IN RE: MANUFACTURERS LIFE INSURANCE CO.

NPC BN 18-213

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a confidentiality breach involving the misdelivery of a Variable Unit Linked (VUL) Statement of Account (SOA) belonging to a Manufacturers Life Insurance Co. (Manulife) client.

Facts

On 13 November 2018, a Manulife agent emailed its Customer Care to report that his client, VL, received a VUL SOA by mail.[1] The VUL SOA, however, belonged to another Manulife client, LTE.[2]

Manulife sent an Incident Notification dated 30 November 2018 to the National Privacy Commission (NPC). Manulife explained that it learned of the incident on 14 November 2018.[3] The VUL SOA contained the following information: "1) Name of client; 2) Address; 3) Policy number; 4) Name of insured; and 5) Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments, etc.)."[4]

---

[1] Full Report, 21 October 2020, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[2] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[3] *Id.*
[4] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Manulife also reported that it discovered that "LTE's outdated mailing address resulting [sic] to the same being delivered to her old address now being occupied by VL."[5]

As a result, Manulife immediately requested VL to surrender or return the misdelivered VUL SOA to her agent.[6] Manulife also asked its Information Services (IS) Team to immediately conduct an investigation of the incident.[7]

Manulife's IS Team initially reported to management that "[t]he old address supplied by the client, which address had already been previously updated, was erroneously tagged as the client's current mailing address"[8] and that "only VUL SOAs were affected."[9]

As its measures to address the breach, Manulife reported that the IS Team implemented fixes to ensure the system generating the VUL SOAs would use the correct and updated addresses of its clients.[10] In the meantime, Manulife stated that "no VUL SOAs were generated and sent out."[11] The fixes were reported to have been completely implemented on 16 November 2018.[12] Manulife did not affirm whether VL fulfilled its request to surrender or to destroy the VUL SOA.

Manulife maintained that "[d]espite the information contained in the VUL SOA," it had appropriate measures in place to minimize the risk of harm or fraud that may arise from the misdelivery.[13] It argued:

> Should a person call the Company's hotline, minimum validation procedures are in place to verify the identity of the client. These validation questions pertain to information that cannot be found in the VUL SOA. For other transactions involving the client's policy, specific forms have to be filled out and identification documents need to be submitted.

---

[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> In light of the validation requirements in place that sufficiently protect the client from identity theft and fraud, or some other serious harm, it is respectfully asserted that Manulife Philippines is not required to notify the affected client. Nevertheless, rest assured that the Company will make the necessary notification if further investigation reveals that the same is warranted.[14]

On 06 October 2020, the NPC, through its Complaints and Investigation Division (CID), issued an Order directing Manulife to submit its Full Report within fifteen (15) days from receipt.[15] With respect to Manulife's Incident Notification dated 30 November 2018, the CID concluded that "the notification did not provide the process conducted to notify the affected data subject."[16] The CID also found that the Incident Notification did not "offer assistance that may be required to mitigate any possible damage that may be caused by the incident."[17]

On 21 October 2020, Manulife submitted its full report in compliance with the CID's Order. It reiterated its narration in the Incident Notification dated 30 November 2018, with additional details as to security measures it had taken since the breach occurred.[18] Manulife also submitted a copy of its Data Privacy Manual.[19]

On 14 November 2018, or the day after the breach, the IS Team investigated the VUL SOA generation.[20] It confirmed that LTE's old mailing address, which was now VL's current address, was erroneously tagged as LTE's current mailing address in the Client Administration System (CAS).[21] According to Manulife, the IS Team reported that the CAS "fetched the first address recorded in a policy record instead of the most current one."[22] The IS Team concluded that this error resulted from a system patch done at the end of October

---

[14] Incident Notification, 30 November 2018, at 1-2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[15] Order, 06 October 2020, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[16] *Id.* at 1.
[17] *Id.*
[18] Full Report, 21 October 2020, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[19] *Id.*
[20] *Id.* at 1-2.
[21] *Id.* at 1.
[22] *Id.* at 1-2.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

2018.[23] The issue was then escalated to Manulife's Data Protection Officer.[24]

After an investigation by its Operations team and IS team, Manulife reported that it discovered the erroneous tagging similarly affected a total of one hundred (100) printed VUL SOAs.[25] Nonetheless, Manulife reported that it was able to stop its courier from sending eighty-nine (89) of the printed VUL SOAS.[26] Manulife explained that:

> Out of the 11 delivered VUL SOAs:
> - 8 were actually received by the correct clients;
> - 1 had the correct address;
> - 1 was sent to the client's office address where he was still connected at that time;
> - 1 pertained to a client who was outside of the Philippines. This client was contacted by a Manulife agent and did not pose any complaint or issue regarding his non-receipt of the SOA.[27]

As such, Manulife concluded that other than LTE, no other clients were impacted by the incident.[28]

According to Manulife, the personal data of LTE involved and disclosed to VL were: "a) Name of affected client as Policy Owner and Insured; b) Address, old address of affected client which was now the address of the unintended recipient; c) Policy number of affected client; and d) Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments)."[29] Nonetheless, Manulife argued that the personal data involved is insufficient for VL to access LTE's Manulife account.[30] Further, Manulife argued that VL remained unaware of LTE's current address.[31]

---

[23] *Id.*
[24] Full Report, 21 October 2020, at 2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[25] *Id.*
[26] *Id.* at 1-2.
[27] *Id.* at 2.
[28] *Id.*
[29] *Id.* at 3.
[30] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[31] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Manulife also explained why "there is a low likelihood of any adverse impact on the data subject":[32]

> a) It is highly unlikely that the data received by the **sole** unintended recipient, the very same person who reported the incident to her Manulife agent, would be used for identity theft or other nefarious purposes by the recipient.
>
> b) It should also be noted that validation procedures are in place to verify the identity of a client who calls or communicates with the Company. These validation questions pertain to information that cannot be found in the VUL SOA that was sent to the unauthorized recipient. This means that the information the unauthorized recipient got from the VUL SOA would not be sufficient for her to conduct transactions on the policy belonging to the other client.
>
> c) Further, for major transactions involving a client's policy (such as change of address or beneficiary, surrender of policy, policy loans), specific forms have to be filled out and signed by the client, and valid identification documents have to be submitted.[33]

Manulife also reported taking "safeguards to minimize harm or mitigate impact of the breach."[34] It explained that it stopped sending VUL SOAs immediately upon learning of the error and "until the system issue was identified and fixed."[35] It also stated that it checked LTE's policy for possible suspicious transactions[36] and that "[t]o date, there has been no red flag for any account takeover or fraud on the data subject's account."[37]

Manulife stated that once the issue with its CAS was resolved, it performed a qualitative check and an audit on the VUL SOAs sent out for the next thirty (30) days, "to ensure that the correct information were being picked up in the SOAs" prior to being sent out to clients.[38] Manulife also reported adding "enhancements to the software

---

[32] *Id.* at 2.
[33] *Id.*
[34] *Id.* at 3.
[35] *Id.*
[36] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[37] *Id.*
[38] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

development lifecycle" to avoid recurrence of the incident.[39] It also stated that "mandatory testing and Quality Assurance were made compulsory prior to the release of any SOA."[40] According to Manulife, "[a]s far as practicable, taking into consideration the inherent and residual risks, all system enhancements involving clients' data have undergone the necessary testing and signoffs before they were implemented."[41]

On remedial measures to address the breach, Manulife reiterated that it advised VL to either return the VUL SOA to Manulife or to destroy it.[42] Similar to its Incident Notification,[43] however, Manulife did not confirm whether VL returned or destroyed the VUL SOA.

Manulife also reported engaging the services of a third-party service provider, KPMG, to "conduct an evaluation of existing processes, systems and controls that impact data privacy."[44] Manulife explained that this third-party independent evaluation was "supposed to have been done at the early part of [2020] but was delayed due to the current COVID-19 situation."[45]

Given the foregoing measures, Manulife argued that the incident "has almost no adverse impact on the Company and the public at large."[46] Manulife maintained that "[i]f at all, the incident led the Company to improve its existing systems and processes to better protect its clients' information."[47] Manulife also noted that "to date, it has not received any complaint arising from mis-directed [sic] VUL SOAs."[48]

Finally, Manulife requested exemption from the notification of the affected data subject.[49] It reasoned:

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] Full Report, 21 October 2020, at 1-2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[43] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[44] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[45] *Id.*
[46] *Id.* at 2.
[47] *Id.*
[48] *Id.*
[49] *Id.* at 4.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> In determining whether there was a need to notify the data subject of the incident, the primary consideration was the likelihood of harm or negative consequence caused by the mis-delivered VUL SOA.
>
> In light of the validation requirements in place that sufficiently protect the client from identity theft and fraud, or some other serious harm, it is respectfully requested that pursuant to Section 19, Rule V of the National Privacy Commission Circular 16-03 on Personal Data Breach Management, the Company be exempted from Notification Requirements. This request is bolstered by the fact that despite the lapse of two years from the incident, there was in fact no suspicious transaction on data subject's account.[50]

On 09 December 2022, the CID assessed that the matter does not fall within mandatory notification under NPC Circular 16-03 (Personal Data Breach Management):

> It must be remembered that Manulife specified that they have a validation procedure in place to verify the identity of a client who calls or communicates with their Company. These validation questions pertain to information which cannot be found in the SOA sent to the unintended recipient. But it may not be easily possible since confirmation for such change and account log-in are required.
>
> Although there is reason to believe that the information may have been acquired by unauthorized individuals, we determine **that the limited personal data affected by the subject breach cannot be used to enable identity fraud** to claim any benefits arising from the insurance contract. **Also, when the unintended recipient immediately reported the mixed-up to Manulife, the recipient's action negated any risk which may arise from the incident caused by a system patch.** Thus, the likelihood of giving rise to real risk of serious harm to the affected data subjects is very low, if not, negligible.
>
> Thus, with only two (2) out of three elements for a mandatory breach notification present in this case, it is hereby determined that notification, in this case, is not required.[51]

The CID stated that the incident was addressed, and that Manulife satisfactorily complied with the Order.[52] It concluded that the matter

---

[50] Full Report, 21 October 2020, at 4, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[51] Final Breach Notification Evaluation Report, 09 December 2022, at 6, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[52] *Id.* at 8.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

does not fall under mandatory breach notification as provided in NPC Circular 16-03,[53] and as such, Manulife was not required to notify its affected data subject.[54]

Issue

Whether Manulife sufficiently addressed the breach incident and implemented security measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. The incident does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03. Only the first two requisites are present in this case. The third requisite of real risk of serious harm is absent because of prior and subsequent security measures implemented by Manulife.

Section 11 of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor 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

[53] *Id.*
[54] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> rise to a real risk of serious harm to any affected data subject.[55]

Following this, mandatory breach notification to the Commission has the following requisites:

1. The breach involves sensitive personal information, or information that may be used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.[56]

The first requisite is present. The nature of the information involved may enable identity fraud.

In this case, the information on the VUL SOA is considered "information about the financial or economic situation of the data subject" under Section 11 (A) of NPC Circular 16-03.[57] It contains specific information on LTE's life insurance policy, namely "Account summary (face amount, units bought/sold, premium amount, balances, charges/fees, current value, payments)"[58]

Further, the information on the VUL SOA is considered information "which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits" under Section 11 (A).[59] The VUL SOA includes a Manulife client's name, address, policy number, and name of insured,[60] which are necessary considerations for Manulife's decision to grant insurance claims and release of proceeds, if any.

---

[55] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[56] In re: Commission on Elections, Smartmatic Group of Companies, RVA, WS, and other John Does and Jane Does Initiated as a Sua Sponte NPC Investigation on Possible Data Privacy Violations Committed in Relation to the Alleged Hack and Breach of the Commission on Elections System or Servers, NPC SS 22-001 and NPC SS 22-008, 22 September 2022, at 19, *available at* https://www.privacy.gov.ph/wp-content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-Commission-on-Elections-Decision-Final.pdf (last accessed 31 January 2023).
[57] NPC Circ. No. 16-03, § 11 (A).
[58] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[59] NPC Circ. No. 16-03, § 11 (A).
[60] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Other similar information referred to in the last sentence of Section 11(A) of NPC Circular 16-03 need not necessarily be personal information.[61] For mandatory breach notification, Section 20 (f) of Republic Act No. 10173 or the Data Privacy Act (DPA) only requires that the information may enable identity fraud:

> Section 20. *Security of Personal Information.*
>
> . . .
>
> (f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or **other information that may, under the circumstances, be used to enable identity fraud** are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.[62]

Further, Section 11 (A) of NPC Circular 16-03 itself includes the phrase "shall include, but not be limited to," which means the enumeration is not an exclusive list:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor 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

[61] NPC Circ. No. 16-03, § 11 (A).
[62] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this purpose a National Privacy Commission, and For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 § 20 (f) (2012). Emphasis supplied.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> 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.[63]

In other words, "other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits" does not necessarily refer to personal information, so long as the information may enable identity fraud.[64]

In this case, the name of the insured, and policy number are important—if not the most important—details with respect to a life insurance policy. The outdated address on the VUL SOA provides even more specific details that may be used to assume the policy holder's identity.

Given the foregoing, and the fact that VL did not surrender or provide confirmation of the destruction of the VUL SOA, unauthorized acquisition of the information on the VUL SOA may be used to fraudulently assume the identity of the policy holder LTE.

The second requisite is also present. An unauthorized person acquired the information in LTE's VUL SOA.

The Commission held that a loss of control over personal data held in custody is enough for a Personal Information Controller (PIC) to have "reason to believe that the information may have been acquired by an unauthorized person."[65]

In this case, Manulife categorically stated in its Incident Report[66] and Full Breach Report[67] that VL received the VUL SOA. It even stated that VL was advised either to return it or destroy it.[68] Hence, Manulife

---

[63] NPC Circ. No. 16-03, § 11. Emphasis supplied.
[64] *Id.* § 11 (A).
[65] NPC BN 20-158, 21 September 2020, at 5 (NPC 2020) (unreported).
[66] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[67] Full Report, 21 October 2020, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[68] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

admitted and confirmed that there was loss of control by the PIC and the acquisition of the affected data subjects' personal data by an unauthorized person.

Nonetheless, the third requisite is not present due to the security measures implemented by Manulife.

The Commission takes this opportunity to discuss the determination of the presence of the third requisite of mandatory breach notification. Section 11 (C) of NPC Circular 16-03 provides:

> Section 11. *When notification is required*. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions.
>
> . . .
>
> 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.[69]

For this purpose, the phrase "likely to give rise to a real risk" in Section 11 (C) means that a link exists between the breach and the possible resulting harm to any affected data subject.[70] The risk must be apparent and not the product of mere speculation.[71] "Serious harm" means that the consequences and effects to any affected data subject is significant based on the surrounding circumstances of the breach.[72]

In determining whether the unauthorized acquisition is likely to give rise to real risk of serious harm, a PIC or the Commission may consider several factors, such as: the nature and amount of information involved in the breach, the period of time that has lapsed since the breach, objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.

---

[69] NPC Circ. No. 16-03, § 11.
[70] NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8 (NPC 2023) (unreported).
[71] *Id.*
[72] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

In this case, the unauthorized acquisition of information was due to the erroneous delivery to VL[73] There is no showing that she deliberately intended to obtain LTE's information, as she reported the misdelivery to her agent, who in turn reported the issue to Manulife.[74] Thus, the objective of the unauthorized acquisition was not for fraudulent purposes.

Nonetheless, the nature and amount of information involved in this matter may enable identity fraud. The name of the policy holder, name of the insured, and policy number are important, if not the most important, details with respect to claims on an insurance policy, and the other information such as address and account summary provides even more specific details. Despite Manulife's request to VL, it did not affirm in any of its submissions that VL actually surrendered or confirmed the destruction of LTE's VUL SOA.

Given the foregoing circumstances, including the possibility of fraudulent actions or claims in relation to LTE's insurance policy, there was a real risk of serious harm to the data subject in this case. Manulife itself admitted this risk when it stated that "the appropriate measures in place to minimize the risk of identity theft or fraud that may arise from the misdelivered VUL SOA."[75]

The security measures implemented by Manulife, however, prevented the occurrence of the risk of serious harm to the affected data subject.

Manulife was able to substantiate its claim of "low likelihood of any adverse impact on the data subject"[76] due to the validation measures that it had in place. Manulife stated that "for major transactions involving a client's policy (such as change of address or beneficiary, surrender of policy, policy loans), specific forms have to be filled out and signed."[77] Thus, any person intending to conduct a transaction as

---

[73] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).
[74] *Id.*
[75] Full Report, 21 October 2020, at 3, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[76] *Id.* at 2.
[77] *Id.*

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

to an insurance policy must also submit valid identification documents, in addition to the validation questions, to Manulife.[78]

Manulife also reported continuously monitoring the generation of VUL SOAs.[79] As of 21 October 2020, when Manulife filed its Full Breach Report, it stated that it had continuously monitored LTE's policy for possible suspicious transactions, and that "there has been no red flag for any account takeover or fraud on the data subject's account."[80]

Manulife also flagged the erroneous tagging that similarly affected a total of one hundred (100) printed VUL SOAs.[81] It was able to stop its courier from sending eighty-nine (89) VUL SOAs, and to monitor and resolve the delivery of the remaining eleven (11).[82] In fact, Manulife explained in its Full Report that:

> Out of the 11 delivered VUL SOAs:
> - 8 were actually received by the correct clients;
> - 1 had the correct address;
> - 1 was sent to the client's office address where he was still connected at that time;
> - 1 pertained to a client who was outside of the Philippines. This client was contacted by a Manulife agent and did not pose any complaint or issue regarding his non-receipt of the SOA.[83]

Manulife also reported halting the generation of VUL SOAs altogether while its IS Team implemented fixes for the issue of erroneous tagging of addresses.[84]

To reiterate, the security measures implemented by Manulife—the requirement of answering validation questions and submitting identification documents for any changes or major transactions on a client's insurance policy, halting the generation and delivery of VUL

---

[78] *Id.*
[79] *Id.* at 3.
[80] *Id.*
[81] Full Report, 21 October 2020, at 2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[82] *Id.* at 1-2.
[83] Full Report, 21 October 2020, at 2, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2020).
[84] Incident Notification, 30 November 2018, at 1, *in* In re: Manufacturers Life Insurance Co., NPC BN 18-213 (NPC 2018).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

SOAs until the client address tagging issue was fixed, and constant monitoring until 21 October 2020—were sufficient to protect LTE from fraudulent transactions resulting from the disclosure of her information. This removed the real risk of serious harm to the affected data subject.

Given the foregoing, the Commission finds that Manulife was able to address the breach and implement security measures to prevent real risk of serious harm from occurring. As such, the matter does not fall under mandatory breach notification.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-213 In re: Manufacturers Life Insurance Co. is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
29 June 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

JJN
Assistant Vice President,
Head of Risk Management &
Data Protection Officer
Manufacturers Life Insurance Co.

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

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228