explained that neither received complaints nor reports since the date of the incident that would indicate otherwise.[30]

On 19 September 2018, ESC submitted its Full Report on the incident.[31]

On 20 May 2022, ESC submitted a Comprehensive Technical Report in reference to the incident.[32]

On 22 June 2022, ESC provided additional information and proof in reference to the Data Breach Report submitted on 03 November 2017.[33] ESC likewise submitted proof of the remediation efforts it conducted as a Personal Information Controller (PIC).[34]

---

[23] Easytrip Breach Report, 03 November 2017, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2017).
[24] *Id.*
[25] *Id.*
[26] Full Report, 19 September 2018, at 5, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Compliance, 11 November 2022, Annex C, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2022).
[33] *Id.* Annex D.
[34] *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

On 27 October 2022, the NPC, through its Complaints and Investigation Division (CID), ordered ESC to submit a full breach report detailing the incident containing the following information: (1) nature of the breach, (2) personal data possibly involved, and (3) remedial measures taken subsequent to suspected breach.[35]

On 11 November 2022, ESC submitted its Full Report containing its initial notification to the NPC, its Full Report submitted on 19 September 2018, the letter containing the Comprehensive Technical Report dated 20 May 2022, and the letter containing additional information and proof dated 22 June 2022.[36]

Issue

Whether the breach incident falls under mandatory breach notification.

Discussion

The Commission finds that this matter does not fall under mandatory breach notification. Thus, the Commission resolves to close the case.

Section 11 of the NPC Circular 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

[35] Order (to submit Full-Breach Report), 27 October 2022, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2022).
[36] Compliance, 11 November 2022, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2022).

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

> 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.[37]

As such, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[38]

The first requisite provides that the breach involves sensitive personal information or information that may be used to enable identity fraud. Section 3 (l) of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) defines sensitive personal information as:

> Section 3. *Definition of Terms*.
>
> . . .
>
> (l) Sensitive personal information refers to personal information:
>
> (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

---

[37] National Privacy Commission, Personal Data Breach Management, Circular No. 3, Series of 2016 [NPC Circ. No. 16-03], §11 (15 December 2016).
[38] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a *Sua Sponte* NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2023).

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

> (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
>
> (3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
>
> (4) Specifically established by an executive order or an act of Congress to be kept classified.[39]

In this case, the account balance and account number of the dummy account were the only compromised personal information as a result of the breach.[40] These are not considered as sensitive personal information as defined under Section 3 (l) of the DPA nor as information that may enable identity fraud.

In fact, the account number and balance of the dummy account, absent any accompanying information, may not be considered personal information since it does not specifically point to the identity of a specific person. Thus, the first requisite is not present.

For the second requisite, there is reason to believe that the information may have been acquired by an unauthorized person. The seller, an unauthorized person, gained access to the dummy account's number and balance through the mobile application.[41]

Lastly, the third requisite that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject is absent in this case.

---

[39] 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) (2012).
[40] Full Report, 19 September 2018, at 2-3, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[41] *Id.* at 1.

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

To determine whether there is a likelihood that the unauthorized acquisition of information will give rise to a real risk of serious harm, there shall be a relation between the incident and any possible resulting harm to affected data subjects. The risk shall be apparent and not a product of mere speculation. Consequently, "serious harm" means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.

In determining whether the unauthorized acquisition is likely to give rise to a real risk of serious harm, a PIC or the Commission may consider several factors such as: the nature of the information involved in the breach, amount of information of a data subject, period of time lapsed from the breach, purpose of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of information involved in the breach, if any.

Here, there was no reported harm to any other data subject since it was only the dummy account's information that was compromised. There were also no significant consequences or effects as a result of the incident since there were no reports or complaints received by ESC coming from other ESC account holders.[42]

The nature of the information involved in the breach only involves fabricated information since the dummy account was only created by the ESC team to entrap the seller.

With regard to the amount of information involved, the breach only affected the account and balance of the dummy account and it did not affect the ESC database which includes other customer information such as license plates, taxpayer identification number (TIN), addresses, and contact numbers.[43]

Further, no other personal data was involved in the breach because ESC's team immediately ran all auditing and logging tools on the

[42] Full Report, 19 September 2018, at 5, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[43] *Id.* at 1.

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

system to capture the said reloading activity between the seller and the dummy account.[44]

As part of ESC's security measures, it hired third party security experts to strengthen its technical measures and to avoid the extent of the potential misuse and exposure of information involved in the breach.[45] ESC also added security measures to prevent data leakage by Internet Protocol (IP) Blocking, disabling its internet control message protocol (ICMP), strengthening its web application firewall (WAF), creating a new web service, creating ESC android mobile reloading and balance inquiry, and disabling online reloading facility for global payments.[46] Thus, ESC observed stringent technical measures to minimize any possible harm or any potential negative consequences of the breach to its customers.

Considering all these factors, the unauthorized acquisition did not give rise to a real risk of serious harm to any affected data subject. Thus, the third requisite is absent.

Since the first and third requisites for mandatory breach notification are absent in this case, the Commission finds that the breach reported by ESC does not require mandatory breach notification.

Section 20 (a) and (c) of the DPA provides for the obligation of PICs in implementing security measures for the protection of personal information:

> 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.
>
> . . .

[44] *Id.* at 2.
[45] Easytrip Breach Report, at 1, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).
[46] Full Report, 19 September 2018, at 4, *in* In Re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180 (NPC 2018).

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) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:
>
> (1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;
>
> (2) A security policy with respect to the processing of personal information;
>
> (3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
>
> (4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.[47]

The Commission takes this opportunity to remind PICs of their constant responsibility to protect the personal data of its data subjects against accidental, unlawful, or unauthorized interference. When implementing security measures, the PIC should consider the nature of the personal information, current data privacy best practices, and security measures considering the developments in technology and the risks that data subjects are being subjected to in order to guarantee that the personal data it processes are continuously safeguarded.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 17-028 and NPC BN 18-180 In re: Easytrip Services Corporation is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
11 May 2023.

---

[47] Data Privacy Act of 2012, § 20.

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

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

(on official leave)
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

LAL
Data Protection Officer
Easytrip Services Corporation

COMPLAINTS AND INVESTIGATION 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