IN RE: SOCIAL SECURITY SYSTEM **NPC BN 18-038**

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach notification submitted by the Social Security System (SSS) involving the disclosure of its members' information.

Facts

On 22 March 2018, the SSS notified the National Privacy Commission (NPC) of a breach that occurred in its Tarlac Branch:

> In line with the implementation of the Data Privacy Act of 2012, we are respectfully reporting a data breach incident involving the personal information of twenty-two (22) SSS members. On March 14, 2018, MCM, [ ], SSS Tarlac Branch, submitted a Memorandum, addressed to the SSS President and CEO and two (2) other Branch Operations Sector Officers, concerning a complaint against SSS Tarlac Branch. A concerned citizen with email address, [ ], was copy furnished as shown in the said Memorandum. Attached to the Memorandum are several documents containing personal and sensitive personal information.[1]

In its data breach notification, the SSS informed the NPC that the breach involved the Social Security Number, Full Name, Father's Name, Mother's Name, Contact Number, Email Address, Gender, Marital Status, Height and Weight, Date of Birth, Place of Birth,

[1] Data Breach Notification, 20 March 2018, *in* In re: Social Security System, NPC BN 18-038 (NPC 2018).

Address, Photo and Signature of three (3) data subjects.[2] It also involved the Social Security Number, Full Name, Date of Birth and Gender of nineteen (19) data subjects.[3]

According to MCM, [ ] of the SSS Tarlac Branch, she attached the documents containing the personal data of the affected data subjects to the memorandum as documentation of the verification measures that she conducted in relation to the concerns raised by the alleged SSS client with email address [ ].[4] MCM stated that she obtained the personal data of the affected data subjects who were named "OLS" or "OLS" upon conducting a database search.[5]

To address the breach, the SSS stated that MCM would personally explain and apologize to the three (3) data subjects.[6]

On 17 September 2018, the NPC, through its Complaints and Investigation Division (CID), issued a Memorandum dated 07 September 2018 requiring the SSS to submit a full report detailing the incident.[7] In the Memorandum, the CID required additional information on the nature of the breach, personal data possibly involved, and measures taken to address the breach.[8]

On 09 December 2020, the CID issued an Order requiring the SSS to submit documents in connection with the investigation of the breach.[9]

On 24 September 2021, the CID sent an email to the SSS requesting documents to submit the following:

a. Data Privacy and Security Policy with a report on the changes made therein after the incident particularly on the (1) email handling, and (2) reporting lines in case of complaints and breach, as well as the security measures in place;

---

[2] *Id.* at 1.
[3] *Id.*
[4] *Id.* at 3.
[5] *Id.*
[6] *Id.* at 2.
[7] Memorandum, 07 September 2018, *in* In re: Social Security System, NPC BN 18-038 (NPC 2018).
[8] *Id.* at 1-2.
[9] Order, 09 December 2020, *in* In re: Social Security System, NPC BN 18-038 (NPC 2020).

b. Copies of communications with the owner of the subject email account with address [ ], as well as the reply/results of the request to delete and prohibition from disseminating;
c. Proof of deletion of the subject email and its attachments from the subject email account;
d. We noted that the attached proof of sending via registered mail contains only the mailing to 10 out of 22 affected data subjects. Attach proof of receipt/sending of notification via registered mail to the other 12 of the 22 affected data subjects;
e. Attach the Results of the Privacy Impact Assessment (PIA) on the identification of privacy risks and adaption of the appropriate security measures to protect personal data against natural and human dangers in accordance with the guidelines provided under NPC Advisory No. 2017-03 on PIA;
f. Proof of cascading, training and continuing education in relation to personal data security/privacy and related policies as well as proof of attendance of the officers and employees and training materials thereof;
g. Physical, organizational and technical measures undertaken to eliminate/prevent recurrence of the incident, as well as proof of implementation thereof.[10]

On 12 October 2021, the SSS submitted its compliance with the Order dated 24 September 2021.[11] SSS' submissions include the Office Orders covering the changes in its data privacy and security policy, communications with the owner of the subject email address, proof of the notification sent to the affected data subjects, documentation of the results of the Privacy Impact Assessment documentation of training and continuing education programs on data security and privacy and documentation of the physical, organizational and technical measures it took to eliminate or prevent the recurrence of the incident.[12] The SSS also clarified that twenty-one (21) data subjects were notified through registered mail on 16 March 2018.[13] The SSS explained that in the email

[10] Letter, 24 September 2021, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[11] Letter Re Compliance with the Request to Submit Additional Documents Needed for Further Investigation, 12 October 2021, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[12] *Id.* at 1-2.
[13] *Id.* at 1.

sent on 19 March 2019 to [ ], it requested the user to immediately delete the email that was erroneously sent on 14 March 2018 and informed the user that she was prohibited from disseminating, distributing, or copying the email.[14]

On 09 November 2021, the CID sent an email to the SSS requesting additional documents and information.[15] Specifically, the CID requested the flowchart of the process implemented by the SSS in reporting the breach to the NPC and a copy of the assessment procedure or its equivalent concerning the data privacy matters of the SSS' clients.[16]

On 16 November 2021, the SSS submitted its compliance with the Order dated 09 November 2021.[17] The SSS provided the additional information requested by the CID including a chronology of the events surrounding the breach as well as a flowchart of the notification process followed by the SSS in the event of a breach.[18]

On 05 January 2023, the CID issued an Order directing the SSS to submit a Post-Breach Report, which contains proof of confirmation of deletion of the email by OLS, the owner of the email address [ ], and proof that the notification was successfully received by the affected data subjects.[19] On 13 January 2023, the SSS requested an extension of time to submit its Post-Breach Report.[20]

On 17 January 2023, the CID issued a Resolution granting the request for extension and ordering the SSS to submit its compliance on 26 January 2023.[21]

---

[14] *Id.* Annex C.
[15] Letter, 09 November 2021, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[16] *Id.*
[17] Letter Re Compliance with the Request to Submit Additional Documents Needed for Further Investigation, 16 November 2021, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[18] *Id.* at 1-3.
[19] Order (To submit a Post-Breach Report), 05 January 2023, *in* In re: Social Security System, NPC BN 18-038 (NPC 2023).
[20] Email Re Request for Extension, 13 January, 2023, *in* In re: Social Security System, NPC BN 18-038 (NPC 2023).
[21] Resolution (of the Request for Extension filed on 13 January 2023), 17 January 2023, *in* In re: Social Security System, NPC BN 18-038 (NPC 2023).

On 25 January 2023, the SSS submitted its compliance with the Order dated 05 January 2023.[22] As proof of the email communications between the SSS and the owner of the email address [ ], the SSS attached to its compliance copies of the emails sent by MCM on 19 March 2018 and 18 January 2023 requesting deletion of the email containing the information of the affected data subjects.[23] According to the SSS, MCM did not receive any response to these emails.[24] Additionally, the SSS also attached a copy of the notification that it received from Microsoft stating that the mailbox of the addressee of the email sent on 18 January 2023 was no unavailable, and that the email was not found at Yandex.com .[25] As proof that the affected data subjects were duly notified, the SSS attached as proof copies of the notification letters sent,[26] a certification from the Postmaster of the Tarlac City Philippine Postal Services showing successful delivery of fifteen (15) notification letters out of all of those sent,[27] documentation of the coordination efforts made by MCM to cause the personal delivery of the notification letters to the remaining data subjects[28] and documentation supporting the final delivery status of the remaining six (6) notification letters.[29]

Issue

I. Whether the incident is subject to mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Management).

II. Whether the SSS conducted proper breach management in compliance with NPC Circular 16-03.

Discussion

The breach is subject to mandatory breach notification under Section 11 of NPC Circular 16-03. Here, the SSS conducted proper breach management by notifying its affected data subjects and implementing security measures to mitigate the risks associated with the breach and

---

[22] Letter, 25 January 2023, *in* In re: Social Security System, NPC BN 18-038 (NPC 2023).
[23] *Id.* Annex I.
[24] *Id.* at 1.
[25] *Id.* Annex II.
[26] *Id.* Annex III
[27] *Id.* Annex IV.
[28] Letter, 25 January 2023, Annex V, *in* In re: Social Security System, NPC BN 18-038 (NPC 2023).
[29] *Id.* Annex VI.

prevent its recurrence. Thus, the Commission resolves to close the matter.

I. The matter falls under mandatory breach notification under Section 11 of NPC Circular 16-03.

Section 11 of NPC Circular 16-03 on mandatory breach notification 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 rise to a real risk of serious harm to any affected data subject.[30]

Following this, the requisites for mandatory breach notification to the Commission are:

[30] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).

1. The breach involves sensitive personal information, or information that may, under the circumstances, be used to enable identity fraud;[31]
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.[32]

All the requisites are present in this matter.

First, the breach involves sensitive personal information or information that may, under the circumstances, be used to enable identity fraud.

According to the SSS, the information involved in the breach included the SSS Number, Full Name, Date of Birth and Gender of all twenty-two (22) affected data subjects.[33] For three (3) of these data subjects, their Father's Name, Mother's Name, Contact Number, Email Address, Marital Status, Height and Weight, Place of Birth, Address, Photo, and Signature were involved in the breach.[34]

The SSS Number, Date of Birth, Gender, and Marital Status of the affected data subjects are considered sensitive personal information under Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Section 3 (l) of the DPA defines sensitive personal information as follows:

> Section 3. *Definition of Terms*. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

---

[31] In re: Pacific Plaza Towers Condominium Corporation, NPC BN 18-138, 13 November 2023, at 7, *available at* https://privacy.gov.ph/wp-content/uploads/2024/08/NPC-BN-18-138-2023.11.13-In-re-Pacific-Plaza-Resolution-Final.pdf (last accessed 03 January 2025).
[32] 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://privacy.gov.ph/wp-content/uploads/2024/05/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-COMELEC-Decision-FinalP.pdf (last accessed 03 January 2025).
[33] Data Breach Notification, 20 March 2018, at 1, *in* In re: Social Security System, NPC BN 18-038 (NPC 2018).
[34] *Id.*

. . .

> (l) *Sensitive personal information* refers to personal information:
>
> > (1) About an individual's race, ethnic origin, **marital status**, **age**, color, and religious, philosophical or political affiliations;
> >
> > (2) About an individual's **health**, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
> >
> > (3) **Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns;** and
> >
> > (4) Specifically established by an executive order or an act of Congress to be kept classified.[35]

Here, the SSS Number is considered sensitive personal information because it is issued by a government agency, and it is peculiar to the individual to whom it is issued. Date of Birth is also sensitive personal information because it can be used to determine the data subject's age.

The SSS Number, Full Name, Father's Name, Mother's Name, Contact Number, Email address, Gender, Marital Status, Height and Weight, Date of Birth, Place of Birth, Address, Photo, and Signature of the affected data subjects can also be considered other information that may be used to enable identity fraud under the circumstances.

In determining whether other information involved in the breach may enable identity fraud, Section 11 of NPC Circular 16-03 should be read

---

[35] 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 § 3 (l) (2012). Emphasis supplied.

together with Section 20 (f) of DPA. Section 20 (f) expressly requires the consideration of the specific circumstances of the breach in making this determination:

> 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.[36]

The Commission previously held that a data subject's name and email may be considered under other information that may enable identity fraud.[37] The Commission explained:

> This Commission takes this opportunity to stress that information that may be used to enable identity fraud under Section 11 (A) is not limited to the categories of information listed therein, such as 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

[36] *Id*. § 20 (f) Emphasis supplied.
[37] In re: E-Science Corporation, NPC BN 20-124, 10 September 2020, at 3, *available at* https://privacy.gov.ph/wp-content/uploads/2024/09/NPC-BN-20-124-2020.09.10-In-re-E-Science-Corporation-Resolution.pdf (last accessed 03 January 2025).

> made the basis of decisions concerning the data subject, including the grant of rights or benefits.
>
> **Contrary to Respondent's claim, names and e-mail addresses are information that may be used to enable identity fraud. An e-mail address is considered personal information and an unauthorized acquisition thereof could easily trace the identity of the data subject through the conduct of "Phishing" attacks to obtain more information about the user which would then be used to access important accounts resulting to identity theft and financial loss.**[38]

In that case, the Commission determined that the names and email addresses of the data subjects are information that may be used to enable identity fraud.[39] The Personal Information Controller (PIC) reported that a hacker accessed and implanted ransomware in an online database.[40] Because of these circumstances, the Commission concluded that the hacker may contact and send malicious emails directly to the data subjects.[41]

Here, the Memorandum and its attachments contain information that may be used to enable identity fraud. The email addresses of the affected data subjects, taken together with the other personal data involved may be used by an unauthorized person to gain access to important accounts belonging to the data subject. Further, an unauthorized person in possession of the data subject's photo and signature may use these to bypass certain validation measures to the prejudice of the data subject. Based on the nature and amount of information sent by the SSS to [ ], the breach involves information that may, under the circumstances, be used to enable identity fraud.

Thus, the first requisite is present because the breach involves both sensitive personal information and other information that may, under the circumstances, be used to enable identity fraud.

---

[38] *Id.* Emphasis supplied.
[39] *Id.* at 4.
[40] *Id.*
[41] *Id.*

Second, there is reason to believe that the information may have been acquired by an unauthorized person.

An unauthorized person acquired the information when the Memorandum and its attachments were sent to the email, [ ].[42] Here, the email was addressed to officials of the SSS particularly the President and CEO and two (2) other Branch Operations Sector Officers.[43] The Memorandum and its attachments, however, were also inadvertently sent to [ ].[44] As observed by the SSS, the Memorandum was an internal correspondence not intended to be sent to [ ].[45]

Thus, the second requisite is present since there is a reasonable belief that an unauthorized person acquired the information involved in the breach.

Third, there is a real risk of serious harm in this case.

The following factors are considered in determining the presence of the third requisite of mandatory breach notification. Section 11 I 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.[46]

---

[42] Letter Re Compliance with the Request to Submit Additional Documents Needed for Further Investigation, 16 November 2021, at 2, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[43] *Id.*
[44] *Id.*
[45] Letter Re Data Breach Incident Report Dated March 20, 2018, 21 September 2018, at 2, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[46] NPC Circ. No. 16-03, § 11.

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.[47] The risk must be apparent and not the product of mere speculation.[48] Serious harm means that the consequences and effects to any affected data subject are significant based on the surrounding circumstances of the breach.[49]

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.[50]

In this case, the nature and amount of the information acquired by the unauthorized individual show that there is a real risk of serious harm in this case. The potential for misuse and exposure of the information involved is great considering the nature and amount of information that was disclosed for each of the affected data subjects. Thus, the third requisite is present because there is a real risk of serious harm to the affected data subjects.

Thus, this matter falls under mandatory breach notification under Section 11 of NPC Circular 16-03.

II. SSS conducted proper breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Considering that all the requisites for mandatory breach notification are present, it was not only necessary for SSS to notify the Commission and the affected data subjects but also implement measures to mitigate the risks resulting from the breach and prevent its recurrence.

---

[47] In re: Easytrip Services Corporation, NPC BN 17-028 and NPC BN 18-180, 11 May 2023, at 8, available at https://privacy.gov.ph/wp-content/uploads/2024/06/NPC-BN-17-028-_-18-180-2023.05.11-Resolution-FinalP.pdf (last accessed 03 January 2025).
[48] *Id.*
[49] *Id.*
[50] *Id.*

In this case, the SSS notified the Commission and the affected data subjects. The SSS notified the Commission of the breach on 22 March 2018.[51] In its data breach notification, the SSS described the personal data involved, measures taken to address the breach and measures being taken to address the breach.[52]Also, the SSS provided additional information on the breach in its compliance dated 12 October 2021.[53]

Notably, MCM informed the SSS of the breach through its Data Protection Officers (DPOs) on 15 March 2018.[54]

Section 17 of NPC Circular 16-03 provides:

> Section 17. *Notification of the Commission.* The personal information controller shall notify the Commission of a personal data breach subject to the following procedures.
>
> A. *When Notification Should be Done.* The commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a data breach has occurred.
>
> B. *Delay in Notification.* Notification may only be delayed 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.
>
> The personal information controller need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for

[51] Data Breach Notification, 20 March 2018, *in* In re: Social Security System, NPC BN 18-038 (NPC 2018).
[52] *Id.* at 1-2.
[53] Letter Re Compliance with the Request to Submit Additional Documents Needed for Further Investigation, 12 October 2021, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[54] Letter Re Compliance with the Request to Submit Additional Documents Needed for Further Investigation, 16 November 2021, at 2, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).

> any delay in notification, if such delay would be prejudicial to the rights of the data subjects.
>
> Delay in notification shall be excused if it is used to perpetuate fraud or to conceal the personal data breach.[55]

Here, the delay in the notification made by the SSS to the Commission is warranted. The SSS provided a chronology of the events as well as a flowchart of its notification process to explain the cause of the delay.[57] The delay was clearly due to the measures taken by the SSS to determine the scope of the breach. Although the breach was reported by MCM to the SSS on 15 March 2018, the SSS took measures to determine the scope or the breach and to prevent further disclosures following its internal notification process.[58] After receiving the SSS Data Breach Incident Report from MCM on 19 March 2018, the SSS promptly notified the Commission of the breach within seventy-two (72) hours or on 22 March 2018.[59]

In addition to this, the SSS also duly notified the affected data subjects. On 16 March 2018, the SSS through MCM sent out twenty-one (21) letters to the data subjects informing them of the incident.[60] Fifteen (15) of the letters were delivered successfully and six (6) were returned to sender.[61] The SSS took additional efforts to personally deliver the letters to the affected data subjects.[62] As shown in the copies of the notification letters sent to the affected data subjects, the SSS notified each data subject of the nature of the breach, the personal data possibly involved, and the contact details of its DPOs.[63] Also, the SSS stated that its Tarlac Branch is coordinating with the other departments of the SSS to take steps to improve the security of its members' information.[64] Additionally, the SSS informed the affected data subjects of its efforts to minimize or eliminate the potential harm brought about by the

---

[55] NPC Circ. No. 16-03, § 17.
[57] Letter Re Compliance with the Request to Submit Additional Documents Needed for Further Investigation, 16 November 2021, at 1-3, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).
[58] *Id.*
[59] *Id.*
[60] Letter, 25 January 2023, at 1, *in* In re: Social Security System, NPC BN 18-038 (NPC 2023).
[61] *Id.*
[62] *Id.*
[63] *Id.* Annex III.
[64] *Id.*

breach and requested them to take preventive measures against possible misuse of their information.[65]

The SSS took measures to address the breach and to prevent its recurrence. On 19 March 2018 and 18 January 2023, the SSS sent an email to [ ] requesting the deletion and non-dissemination of the email containing the personal data of the affected data subjects. While the SSS did not receive a reply from [ ], it received a notification that the email sent on 18 January 2023 was undelivered because the email address of the recipient was already inactive at that time.[66] The SSS had also implemented a Customer Relationship Management System, conducted training and continuing education to its personnel, and adopted other measures to prevent the occurrence of similar breaches.[67] Thus, the SSS had taken adequate measures to address the breach and to prevent recurrence of the breach.

Given the foregoing factors, the SSS conducted proper breach management. The SSS duly notified the Commission and the affected data subjects of the breach. It also implemented sufficient measures to address the breach and prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-038 In re: Social Security System is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
17 September 2024.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

---

[65] *Id*.
[66] Letter, 25 January 2023, at 1, *in* In re: Social Security System, NPC BN 18-038 (NPC 2023).
[67] Letter Re Compliance with the Request to Submit Additional Documents Needed for Further Investigation, 12 October 2021, *in* In re: Social Security System, NPC BN 18-038 (NPC 2021).

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

GDS
Data Protection Officer
Social Security System

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