Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: E-SCIENCE CORPORATION **NPC BN No. 20-124**

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

RESOLUTION

***AGUIRRE*, D.P.C.:**

This Resolution refers to the request for Postponement of Notification to affected data subjects of E-Science Corporation ("E-Science") dated 3 July 2020, involving a data breach incident affecting approximately four thousand (4,000) test records of data subjects, for it is still investigating the matter internally.[1]

The Facts

On 26 June 2020, one of E-Science's databases was accessed by a hacker and a schema was created containing a message asking for a ransom. The hacker further stated that E-Science's databases were already downloaded and backed up in their servers. They also warned E-Science that if they do not receive the payment in the next nine (9) days, they will *"sell the database to the highest bidder or use them otherwise."*[2] The sensitive personal information affected were approximately four thousand (4,000) test records of data subjects from eight (8) different organizations including names, e-mail addresses, and work addresses. They claim that no other personal information, passwords, financial data, and real-time data were accessed.[3]

After the said attack was identified, E-Science has conducted the following safeguards that would minimize harm and mitigate the impact of the personal data breach:

---

[1] E-mail dated 3 July 2020 submitted by the Data Protection Officer of E-Science.
[2] Data Breach Report dated 2 July 2020, at p. 2.
[3] *Ibid*, at pp. 2-3.

(1) June 30: An investigation was started by the Network and Systems Team;
(2) July 1: A meeting between the management and the people involved agreed on a set of preventive measures;
(3) July 2: An initial notification was sent to the National Privacy Commission; and
(4) Other internal security action items have been laid out.[4]

Furthermore, E-Science has described in full the measures taken or proposed to be taken to address the said breach, *to wit:*

(1) Set-up a system where there is a centralized accessibility monitoring of E-Science IP addresses;
(2) Reset all VPN credentials;
(3) Make sure code repository and databases are accessible via VPN or from network in the office only;
(4) No sensitive information is used for test data in Dev/QA instances, and review in UAT instances;
(5) Make sure no sensitive data like password is saved in source code, which then goes to the code repository;
(6) Comply to Web and Device Security Test before releasing a product;
(7) Implement database credentials rotation;
(8) Review project accesses of AWS accounts;
(9) Set multifactor authentication in AWS accounts to on;
(10) Set a standard on naming database schema;
(11) Create and use unique database credentials, instead of current practice of using shared accounts; and
(12) Review the accounts registered to databases and code repository. Also, monitor internal user access.[5]

E-Science has also reported that it was able to restore the test data from back up and that security measures are implemented and monitored regularly. However, it has not yet sent notifications to the affected data subjects because it is still currently doing further investigations so that it can prevent sending the same to unaffected individuals.[6]

[4] *Ibid.*, at p. 2.
[5] *Ibid.*, at p. 3.
[6] *Ibid.*, at p. 3.

Hence, on 3 July 2020, E-Science sent an e-mail to the Commission requesting for notification extension to the affected data subjects since it is still investigating the matter internally.[7]

Discussion

This Commission grants the herein request for notification extension or postponement of notification to data subjects of E-Science in accordance with NPC Circular No. 16-03 (Personal Data Breach Management).

Under Section 18(A) of NPC Circular No. 16-03, the personal information controller ("PIC") shall notify the data subjects affected by a personal data breach 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 seventy-two (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.

However, the PIC may request for postponement of the notification when it is not reasonably possible to notify the data subjects within the prescribed period. **Section 18(B) of NPC Circular No. 16-03** provides that:

> **If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for** an exemption from the notification requirement, or **the postponement of the notification.** A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects. The Commission may authorize the

[7] E-mail dated 3 July 2020 submitted by the Data Protection Officer of E-Science.

> postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.[8]

In this case, the hacked data include four thousand 4,000 test records of data subjects from eight (8) different organizations that contain names, e-mail addresses, and work addresses. Moreover, E-Science opted not to send notifications yet in order to prevent sending the same to unaffected individuals.

Considering the large number of test records involved in this data breach incident that not only reach hundreds but thousands, the Commission acknowledges that it may not be reasonably possible for E-Science to notify the affected data subjects within the prescribed period of seventy-two (72) hours upon its knowledge of the said data breach incident. Moreover, E-Science's reasoning that it did not send notifications to prevent sending the same to unaffected individuals is also plausible. To do otherwise may just result to further data breach incidents particularly if it would send notifications without appropriate, accurate, and sufficient safeguards in place in view of the thousands of records involved or affected. Therefore, granting the request for postponement to notify data subjects is proper.

Meanwhile, while E-Science has submitted an Initial Report to notify the Commission of the data breach incident and has acted upon the matter on the notification to data subjects with the request for postponement thereof, it has not however submitted a Full Breach Report as required by NPC Circular No. 16-03.

Under Section 17(C) of NPC Circular No. 16-03, it provides that:

> [T]he Commission shall be notified within the 72-hour period based on available information**. The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.[9]

[8] Emphasis supplied.
[9] Emphasis supplied.

The Commission has received on 2 July 2020 an Initial Report on the said data breach incident of E-Science. However, no Full Breach Report has been submitted until now. Further, E-Science did not request for and no additional time was granted by this Commission for the submission of the such report. It should be noted that Notification of the Commission and Notification of Data Subjects are two (2) different and separate requirements under Sections 17(C) and 18(A) of NPC Circular No. 16-03, respectively. Thus, the PIC should promptly comply with both sections accordingly.

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.

SO ORDERED.

Pasay City, Philippines
6 August 2020.

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:

JYP
Data Protection Officer
E-Science Corporation

COMPLIANCE AND MONITORING DIVISION
GENERAL RECORDS UNIT
National Privacy Commission