IN RE: REJOB ENGLISH ASSESSMENT, INC. (FORMERLY GOLA ENGLISH TUTORIAL, INC.) **NPC BN 18-131**

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach involving unauthorized access to Google Form responses of the applicants of Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc.) (REA).

Facts

On 20 July 2018, GOLA English Tutorial, Inc. (GOLA) notified the National Privacy Commission (NPC) of a breach involving personal information:

> GOLA hires tutors whose application/s are processed via Google Forms, an external party application.
>
> As a first step of our application process, we require applicants to fill out the online form via Google Forms for information pertinent to their application.
>
> Unfortunately, the privacy setting implemented for the online form allowed all applicants who completed their application to view other tutor applicants' responses.
>
> Once the tutor applicant completed filling out the online form, he /she was redirected to a page which confirmed his/her application and provided for an option to "view other responses." As such, the personal information accomplished by the other tutor applicants became viewable to other tutor applicants by clicking the "view other responses" link.[1]

[1] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc., 27 July 2018, at 1, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).

GOLA explained that one (1) applicant was able to view the personal information of the other applicants.[2] The same applicant notified GOLA about the breach.[3] GOLA reported that there were at least two hundred forty-six (246) applicants affected.[4]

The information involved were the following: complete name, current address, mobile phone number, email address, educational attainment, and name of their school.[5] GOLA's Google Form also asked the applicant whether they had teaching experience and if so, what the name of their previous workplace was, how they found out about GOLA, and whether they were amenable to working full-time.[6]

GOLA reported that it immediately disabled the feature that allowed others to view the applicants' personal information.[7] It also stated that it would individually inform the affected applicants of the breach and the mitigating measures taken through the email address they provided.[8]

On measures to prevent recurrence of the incident, GOLA stated that it would use e-mail instead of an external third party for the tutor-application process.[9] It also stated it would "proceed with appointing a Data Protection Officer and completing [its] registration with the NPC in parallel with the completion of [GOLA's] post-incorporation requirements."[10]

On 14 February 2022, the NPC, through its Complaints and Investigation Division (CID), issued an Order directing GOLA to submit its Post-Breach Report on the incident through e-mail within fifteen (15) days from receipt.[11] The Order, which was sent via email, bounced back. [12]

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.* at 1-2.
[6] *Id.*
[7] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc., 27 July 2018, at 2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Order, 14 February 2022, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2022).
[12] Failed Delivery Email from Microsoft Outlook, 15 February 2022, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2022).

On 15 February 2023, the CID issued another Order directing GOLA, now REA, to submit a Post-Breach Report within five (5) days from receipt.[13]

On 20 February 2023, REA requested for an additional fifteen (15) days, or until 07 March 2023, to file its Post-Breach Report.[14] It clarified that the request was not intended to cause delay, but rather "it foresees its inability to comply with [the Order] within the 5-day period due to the limited mobility of its staff still presented by the COVID-19 pandemic."[15]

On 21 February 2023, the CID issued a Resolution granting REA's request for extension of time:

> In view of the abovementioned circumstances, the Commission deems it proper to afford the PIC an opportunity to comply with the Order dated 15 February 2023. Thus, in line with principle of due process and considering as the granting of such request will not prejudice the conduct of the investigation, we grant the request for extension of time.
>
> WHEREFORE, premises considered, **Rarejob English Assessment, Inc.** (formerly Gola English Tutorial, Inc.) request for an extension of time is hereby **GRANTED. Rarejob English Assessment, Inc.** (formerly Gola English Tutorial, Inc.) is given an additional period of fifteen (15) calendar days from the date of this Order, or until **07 March 2023** to submit its compliance.
>
> **SO ORDERED.**[16]

On 07 March 2023, REA submitted its Compliance.[17] REA reiterated substantially the same narration it provided in its initial notification.

In 2018, REA processed the application of tutors through Google Forms, an external party application.[18] The settings implemented for the Google Form, however, allowed all applicants who completed it to

---

[13] Order, 15 February 2023, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[14] Letter Re: Data Breach Notification filed by Rarejob English Assessment, Inc., 20 February 2023, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2023).
[15] Letter Re: Data Breach Notification filed by Rarejob English Assessment, Inc., 20 February 2023, at 2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2023).
[16] Resolution, 21 February 2023, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[17] Compliance, 07 March 2023, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[18] *Id.* at 1.

view other applicants' responses.[19] On 19 July 2018, one (1) applicant notified REA that "he was able to view the personal information of the other applicants."[20] On 20 July 2018, or the following day, REA sent its Data Breach Notification to the NPC through complaints@privacy.gov.ph.[21] REA also submitted the same to reports@privacy.gov.ph on 23 July 2018.[22] REA reported that "[t]o date, there have been no further complaints or matters arising from [the] incident."[23]

REA explained that it immediately disabled the feature that allowed the applicants to see other responses.[24] REA provided that the settings implemented "allowed only the viewing of data," and as such, "no actions were taken to recover the data."[25] REA added that an investigation was conducted, but that it was "on a purely internal basis and no physical investigation report was prepared."[26]

REA also claimed that it notified the two hundred forty-six (246) affected data subjects of the breach and mitigating measures taken through their respective e-mail addresses.[27] The e-mail notification, however, could no longer be recovered for submission "due to the deletion of the 'gola.com.ph' domain after the corporation changed its name to REA in 2021."[28] It also stated that other than notification, no additional assistance was provided to the affected data subjects "because no data was taken."[29]

To prevent the recurrence of the incident, REA reported that it shifted to the use of email correspondence in the tutor application process rather than using an external party.[30] It allowed "only one person in the relevant department to take charge of the said process."[31] REA also stated that it "called the attention of the relevant employees" and "reinforced the need to be hyper-aware of the Data Privacy Act's

---

[19] *Id.*
[20] *Id.* at 1-2.
[21] *Id.* at 2.
[22] *Id.*
[23] Compliance, 07 March 2023, at 2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[24] *Id.*
[25] *Id.*
[26] *Id.* at 3.
[27] *Id.*
[28] *Id.*
[29] Compliance, 07 March 2023, at 3, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[30] *Id.*
[31] *Id.*

requirements."[32] Finally, it stated that it was still "in the process of appointing a suitable [DPO]."[33]

Issue

Whether the matter falls under mandatory breach notification and whether REA sufficiently addressed the breach 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 (Personal Data Breach Management). Nevertheless, REA sufficiently addressed the breach and implemented security measures to prevent its recurrence.

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.[34]

---

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

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

1. The breach involves sensitive personal information, or information that may, under the circumstances, be used to enable identity fraud;[35]
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.[36]

The first requisite is absent in this case. The nature of the information involved is not sensitive personal information and cannot, under the circumstances, enable identity fraud.

REA admitted that the personal data involved in the breach included, among others, the applicants' educational attainment and the name of their school.[37] Under Section 3 (l) of Republic Act No. 10173 or the Data Privacy Act (DPA), personal information about an individual's education is considered sensitive personal information.[38]

In *RCJ v. DL*, however, the Commission explained that not all information related to education should automatically be considered sensitive personal information:

> In construing Section (3) (l) of the DPA as a whole and considering the company of words in this Section, the information enumerated, which includes "education", may be used to profile an individual. Thus, to harmonize and give effect to the provision as a whole, only information about education which can profile a particular individual falls within the definition of sensitive personal information.
>
> Granular or detailed information relating to the education of an individual can be used to profile that particular individual. For

---

[35] NPC BN 18-158, 13 November 2023, at 10 (NPC 2023) (unreported).
[36] 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 28 May 2024).
[37] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc., 27 July 2018, at 1-2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).
[38] 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).

> instance, transcript of records containing a comprehensive breakdown of a student's grades and other definitive administrative information, such as a student identification number, can be used to personally identify the student.[39]

In that case, the Commission determined that the petitioner's transcript of records, which included a detailed breakdown of his grades, was considered sensitive personal information since the information can profile him.[40] Thus, the processing in relation to the information about his education should be in accordance with Section 13 of the DPA.[41]

Here, the educational attainment and name of the school of REA's applicants are general in nature and cannot be used to profile a particular applicant or enable identity fraud. As such, it cannot be considered as sensitive personal information under Section 3 (l) of the DPA.

Further, the applicants' personal information—their name, address, mobile phone number, and name of their previous workplace—cannot be considered as other information that may, under the circumstances, be used to enable identity fraud.[42]

The first requisite of mandatory breach notification should be read together with Section 20 (f) of the DPA. Section 20 (f) expressly requires the consideration of the specific circumstances of a breach in determining whether other information involved in the breach 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

---

[39] RCJ v. DL, NPC BN 22-012, 10 November 2022, at 7, *available at* https://privacy.gov.ph/wp-content/uploads/2023/08/NPC-22-012-2022.11.10-RJC-v.-DL-Decision.pdf (last accessed 28 May 2024).
[40] *Id.* at 8.
[41] *Id.*
[42] NPC Circ. No. 16-03, § 11.

> 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.[43]

While the Commission previously held that a data subject's name and email may be considered under "other information that may enable identity fraud,"[44] that decision took into consideration the unique circumstances of the case. 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 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.**[45]

In that case, the Commission, after considering the circumstances, determined that the names and email addresses of the data subjects are information that may be used to enable identity fraud.[46] The PIC reported that a hacker accessed and implanted ransomware in an online database.[47] Because of these circumstances, the Commission concluded that the hacker may contact and send malicious emails directly to the data subjects.[48]

---

[43] Data Privacy Act of 2012, § 20 (f). Emphasis supplied.
[44] NPC BN 20-124, 10 September 2020, at 3 (NPC 2020) (unreported).
[45] *Id*. Emphasis supplied.
[46] *Id.* at 4.
[47] *Id.*
[48] *Id.*

Here, the disclosure of the applicants' information would not have enabled identity fraud.

The applicant was able to view the other responses due to REA's inadvertent failure to turn off the "view other responses" function.[49] There is no showing that the applicant who notified REA deliberately intended to obtain the other applicants' information, as he was the one who reported the incident to REA.[50] Further, REA noted in its Post-Breach Report that "[t]o date, there have been no further complaints or matters arising from [the] incident."[51] Given the specific circumstances of the matter, the personal information involved could not have been used to commit identity fraud. As such, the personal information of the data subjects cannot be considered as other information that, under the circumstances, may enable identity fraud.

The second requisite is present in this case. There was acquisition of the information by an unauthorized person.

The Commission previously 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."[52]

REA admitted in its Post-Breach Report that one (1) applicant notified REA that "he was able to view the personal information of the other applicants."[53] This shows that there is not just a reasonable belief but certainty that an unauthorized person acquired the information involved in the breach.[54]

The third requisite is also absent. There is no real risk of serious harm in this case.

---

[49] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc., 27 July 2018, at 1, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).
[50] Compliance, 07 March 2023, at 1-2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[51] *Id.* at 2.
[52] In re: Batangas Bay Carriers, Inc., NPC BN 20-157, 21 September 2020, at 5, *available at* https://www.privacy.gov.ph/wp-content/uploads/2022/01/Resolution-NPC-BN-20-157-In-re-Batangas-Bay_Sep-21.pdf (last accessed 11 July 2024).
[53] Compliance, 07 March 2023, at 1-2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[54] In re: Batangas Bay Carriers, Inc., NPC BN 20-157, at 5.

The Commission takes this opportunity to discuss the factors considered in determining 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.[55]

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.[56] The risk must be apparent and not the product of mere speculation.[57] Serious harm means that the consequences and effects to any affected data subject are significant based on the surrounding circumstances of the breach.[58]

In determining whether the unauthorized acquisition is likely to give rise to a 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.[59]

In this case, as previously established, the unauthorized acquisition was due to REA's inadvertent failure to turn off the "view other responses" function.[60] There is no showing that the tutor-applicant who notified REA deliberately intended to obtain the other applicants'

---

[55] NPC Circ. No. 16-03, § 11.
[56] 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/2024/05/NPC-BN-17-028-_-NPC-BN-18-180-2023.05.11-In-re-Easytrip-Reso-Final.pdf (last accessed 28 May 2024).
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly, GOLA English Tutorial, Inc., 27 July 2018, at 1, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).

information, as he even reported it to REA.[61] Thus, the objective of the unauthorized acquisition was not for malicious or fraudulent purposes. Further, REA reported that it immediately disabled the feature that allowed the personal information of the applicants to be viewed by others.[62] As such, further exposure or misuse of the information is unlikely.

Finally, Section 20 of the DPA provides that Personal Information Controllers (PICs) must implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any unlawful disclosure:

> Section 20. *Security of Personal Information*. (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[63]

In this case, REA implemented sufficient security measures on the information to address the breach and prevent its recurrence. REA reported that it shifted to the use of email correspondence in the tutor application process rather than using an external party application like Google forms.[64] Further, it designated only one person to take charge of the new email application process.[65] REA also reminded its employees and "reinforced the need to be hyper-aware of the Data Privacy Act's requirements."[66]

Given the foregoing factors, the unauthorized acquisition did not give rise to a real risk of serious harm to any affected data subject. Thus, the third requisite is absent.

Considering that the first and third requisites are absent, the matter does not fall under mandatory breach notification. Nevertheless, REA conducted proper breach management, including the implementation of reasonable and appropriate security measures. The measures

---

[61] Compliance, 07 March 2023, at 1-2, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[62] Personal Data Breach Notification from Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc., 27 July 2018, at 2, *in* In re: Rarejob English Assessment, Inc., NPC BN 18-131 (NPC 2018).
[63] Data Privacy Act of 2012, § 20 (a).
[64] Compliance, 07 March 2023, at 3, *in* In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.), NPC BN 18-131 (NPC 2023).
[65] *Id.*
[66] *Id.*

implemented by REA are sufficient to address the breach and to prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-131 In re: Rarejob English Assessment, Inc. (formerly GOLA English Tutorial, Inc.) is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
16 May 2024.

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:

PVO
Representative
Rarejob English Assessment, Inc.

AOT
Counsel for Rarejob English Assessment, Inc.
De Guzman San Diego Mejia & Hernandez Law Offices (GSMH Law)

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