Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: BREACH NOTIFICATION REPORT OF SUN LIFE OF CANADA
x----------

CID BN 17-021

RESOLUTION

AGUIRRE, D.P.C.

In an Order dated 23 July 2020, the Commission required Sun Life of Canada (Philippines), Inc. ("Sun Life") to show cause why it should not be subject to contempt proceedings and other actions available to the Commission for failing to comply with the Commission's decision, thus:

> **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.

In response to the Show Cause Order, Sun Life sent a letter dated 26 August 2020 explaining that:

1. A notification two years after the incident would cause undue alarm on the part of the data subjects.
2. The December 2019 Letter is not prohibited under NPC Circular 16-03.
3. Sun Life merely tried to exhaust all administrative remedies.
4. Sun Life believed in good faith that the Honorable Commission had yet to resolve the December 2019 Letter.
5. Sun Life did not willfully violate the Resolutions of this Honorable Commission.

A. Requirements for exemption from notification of data subjects

At the outset, it should be emphasized that notification of data subjects of data breaches is the general rule and exemption will only be allowed in exceptional circumstances when the Commission determines that

"such notification would not be in the public interest or in the interest of the affected data subjects."[1] It is a basic rule of evidence and procedure that the Commission, in making this determination, cannot simply rely on bare allegations. It looks at the available evidence on record to see whether these are sufficient to overcome the presumption that notification is in the best interest of the data subjects.

In this case, in seeking to be exempted from notifying its data subjects, Sun Life alleged in its 19 October 2017 breach notification that the breach is unlikely to give rise to a real risk of serious harm to data subjects since controls are in place to prevent the takeover of the account or any amendment, withdrawal or cancellation.[2] It also alleges that "notification would not be in the best interest of the affected policy holders and may cause undue alarm."[3] No evidence being submitted to support Sun Life's claims, this Commission denied its request for exemption.

Seeking the reconsideration of the Commission's 29 July 2019 Resolution, Sun Life filed a letter dated 5 September 2019 reiterating its earlier submissions emphasizing the measures it has taken to prevent a recurrence of the incident, the controls it has in place to prevent any fraudulent use of the information on its system, and the lack of any concern or complaints received in relation to the information that was disclosed. Despite the Commission's finding in its previous Resolution regarding Sun Life's failure to submit any evidence to support its claims, Sun Life again chose not to provide this Commission with any evidence to support its assertions. Instead, it simply asserts that "there is no vulnerability pertaining to access in this case that may be exploited by others."

While Sun Life may have taken the necessary steps to secure its system and prevent a recurrence of that incident, these remain mere assertions in the absence of any evidence to support them. In addition, the steps outlined by Sun Life are only with regard to the risks that may arise in relation to its own system. It did not consider the other risks, such phishing or social engineering attacks, that its data subjects may be subjected to as a result of the breach.

---

[1] National Privacy Commission Circular 16-03, Sec. 18(b).
[2] *See*, 19 October 2017 letter of Sunlife.
[3] *Id.*

When the Data Privacy Act ("DPA") states as one of the criteria for notification that the "unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject,"[4] it does not qualify that the risks and harms that should be considered are only those within the control of the personal information controller that was breached. Instead, the risks and harms that data subjects may face must be viewed holistically taking into consideration all the relevant circumstances.

B. The procedure followed by Sun Life is improper

In response to this Commission's Show Cause Order, Sun Life explained that the procedure it followed was not prohibited under this Commission's rules and that it was merely trying to exhaust all administrative remedies when it met with our Enforcement Division to submit additional documents in support of its request for reconsideration. These will be discussed *in seriatim*.

i. A second Motion for Reconsideration is not allowed.

Sun Life asserts that: "there is nothing in NPC Circular 16-03 that prohibits a second motion for reconsideration. Absent such prohibition, the Honorable Commission cannot categorically state that 'a second request or motion for reconsideration is not allowed under NPC Circular 16-03.'"[5]

Sun Life correctly states that NPC Circular 16-03 does not contain any prohibition on the filing of a second motion for reconsideration. It also does not contain anything on the process of filing a motion for reconsideration. As Sun Life is undoubtedly aware, NPC Circular 16-03 only provides for the obligation of personal information controllers in relation to breaches, including the obligation to notify the Commission and data subjects in the event of a breach.[6] The Commission's Rules of Procedure are contained in NPC Circular 16-04, Section 2 of which states:

---

[4] Republic Act No. 10173, Sec. 20 (f).
[5] Sun Life's letter dated 26 August 2020, p. 4.
[6] *See*, NPC Circular 16-03, Sec. 2. *Emphasis supplied.*

> **SECTION 2.** ***Scope and Coverage***. **–** These rules shall apply to all complaints filed before the National Privacy Commission or such other grievances, requests for assistance or advisory opinions, and **other matters cognizable by the National Privacy Commission.**

The proceedings involving personal data breach notifications clearly fall under "other matters cognizable by the National Privacy Commission." Hence, the determination whether a personal information controller such as Sun Life may be exempted from the requirement of notifying its data subjects is a matter falling within the scope of NPC Circular 16-04.

It is a basic rule of statutory construction that statutes must be construed and harmonized with other statutes to form a uniform system of jurisprudence.[7] Simply because NPC Circular 16-03 does not contain a provision prohibiting the filing of a second motion for reconsideration does not mean that it is allowed, as Sun Life claims, especially since it is expressly prohibited by NPC Circular 16-04:

> **SECTION 30.** ***Appeal***. **–** The decision of the National Privacy Commission shall become final and executory fifteen (15) days after the receipt of a copy thereof by the party adversely affected. **One motion for reconsideration may be filed**, which shall suspend the running of the said period. Any appeal from the Decision shall be to the proper courts, in accordance with law and rules.[8]

On the basis of this same provision, this Commission's 28 October 2019 Resolution denying Sun Life's Motion for Reconsideration has already become final and executory. As Sun Life itself admitted in its response to the Show Cause Order:

> 4. On 04 December 2019, Sun Life received the Honorable Commission's Resolution dated 28 October 2019 (the "October Resolution") denying the request for reconsideration in the September 2019 Letter.
>
> 5. On 23 December 2019, Sun Life responded to the October Resolution by submitting a letter dated 23 December 2019 (the "December 2019 Letter") requesting for the deferment of the running of the period within which to comply with the requirements of the July Resolution pending a meeting with the Honorable Commission's Enforcement Division.[9]

---

[7] *See,* Akbayan-Youth v. Commission on Elections, G.R. No. 147066, 26 March 2011.
[8] Emphasis supplied.
[9] Sun Life's letter dated 26 August 2020, p. 2.

Even assuming Sun Life's filing of the 23 December 2019 letter is allowed, it was filed beyond reglementary period having been filed nineteen (19) days after Sun Life received a copy of this Commission's resolution denying its request for reconsideration.

ii. Sun Life's reliance on the doctrine of exhaustion of administrative remedies is misplaced.

Its second request for reconsideration having been filed out of time and in clear contravention of the prohibition on the filing of second motions for reconsideration, Sun Life cannot now claim that it was merely exhausting administrative remedies when it sought to meet with this Commission's Enforcement Division and submit additional evidence.

In the first place, the proper time to submit evidence to substantiate its request for exemption was when it first filed the same or, at the very least, when this Commission called its attention to this deficiency in the 29 July 2019 Resolution. In both instances, Sun Life either failed or chose not to.

If Sun Life believes that this Commission's decision denying its request for exemption did not consider all the relevant factors, it only has itself to blame for not submitting all the necessary evidence and raising all of its arguments when it had numerous opportunities to do so.

Similar to parties coordinating with the sheriff in the execution stage of a court case, it should be stressed that there is nothing wrong with meeting with the Enforcement Division to clarify how compliance with this Commission's resolution should best be carried out. It is an altogether different matter, however, to attempt to get the sheriff to intercede on a party's behalf to reverse the decision of the court. This is what Sun Life attempted to do in this case. While this Commission endeavors to keep an open line of communication with its stakeholders, this does not mean that proper procedure can be dispensed with especially in pending cases and more so in cases, such as this one, where a decision has already been rendered. This is not what the doctrine of exhaustion of administrative remedies contemplates.

In addition, Sun Life attempts to justify its refusal to comply with this Commission's decision by pointing to the length of time that has passed from the time it requested for exemption until the denial, stating:

> Without a doubt, it heightened Sun Life's earlier concern that a notification would cause undue alarm on the part of the data subjects.
>
> Considering the foregoing factual antecedents, it was reasonable for Sun Life to be persistent in seeking a reconsideration of the July Resolution and the October Resolution, hence, the submission of the October 2019 Letter and the December 2019 Letter.[10]

To reiterate, the notification of data subjects is the general rule. In asking for exemption from this general rule, personal information controllers like Sun Life bind themselves to comply with this Commission's Decision on their request. They cannot impose as a condition to such compliance that the Decision must be rendered within a period of time convenient to them. In the absence of a change in circumstances that would render compliance impossible, and Sun Life has not alleged much less submitted any evidence in this regard, it is subject to the requirements of the DPA and NPC Circular 16-03, as clarified by the Commission in its Decision.

Nevertheless, at its core, the notification requirement under NPC Circular 16-03 is for the protection and benefit of data subjects. This Commission acknowledges the efforts Sun Life made to address the breach when it occurred and, although delayed, the efforts it has since undertaken to properly notify and protect its data subjects as shown in its 07 July 2020 and 28 July 2020 letters.

Despite the issues discussed herein being straightforward, rooted as they are in express provisions and clear principles of the Data Privacy Act and its related issuances, this Commission recognizes that misconceptions and misapplications of these doctrines still persist. Considering that the factual antecedents of this case all occurred during the time of Sun Life's previous data protection officer, hopefully Sun Life will take stock of the circumstances of this case and the Commission expects it to take the necessary steps to ensure not only that this situation will not be repeated but, more importantly, that it will be in a better position to safeguard its data subjects. Compliance

[10] Sun Life's letter dated 26 August 2020, p. 3.

with the DPA entails more than simply ticking off boxes on a checklist such as the registration of a Data Protection Officer, conduct of a privacy impact assessment, creation of a data protection policy, or the exercise of breach reporting procedures. Companies must realize that compliance with the DPA involves doing such activities within a framework of protecting the data subjects from very real risks, such as what the affected data subjects faced in this case.

Guided by the principle that the power of contempt should be used sparingly, judiciously, and with utmost self-restraint,[11] this Commission resolves to consider Sun Life as having satisfactorily complied with the Show Cause Order. Sun Life is warned, however, that any violation of a similar nature will be dealt with more severely.

WHEREFORE, the above premises considered, the Commission resolves to consider this matter **CLOSED**. Sun Life of Canada (Philippines), Inc. is hereby given a **STERN WARNING** that a repetition of this conduct or a similar infraction shall be dealt with more severely.

SO ORDERED.

City of Pasay, Philippines;
10 September 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[11] *See,* Baustista v. Yujuico, G.R. No. 199654, 03 October 2018.

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

JSC
Data Protection Officer

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