Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: E-SCIENCE CORPORATION **NPC BN 20-124**

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

RESOLUTION

AGUIRRE, D.P.C.:

For the Commission's resolution is the Request for Exemption to Notify the Data Subjects from E-Science Corporation ("E-Science") dated 28 August 2020 involving a data breach incident affecting approximately four thousand (4,000) test records of data subjects.[1]

The Facts

On 6 August 2020, this Commission issued a Resolution[2] with the following disposition, *to wit*:

> **WHEREFORE,** premises considered, E-Science Corporation is **ORDERED** to **1) SUBMIT** with dispatch a Full Report of the Personal Data Breach as required under Section 17(C) of NPC Circular No. 16-03; and **2) SHOW CAUSE** in writing why it should not be liable for failure to submit a Full Report within the required period and be subject to contempt proceedings, as permitted by law, before the appropriate court, and such other actions as may be available to the Commission.
>
> Furthermore, the Commission **GRANTS** the request for Postponement of Notification to Data Subjects of E-Science Corporation and directs them to submit proof of compliance thereof within fifteen (15) days from submission of their Full Breach Report. Pending their verification of the full list of affected data subjects, E-Science Corporation is enjoined to use alternative means of notification under Section 18(d) of NPC Circular No. 16- 03.

However, instead of submitting a proof of compliance on the required Notification to Data Subjects, E-Science submitted a Request for Exemption to Notify the Data Subjects.[3] Citing Section 11 of NPC Circular 16-03, it contended that after full investigation, it has confirmed that the incident was only limited to names, e-mail

---

[1] Exemption Request to Notify the Data Subjects for NPC BN 20-124 submitted by E-Science Corporation dated 18 August 2020.
[2] Resolution dated 6 August 2020, *In re: E-Science Corporation*, NPC BN 20-124.
[3] *Supra* note 1.

addresses and testing logs. It claimed that no sensitive, personal or biometric data were involved. It also found that there was no PIN, password, birthday, account number, telephone number, or any data involved that could put the individual at risk.[4]

E-Science also stated that it has undertaken subsequent measures to ensure that the risk of harm or negative consequence to the data subjects will not materialize.[5]

Discussion

This Commission denies E-Science's Request for Exemption to Notify the Data Subjects.

Section 11 of NPC Circular 16-03 provides that:

> 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 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**.[6]

In its Request for Exemption to Notify the Data Subjects,[7] E-Science has stated that after its full investigation, it has confirmed that only names, e-mail addresses and testing logs were involved in the subject breach incident.

---

[4] *Ibid.*
[5] *Ibid.*
[6] Emphasis supplied.
[7] *Supra* note 1.

This Commission takes this opportunity to stress that information that may be used to enable identity fraud under Section 11 (A) is not limited to the categories of information listed therein, such as 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.

Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of *"Phishing"* attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.[8]

Republic Act No. 10175, otherwise known as the *Cybercrime Prevention Act* of 2012, provides that computer-related identity theft is a cybercrime offense. Section 4(b)(3) thereof states that:

> **Computer-related Identity Theft. – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right**: Provided, That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.[9]

In the case of *Disini, et al. v. Secretary of Justice, et. al.,*[10] the Supreme Court recognized that the use of identifying information regarding a person could perpetrate the commission of identity theft. The Court had this to say on the crime of Identity Theft:

> The usual identifying information regarding a person includes his name, his citizenship, his residence address, his contact number, his place and date of birth, the name of his spouse if any, his occupation, and similar data. **The law punishes those who acquire or use such identifying information without right, implicitly to cause damage.**

[8] *What is Phishing?* Accessed from https://www.phishing.org/what-is-phishing, last September 11, 2020.
[9] Emphasis supplied.
[10] GR No. 203335, February 11, 2014.

Theft of identity information must be intended for an illegitimate purpose.[11]

In this case, since names, e-mail addresses and testing logs were confirmed to be involved, identity theft could therefore be committed using those information.

Aside from this, determining whether the compromised information may enable identity fraud requires a consideration of circumstances other than the nature of the personal information, such as the manner of disclosure and to whom the information was disclosed. In this case, the names and email addresses of its data subjects were not just disclosed accidentally but taken intentionally. In both its Initial Report[12] and Full-Breach Report,[13] E-Science reported that a hacker was able to access one of its online databases and a ransomware was implanted therein. It recognized that one of the likely consequences of the incident is that the hacker may contact the data subjects directly and send them malicious e-mails. Such reported circumstances surrounding the security incident gives rise to a real risk of serious harm to any affected data subject, such as the commission of identity theft through *Phishing* activities.[14]

Another justification relied upon by E-Science in its Request for Exemption to Notify the Data Subjects is that it has undertaken subsequent measures to ensure that the risk of harm or negative consequence to the data subjects will not materialize. The Commission notes, however, that the measures it has undertaken[15] do not address the abovementioned risks that *Phishing* activities may pose to its data subjects. Such risks may only be addressed through the prompt notification of the affected data subjects regarding the circumstances of the breach so that they can take the necessary precautions.

In view of the foregoing and having met all the conditions for mandatory breach notification under Section 11 of NPC Circular 16-03, E-Science should have promptly notified the affected data subjects the moment it has confirmed that the names, e-mail addresses and testing logs of the affected data subjects were indeed

[11] Emphasis supplied.
[12] Initial Breach Report dated 2 July 2020.
[13] Full Breach Report dated 18 August 2020.
[14] *Ibid*.
[15] See, Initial Breach Report dated 2 July 2020 and Full Breach Report dated 18 August 2020.

involved in the subject breach incident. Its contention that no sensitive, personal or biometric data were involved, or its finding that there was no PIN, password, birthday, account number, telephone number, or any data involved which could put the individual at risk, is of no merit. Its mere confirmation that names, e-mail addresses and testing logs of the data subjects were involved in the breach incident, and the fact that the same was caused by a hacker, are sufficient to require E-Science to notify the affected data subjects. Further, E-Science cannot renege on its obligation to notify the data subjects by simply stating that no sensitive personal information was involved in the data breach incident when it has, at the onset, recognized that there was a need for such notification when it reported the likelihood that the hacker may directly contact and provide malicious e-mails to the affected data subjects. This recognition of the risks posed to its data subjects should have already been enough to move E-Science to immediately notify its data subjects.

Lastly, this Commission granted the Request for Postponement of E-Science on the premise that it will have to conduct further investigation in order to prevent sending the notification to unaffected data subjects. Thus, considering that it has already completed its full investigation on the incident, E-Science should now be prepared to proceed with the required notification of the data subjects without further delay.

WHEREFORE, premises considered, the Request for Exemption to Notify the Data Subjects of E-Science Corporation is hereby **DENIED**. E-Science Corporation is **ORDERED** to submit proof of compliance on the Notification of the Data Subjects within five (5) days from receipt of this Resolution

SO ORDERED.

Pasay City, Philippines
10 September 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JYP
Data Protection Officer
E-Science Corporation

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission