IN RE: ABOITIZ LAND, INC.

NPC BN 18-071

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

ORDER

Before the Commission is the compliance[1] of Aboitiz Land, Inc. (Aboitiz Land) dated 03 November 2022 with the Order of the Commission through the Complaints and Investigation Division (CID) dated 14 October 2022.[2]

On 02 May 2018, an unverified information was received by Aboitiz Land that the hashed values of the log-in credentials (not the actual usernames and passwords) for its website were leaked online.[3] Aboitiz Land investigated the incident, and it was found that the website contained resumes and government-issued IDs of 19 (nineteen) job applicants.[4] On 07 May 2018, Aboitiz Land discovered that the database contained two hundred seventy-six (276) records through the website's "Contact Us" form, which include the mentioned 19 applicants.[5] Aboitiz Land also found possible evidence of unauthorized access as the log-in credentials from its website were posted on a Facebook group called "Pinoy Lulz Security" on 25 April 2018.[6]

Aboitiz Land stated that at that time, there was no conclusive evidence of unauthorized acquisition of records.[7] Lastly, during a meeting with its IT security consultant (RedRock Security), Aboitiz

---

[1] Post-Breach Report dated 03 November 2022 of Aboitiz Land, Inc.
[2] *In re: Aboitiz Land, Inc.*, NPC BN 18-071, Order dated 14 October 2022.
[3] Breach Notification dated 09 May 2018 of Aboitiz Land, Inc., at p. 4.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] Breach Notification dated 09 May 2018 of Aboitiz Land, Inc., at p. 5.

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

Land acknowledged the possibility of unauthorized acquisition of records.[8]

On 09 May 2018, Aboitiz Land notified the Commission of a possible personal data breach and stated that-

> The CMS website contains a database of information collected through the website's "Contact Us" form. The database contains less that three hundred (300) records containing names and contact details of individuals who submitted information through the website's "Contact Us" form. Out of less than three hundred (300) records, approximately less than twenty (20) records contain sensitive personal information or any other information that may be used to enable identity fraud.[9]

In its Initial Report, Aboitiz Land also included a discussion of Section 11 of NPC Circular No. 16-03 (Personal Data Breach Management) stating that although the incident involves sensitive personal information,

> [T]here is no conclusive evidence that those records were actually acquired by an unauthorized person. However, the available evidence supports the conclusion that an unauthorized person was able to enter and access the system. Given that the second condition uses the phrase "may have been acquired", Aboitiz Land acknowledges the "possibility" that an unauthorized person acquired those records.
>
> Aboitiz Land believes that there is minimal risk of serious harm to all data subjects. At most, only nineteen (19) data subjects, whose resumes/CVs or government-issued IDs were uploaded to the website, are at risk of a possible unauthorized acquisition of their sensitive personal information. Such sensitive personal information pertains to details that would otherwise be publicly available online, e.g., through LinkedIn and Facebook profiles and other social media platforms. As discussed, there is no evidence yet of actual unauthorized acquisition of those records[.][10]

---

[8] *Id.*
[9] *Id.,* at p. 1.
[10] *Id.,* at p. 2.

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

According to Aboitiz Land, the sensitive personal information of the 19 data subjects involve their birthday, age, civil status, nationality, gender, religion, health information (weight and height), educational background, government-issued certificates and IDs, their parents' names, including mother's maiden name.[11] Collectively, Aboitiz Land reported a total of 276 data subjects whose personal data also involve their names, addresses, and contact details.[12]

Aboitiz Land also stated that upon initial investigation, its website is vulnerable to Structured Query Language (SQL) injection which is most likely to cause the unauthorized access.[13]

As one of its immediate corrective actions, Aboitiz Land redirected its website to the Seafront Residences website and changed the password of the administration account.[14] Further, Aboitiz Land reported the measures it implemented to address the incident, among them is the coordination with LEENTech Network Solutions (LNS) to take down Aboitiz Land's website from its current server and transfer it to a secure server.[15]

Moreover, Aboitiz Land stated that it will conduct vulnerability assessments of its website and will implement Information Security Management System (ISMS) governance structure to strengthen its information security measure.[16]

Aboitiz Land also stated that it has not notified the affected data subjects and sought the guidance of the Commission to determine the need to notify the affected data subjects.[17]

On 19 October 2020, the CID issued an Order requiring Aboitiz Land to submit a Full Report pursuant to Section 17, Rule V of NPC

---

[11] Breach Notification dated 09 May 2018 of Aboitiz Land, Inc., at p. 3.
[12] *Id.*
[13] *Id.,* at p. 8.
[14] *Id.*
[15] Breach Notification dated 09 May 2018 of Aboitiz Land, Inc., at p. 8.
[16] *Id.,* at p. 9.
[17] *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

Circular No. 16-03, detailing the incident containing the information provided therein.[18]

On 19 October 2022, the CID issued an Order requiring Aboitiz Land to submit a Post-Breach Report containing proper documentation of the security measures it implemented, proof of communication and notification to the data subjects, the outcome of the routine security assessments it has undertaken, and other proof of compliance with the Data Privacy Act of 2012 (DPA).[19]

Accordingly, Aboitiz Land submitted its Post-Breach Report dated 03 November 2022 containing therein statements regarding the security measures it has taken to address the breach.[20] Aboitiz Land stated that it had internal meetings with the departments concerned to conduct further investigations.[21] Aboitiz Land emphasized that-

> …[R]edirecting the domain and changing the password of the admin account made it impossible for any unauthorized user to log into the Website, thereby rendering the leaked hash values useless.[22]

Further, Aboitiz Land averred that according to LNS report, "there was no attack on the content management system (CMS) website as the logs showed direct access by inputting the username and password."[23] In conclusion, LNS stated that there was no data breach considering that:

> 1. There was no illegal IP Addresses identified during the audit;
> 2. The backup file, which was created in connection with website enhancements and code updates, could not be downloaded due to "multiple security measures done using .htaccess";
> 3. No forced login, brute force or injection seen in the logs; and

[18] *In re: Aboitiz Land, Inc.,* NPC BN 18-071, Order dated 19 October 2020.
[19] *In re: Aboitiz Land, Inc.,* NPC BN 18-071, Order dated 19 October 2022.
[20] Post-Breach Report dated 03 November 2022 of Aboitiz Land, Inc., at p. 2.
[21] *Id.*
[22] *Id.*
[23] *Id.,* at p. 3.

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

4. The hash values could not be decrypted as LNS used "a combined SHA-2+MD5 encryption which is impossible to be decrypted and almost impossible to even brute especially if we change password [*sic*] every 6 months or 1 year as a policy."[24]

Lastly, Aboitiz Land verified that the IP address came from an authorized user which is the Loop Digital Marketing, the contractor engaged by Aboitiz Land to update the website.[25]

Furthermore, Aboitiz Land reported on the security measures it implemented for the new website server hosting such as vulnerability assessment, use of Sucuri as web application firewall, Secure Sockets Layer (SSL) encryption,[26] and storage encryption,[27] with corresponding screenshots of the storage configuration.[28]

Moreover, Aboitiz Land submitted that there was no need to notify the affected data subjects since no data breach has resulted from the incident.[29] In relying with the LNS' findings, Aboitiz Land stated that with the redirection of its Website's domain and the change in the password of the administration account, the leaked hash values could not be decrypted, thus, no unauthorized person has accessed to the website.[30]

Finally, Aboitiz Land included in its post-breach report a summary of the outcome of the Routine Security Assessments, and other proof of security measures it has implemented for the protection of personal data.[31]

The Commission resolves that this case falls under the mandatory breach notification requirement, hence, notification of the affected data subjects should be made.

---

[24] Post-Breach Report dated 03 November 2022 of Aboitiz Land, Inc., at p. 3.
[25] *Id.*
[26] *Id.*
[27] *Id.,* at p. 6.
[28] Post-Breach Report dated 03 November 2022 of Aboitiz Land, Inc., at pp. 4-7.
[29] *Id.,* at p. 8.
[30] *Id.,* at pp. 8-10.
[31] *Id.,* at p. 10

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

Section 11 of NPC Circular No. 16-03 provides that the personal information controller (PIC) or personal information processor (PIP) is required to notify the data subjects upon knowledge of or when there is reasonable belief that a personal data breach has occurred, when the following requisites are present:

> 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.[32]

Applying the foregoing, Aboitiz Land admitted in its Breach Notification that the incident involved sensitive personal information contained in less than twenty (20) records, such as age, educational background, and government-issued IDs.[33] Aboitiz Land also stated that the database derived from its website contained less than three hundred (300) records of names and contact details of individuals[34] which can be considered as 'other information that may be used to enable identity fraud.'[35] Thus, the first requisite is present in this case.

For the second requisite, Aboitiz Land stated that "the available evidence supports the conclusion that an unauthorized person was able to enter and access the system."[36] Aboitiz Land also acknowledged the possibility that the records were acquired by

---

[32] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 11 (15 December 2016) (NPC Circular 16-03).
[33] Breach Notification dated 09 May 2018 of Aboitiz Land, Inc., at p. 2.
[34] *Id.*, at p. 1.
[35] *Id.*, at p. 2.
[36] *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

unauthorized persons.[37] Such statements made by Aboitiz Land are admissions that there is indeed a reason to believe that the personal data may have been acquired by an unauthorized person. Thus, the second requisite is also present in this case. Other than these statements, Aboitiz Land failed to show proof of security measures that would prevent the personal data from being acquired by any unauthorized person.

Lastly, there was no evidence showing that "there is a minimal risk of serious harm to all data subjects," especially when the personal data involved may be compromised as to enable identity fraud.[38] A minimal risk, as claimed by Aboitiz Land, is not sufficient to prove that no serious harm affects the data subjects. As mentioned by Aboitiz Land, the records acquired by an unauthorized person may pose a real risk of serious harm to the affected data subjects whose sensitive personal information such as age, educational background, and government-issued IDs are involved. Aboitiz Land should show proof that the incident would not seriously harm the affected data subjects, which, however, it failed to provide to the Commission.

Given the foregoing circumstances, Aboitiz Land, as PIC, should be required to notify all the data subjects affected by the breach under Section 11 of NPC Circular 16-03.

Thus, Section 18(A) of the Circular provides:

> 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:
>
> 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.
>
> 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

[37] Breach Notification dated 09 May 2018 of Aboitiz Land, Inc., at p. 2.
[38] *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

> 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.[39] (Emphasis supplied)

It is the obligation of Aboitiz Land as PIC to notify the affected data subjects when their personal data have been compromised by a breach. This is especially when the incident falls under the mandatory breach notification requirement provided in Section 11 of NPC Circular No. 16-03. By doing so, they can be able to take necessary precautions or other measures to protect themselves against the negative consequences of the breach.[40] Thus, the Commission deems it unmeritorious for Aboitiz Land to conclude that notification is no longer necessary since no breach has resulted from the incident[41] without sufficiently showing it by substantial evidence.

Moreover, Aboitiz Land has not sufficiently complied with the Order of CID dated 19 October 2022 requiring it to submit a proper documentation of the security measures it implemented.[42] Aboitiz Land merely submitted a statement and proof of security measures it implemented "for the New Website Server Hosting."[43] However, Aboitiz Land has not submitted any proof of security measures it implemented to address the incident.

Rule V, Section 17(D) of NPC Circular 16-03 provides that the PIC shall notify the Commission of a personal data breach including the enumerated contents of the notification which are, but not limited to:

> D. *Content of Notification*. The notification shall include, but not be limited to:
>
> 1. Nature of the Breach

---

[39] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(A) (15 December 2016) (NPC Circular 16-03).
[40] *Id.*
[41] Post-Breach Report dated 03 November 2022 of Aboitiz Land, Inc., at p. 8.
[42] *In re: Aboitiz Land, Inc.*, NPC BN 18-071, Order dated 19 October 2022.
[43] Post-Breach Report dated 03 November 2022 of Aboitiz Land, Inc., at p. 3.

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

a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
b. a chronology of the events leading up to the loss of control over the personal data;
c. approximate number of data subjects or records involved;
d. description or nature of the personal data breach;
e. description of the likely consequences of the personal data breach; and
f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved
   a. description of sensitive personal information involved; and
   b. description of other information involved that may be used to enable identity fraud.
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. (Emphasis supplied)

The Commission reserves the right to require additional information, if necessary.[44]

In relation thereof, Rule IV, Section 9 of the same Circular also states that all actions taken by a PIC or PIP shall be properly documented which 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;

[44] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 17 (D) (15 December 2016) (NPC Circular 16-03).

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. Outcome of the breach management, and difficulties encountered; and
D. Compliance with notification requirements and assistance provided to affected data subjects.[45]

Aboitiz Land merely documented the actions it undertook for its New Website Server Hosting, but not the security measures it implemented during the occurrence of the incident or within the reasonable period after the incident has occurred. Moreover, Aboitiz Land included in its Post-Breach Report a statement regarding the vulnerability assessment it made but Aboitiz Land failed to support this by substantial evidence.[46]

As PIC, Aboitiz Land is duty bound to show the Commission proofs that it undertook remedial actions in order to mitigate the breach and that it notified the affected data subjects about the incident.

Hence, the Commission deems it necessary to require Aboitiz Land to notify the affected data subjects and to submit proof of security measures it implemented to address the breach.

WHEREFORE, premises considered, the Commission **NOTES** the Compliance submitted by Aboitiz Land, Inc. (Aboitiz Land) with the Order of the Complaints and Investigation Division (CID) dated 19 October 2022.

Moreover, Aboitiz Land is hereby **ORDERED** to comply with the following **within fifteen (15) days** from the receipt of this Order:

1) **NOTIFY** affected data subjects and submit proof of such notification to the Compliance and Monitoring Division (CMD); and

2) **SUBMIT** proof of security measures implemented to address the breach to the CMD.

---

[45] *Id.*, rule IV, § 9.
[46] Post-Breach Report dated 03 November 2022 of Aboitiz Land, Inc., at p. 4.

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

The Commission also **DIRECTS** the CMD to evaluate and monitor the completeness of Aboitiz Land's data breach notification and assess its breach management pursuant to NPC Circular 16-03.

SO ORDERED.

City of Pasay, Philippines.
04 July 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

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

Copy furnished:

IS
Data Protection Officer
Aboitiz Land, Inc.

COMPLIANCE AND MONITORING 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

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