Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: SUN LIFE OF CANADA (PHILIPPINES) INC. **CID BN 17-039**

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

RESOLUTION

NAGA, D.P.C.:

Before this Commission is a request made by Sun Life of Canada Philippines Inc. (Sun Life) to be exempted from notifying affected data subjects from a data breach incident that occurred last 29 November 2017.

The Facts

On 01 September 2017, Sun Life's Unit Manager (UM) was transferred from Eucalyptus New Business Office (NBO) to Empress NBO. By reason of such transfer, the Licensing Department updated her Agent Information System (AIS). On 26 November 2017, the UM reported to their Helpdesk that she was able to generate the production report that belongs to her Branch Manager (BM) and her direct advisors when she used her personal laptop via Google Chrome browser.

On 27 November 2017, the incident was escalated to the Advisor Technology Support (ATS) and Compliance. It was identified that because of the update, the code of her new BM was saved as the UM's Team Lead Code which allowed her to generate the production report.

Sun Life reported that one hundred one (101) accounts with one hundred (100) policy owners were affected by the breach. The personal data involved are as follows: Due Date; Policy Number; Insured Name; Submitted Applications; Settled Applications; Net Sales Credit; First Year Premium; and Renewal Premium Income.

In response, Sun Life mentioned that they have taken the following measures to address the breach:

a. On 27 November 2017, the UM was requested to delete the production report that she has downloaded from the agent's portal and send confirmation that the same was deleted;
b. The UM code was updated to her own team code in the Agent's Information System;
c. The Licensing Department will file a maintenance request to update the AIS. The Team code field will not accept the code if it does not belong the advisor/ UM whose account is being updated; and
d. IT will be requested to sweep or check the system for another similar occurrence.

On 29 November 2017, Sun Life submitted the breach notification report before the Commission with a request to be exempted from notifying its clients and advisors that were affected by the breach, on the ground that the breach will not cause real risk of serious harm to the rights and freedoms of the policy holders considering that it was the UM herself who reported the said breach.

Discussion

As provided by Section 11 of the NPC Circular 16-03, notification to the affected data subjects shall be required upon knowledge of or when there is reasonable belief by the Personal Information Controller (PIC) or Personal Information Processor (PIP) 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.

The Commission recognizes that Sun Life has premised its request for exemption on the ground that the incident does not meet the third condition laid down by the abovementioned provision as the personal data were disclosed only to the UM.

However, Sun Life failed to take into account that the number of affected data subjects is more than one hundred (100) individuals which falls under the mandatory breach notification as provided by Section 13 (B) of NPC Circular 16-03.

According to Section 38 of the Data Privacy Act of 2012 (DPA), "Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed." Thus, the DPA and the rules and regulations in relation to data privacy should be interpreted in a manner that will uphold the data privacy rights of the individual. Hence, the Commission does not see any reason to disturb the general rule for the PIC to notify the data subjects affected by a personal data breach[1].

The Commission then deems it wise to order Sun Life to notify the affected data subjects to provide them the reasonable opportunity to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.

On another matter, the Commission notes that as of the date of the promulgation of this Resolution, it has yet to receive its full breach report as required under NPC Circular 16-03. The Commission reminds Sun Life that the DPA requires two (2) different reports in case of a data breach.

As held by the Commission in the case of *In re: SLGF (NPC BN 19-115):*

> Section 17 of the NPC Circular 16-03 speaks of two notification requirements to be submitted to the Commission in case a data breach cases. First is the initial notification[2] that

[1] Section 18 of the NPC Circular 16-03
[2] Section 17 (A) of the NPC Circular 16-03

informs to the Commission that a personal data breach has occurred. This has no particular form or content as it merely requires that the Commission to be notified within seventy-two (72) hours. The second notification[3] is the Full Breach Report which contains a more specific and concrete narration of facts surrounding the incident, the effect of such incident and the remedial actions taken by the PIC. The full breach report that the Commission requires must include, but not be limited to:

1. Nature of the Breach
    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.[4]

The foregoing content and information is needed by the Commission in order to determine if the PIC has acted adequately in order to protect the rights of the affected data subject and to see if the PIC has undertaken measures to avoid further damage. These two documents are very much different from one another not only as to its form and content but also as to its purpose.

[3] Section 17 (D) of the NPC Circular 16-03
[4] Section 17 (A) of NPC Circular 16-03

Sun Life submitted before the Commission a breach notification dated 29 November 2017. The breach notification submitted can only be considered as a notification as prescribed under Section 17 (A) of NPC Circular 16-03 as it lacks the necessary content and information required in a full breach report. Therefore, Sun Life is not yet compliant in terms of the submission of the required full breach report.

WHEREFORE, premises considered, this Commission **DENIES** the request of Sun Life to be exempted from notifying data subjects affected by the breach.

Sun Life is hereby **ORDERED** to comply within ten (10) days from receipt of this Resolution with the following:

(1) **NOTIFY** with dispatch the affected data subjects, including proof of compliance consistent with NPC Circular 16-03; and

(2) **SUBMIT** a full breach report detailing the measures it has since undertaken to prevent, avoid or reduce the recurrence of a similar personal data breach.

SO ORDERED.

Pasay City, Philippines;
15 October 2020.

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

(On Official Business)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

(Sgd.)
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JSC
Data Privacy Officer

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