Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: BREACH NOTIFICATION REPORT OF SUNLIFE OF CANADA

CID BN 17-021

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

ORDER

In a Resolution dated 29 July 2019, the Commission required Sun Life of Canada (Philippines), Inc. ("Sun Life") to comply with the notification of data subjects, stating:

> In this case, despite the measures implemented by Sun Life, it cannot be said that there is no real risk of serious harm to the affected data subjects. Circular No. 16-03 requires, as a general rule, that the affected data subjects be notified. It is only in cases "where the Commission determines that such notification would not be in the public interest or in the interest of affected data subjects" may exemption be allowed. No evidence has been submitted to negate the possibility that other persons may have taken advantage of the same vulnerability to access the data.

On 9 September 2019, the Commission received a letter from Sun Life in response to the Resolution, requesting for reconsideration thereof, stating, among others:

> It is respectfully submitted that there is no vulnerability pertaining to access in this case that may be exploited by others. The inadvertent disclosure resulted from an advisor's erroneous inputting of an email list…While it is granted that such data may be (sic) render the data subject's insurance accounts vulnerable, we respectfully submit that it is not likely that the incident will give rise to real risk of serious harm to the rights of the data subject xxx
>
> xxx
>
> In the event that the Honorable Commission decides to deny our request, we likewise respectfully seek an extension of time of 30 days from receipt of the decision to notify the affected data subjects.
>
> xxx

On 23 September 2019, the Enforcement Division issued its findings regarding the Request for Reconsideration:

> Moreover, Sun Life has not provided any update or information as to the accomplishment of the measures it has previously enumerated to undertake to address the breach. In particular, Sun Life has not provided any update as to the pending confirmation of email deletion from clients who inadvertently received the email; results of the sweep of all group email addresses in Office 365; and information as to its checking with Microsoft for the possible removal of the type ahead feature of Office 365.
>
> xxx
>
> The Commission has found that "despite the measures implemented by Sun Life, it cannot be said that there is no real risk of serious harm to the affected data subjects." It has also been determined that "no evidence has been submitted to negate the possibility that other persons may have taken advantage of the same vulnerability to access the data." Sun Life's only response to this lack of evidence is its own conclusion that there is "no vulnerability pertaining to access in this case that may be exploited by others."

In a Resolution dated 28 October 2019, the Commission denied the Request for Reconsideration by Sun Life, stating thus:

> As assessed by the Enforcement Division, notification of the affected data subjects allows them to take the necessary precautions and to avail themselves of measures that would protect them against possible effects of the breach, including their own monitoring for irregular activities that may arise from compromised data.
>
> As to the claim of Sun Life that there is "no vulnerability pertaining to access in this case that may be exploited by others", it must be noted that the Commission's issuances define "vulnerability" as a "weakness of a data processing system that makes it susceptible to threats and other attacks." It is not confined to technical measures nor does it exclude organizational or physical gaps such as employee error in this case.

On 23 December 2019, Sun Life sent a letter to the National Privacy Commission (NPC) requesting to meet with the Enforcement Division to clarify the requirements of the Resolutions issued, stating thus:

> In that meeting, we intend to clarify the requirements in the July Resolution and to substantiate the grounds stated in our Request for Reconsideration dated 9 September 2019. Considering the foregoing, we respectfully seek the Honorable Commission's kind understanding and indulgence and request for the deferment of the running of the period within which to comply with the requirements of the July Resolution until we have met with the Enforcement Division.

On 29 January 2020, the Enforcement Division met with Sun Life's team including its data protection officer and consumer welfare head. During the said meeting, Sun Life's representatives provided additional proof for their position that there is minimal risk of serious harm to the affected data subjects despite the Commission's Resolution already denying its Request for Reconsideration.

On 3 February 2020, Sun Life sent an email to the Enforcement Division outlining its submissions. In the submitted outline, Sun Life states the following as the main points for its "Grounds for Reconsideration":

1) Timeliness of notifying the data subjects;
2) There is no risk of serious harm to the affected data subjects because of the following:
   a. There is minimal probability of fraud and account takeover due to controls in place of Sun Life;
   b. The nature of data exposed are low risk and are not used in the client validation process across all channels of Sun Life;[1] and
   c. The nature of data exposed is not sufficient to perpetuate fraud.
3) Sun Life continuously educates employees and advisors on Data Privacy through face-to-face trainings, e-learning courses and the annual Data Defender's campaign.

On 07 July 2020, Sun Life, through its Data Protection Officer, filed a letter with the Commission stating thus:

> While waiting for the final decision on Sun Life's request filed on 23 December 2019, Sun Life nonetheless notified all the affected data subjects. Below is the status of compliance with the Resolution:

[1] Policy number, issue date, owner name, insured name, basic plan, face amount, mode of payment and premium amount.

Data subjects notified via email or ordinary mail	175
Clients yet to be notified via ordinary mail	108
Will no longer be notified (deceased)	5

> We will file an updated report once all data subjects have been successfully notified. Attached herewith as Annex "A" is a sample of the notification letter. xxx

On 28 July 2020, Sun Life sent another letter containing an update on the notification status as of 28 July 2020, thus:

Data subjects successfully notified via email or ordinary mail	237	82%
Data subjects who will no longer be notified (deceased)	5	2%
Data subjects who were not successfully notified	46	16%

> In relation to Section 18 of NPC's Circular 16-03 on Personal Data Breach Management, Sun Life established "*all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach.*" Unfortunately, despite several delivery attempts and service calls, a total of 46 data subjects cannot be located. Some are no longer in their registered address, while others cannot be contacted. A few cannot be reached because of closed work/business/residential property due to the quarantine. xxx

At the outset, the Commission notes that the recourse taken by Sun Life is not recognized under the NPC Circular on Personal Data Breach Management.[2]

By meeting with the Enforcement Division and submitting additional documents, Sun Life attempted to ask for further reconsideration regarding its notification to affected data subjects even after the Commission already denied their Request for Reconsideration. With this denial, the Resolution dated 29 July 2019 has already become final and executory. The Commission also notes that the additional information

[2] NPC Circular 16-03. Personal Data Breach Management. Dated 15 December 2016.

provided to the Enforcement Division was not included in their 9 September 2019 Request for Reconsideration with the Commission. It is basic that a division cannot overturn a decision or resolution of the administrative agency it belongs to.

In addition, Sunlife's continued refusal to notify the affected data subjects is inconsistent with its statements in its previously filed Request for Reconsideration, thus:

> In the event that the Honorable Commission decides to deny our request, we likewise respectfully seek an extension of time of 30 days from receipt of the decision to notify the affected data subjects.

While the Commission notes its eventual notification of some of the data subjects, this partial compliance comes after a significant amount of time has passed since the Resolution dated 29 July 2019 that ordered the submission of proof of its Compliance within thirty (30) days from the date of receipt thereof and the 28 October 2019 Resolution that denied Request for Reconsideration.

The Commission also notes that Sun Life's 07 July 2020 letter characterizes its 28 December 2019 letter as another request for reconsideration. Aside from the fact that a second request or motion for reconsideration is not allowed under NPC Circular 16-03, Sun Life also mischaracterizes the nature of its 28 December 2019 letter since the body of that letter merely requests for a face to face meeting with the Enforcement Division to clarify its requirements and for the Commission to toll the thirty (30)-day period provided in the Resolution dated 29 July 2019.

This unreasonable delay of Sun Life to comply with the Commission's Resolutions dated 29 July 2019 and 28 October 2019 may already constitute Failure to Notify as provided in NPC Circular 16-03:

> Section 20. Failure to Notify. In case the personal information controller fails to notify the Commission or data subjects, or there is **unreasonable delay** to notification, the Commission shall determine if such failure is justified. xxx[3]

[3] *Id.*, at Section 20. Emphasis supplied.

WHEREFORE, the above premises considered, the Commission resolves to **ORDER** Sun Life of Canada (Philippines), Inc. to show cause in writing, within fifteen (15) calendar days from receipt of this Order, why it should not be liable for Failure to Notify under Section 20 of NPC Circular 16-03 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.

SO ORDERED.

City of Pasay, Philippines
23 July 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:

ATC
Chief Compliance Officer

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission