***IN RE: SUN LIFE OF CANADA (PHILIPPINES), INC.*** **CID BN 18-183**

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

# RESOLUTION

***LIBORO, P.C.:***

This Resolution refers to the Breach Incident Report (Report) dated 24 September 2017 submitted by Sun Life of Canada (Philippines), Inc. ("Sun Life"). The Report includes a narration of a breach incident that Sun Life discovered on 21 September 2018. It involves the disclosure of information of around nine thousand seven hundred eighteen (9,718) clients that were not necessary for the third-party vendor to process.

## Facts

In May 2016, Sun Life engaged the services of an external vendor for the development of its wellness website, SUN Fit and Well. The vendor was engaged in the end-to-end membership management of SUN Fit and Well clients.

In October 2016, the wellness website was launched. From this period until 21 September 2018, the marketing staff of Sun Life has been sending the personal information of the new SUN Fit and Well clients to the vendor. The required information for this endeavor includes the client's Owner name, Insured name, Owner email address, Insured email address, and Insured Age. However, the assigned staff also sent the extract (in Excel form) from Sun Life's information and management system without filtering the information. Consequently, the Excel file transmitted contained information of clients that were not necessary for the vendor to process, such as policy number, policy issue date, servicing agent name, servicing branch date, settlement date, old/new client indicator, and old/new policy indicator. The Excel files were sent weekly, which were not encrypted, nor password protected.

On 21 September 2018, Sun Life's Marketing Department requested its Compliance Team to review the processes and procedures that were done from the year 2016. From the review process, Sun Life was able to determine the practice of sending various Excel files containing the information of clients that came from Sun Life's information and management system.

In response to this discovery, Sun Life sent a data breach incident report on 24 September 2018. In the report, Sun Life outlined the measures it took to address the breach such as requesting the vendor to immediately purge all the data, to submit a certificate to confirm destruction, and to certify that these have not been shared, disclosed, or further processed.

Sun Life also requested for an exemption from notification of the affected data subjects on the ground that it is unlikely that the third-party vendor will use the policy information for unauthorized purposes, or that the disclosure will give rise to a real risk of serious harm to any affected data subject.

In its Resolution dated 21 May 2020, the Commission found that Sun Life's remedial measures were sufficient to handle the incident and granted its request for exemption from notification of the affected data subjects.

The Commission held that the unauthorized disclosure of the additional information was made to Sun Life's personal information processor, whose services are governed by contract which includes a confidentiality clause. The unauthorized acquisition is not likely to give rise to a real risk of serious harm to any affected data subject. Other than these, the excessive information that was shared were not personal information: policy number, policy issue date, servicing agent name, servicing branch name, settlement date, old/new client indicator and old/new policy indicator. Thus, notification would not be in the interest of the data subjects.

Nevertheless, it is required for Sun Life to submit a post-breach report to monitor the results of the measures it adopted to address the breach and to ensure that no further similar incident occurred.

In the said Resolution, the Commission ordered Sun Life to submit the following: (1) post-breach report containing the results of each of the measures it adopted to address the breach; (2) copy of the certificate from the vendor confirming the purge and destruction of all personal data not needed to perform its obligations under the contract; and (3) copy of the certification from the vendor stating that it has not shared, disclosed, or otherwise processed information outside the scope of their contract.

After its receipt of the Resolution on 18 January 2021, Sun Life submitted its Compliance Letter on 28 January 2021. In its letter, Sun Life enumerated the steps it had undertaken, as mentioned in its post-breach report.

## Discussion

Upon reviewing of the Compliance Letter submitted by Sun Life, this Commission finds that Sun Life has fully complied with the order of the Commission in its Resolution dated 21 May 2020.

As provided in Section 9 of the NPC Circular No. 16-03 (Personal Data Breach Management), all actions that are implemented by a Personal Information Controller (PIC) shall be properly documented, which shall include the following:

> A. Description of the personal data breach, its root cause and circumstances regarding its discovery;
> B. Actions and decisions of the incident response team;
> C. Outcome of the breach management, and difficulties encountered; and
> D. Compliance with notification requirements and assistance provided to affected data subjects.
>
> A procedure for post-breach review must be established for the purpose of improving the personal data breach management policies and procedures of the personal information controller or personal information processor.[1]

[1] Section 9 of NPC Circular 16-03

Sun Life has reported in detail all the measures it undertook and provided copies of certification from the vendor, as instructed by the Commission.

According to the post-breach report, Sun Life has undertaken the following remedial measures to prevent similar events from happening in the future:

(1) Immediate cessation of transfer of data to the vendor effective 21 September 2018. Hence, the website management is now directly governed by Sunlife's marketing staff;
(2) Immediate request for the vendor to purge all data and to submit a certificate to confirm destruction;
(3) Revision of process flow for the wellness website member management so that it will only be done internally;
(4) Launching of new enhanced website in November 2018 automating the upgrade of members to "Gold," from the previous manual upgrading of member status;
(5) Requested the vendor to certify that it has not shared, disclosed or otherwise processed information other than upon instruction of Sunlife;
(6) Upon assessment of the earlier conducted Privacy Impact Assessment (PIA), Sunlife found that the PIA conducted was sufficient.
(7) Review or revise processes to ensure that only personal data needed for services to be performed are shared with Sunlife's service providers;
(8) Sweep all arrangements where personal data are shared to ensure that required documents are executed and assessments have been made.

In its Compliance Letter, Sun Life also attached a copy of the certificate from the vendor (1) confirming the purge and destruction of all personal data not needed to perform its obligations under their contract; and (2) stating that it has not shared, disclosed or otherwise processed the personal data and that the same was used solely for the purpose required by Sun Life.

Through careful review and evaluation of the submitted report, this Commission finds that the abovementioned submissions and actions implemented by Sun Life are adequate, sufficient, and compliant to its order indicated in the Resolution dated 21 May 2020 issued by this Commission.

**WHEREFORE,** premises considered, this Commission resolves that the matter of CID 18-183 "In re: Sun life of Canada (Philippines), Inc." is hereby considered **CLOSED**.

**SO ORDERED.**

Pasay City, Philippines;
25 March 2021.

**(Sgd.)**
**RAYMUND ENRIQUEZ LIBORO**
Privacy Commissioner

WE CONCUR:

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

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

Copy furnished:

**ATTY. MJM**
*Data Protection Officer*
Sun Life of Canada (Philippines), Inc.

**COMPLIANCE AND INVESTIGATION DIVISION**
**ENFORCEMENT DIVISION**
**GENERAL RECORDS UNIT**
National Privacy Commission