IN RE: GC, INC.
FORCED LOGOUT **CID 18-J-162**
x----------x

ORDER

LIBORO, P.C.:

Before this Commission is the Data Breach Notification Report[1](DBNR) submitted by GC, Inc. (GC), through M.K., for and on behalf of GC. The DBNR is submitted in compliance with the Order issued by the Commission dated 17 October 2018.

Facts

On 17 October 2018, this Commission issued an Order to GC containing the following dispositive portion, *to wit*:

> **WHEREFORE, PREMISES CONSIDERED**, this Commission hereby **ORDERS** GC to:
>
> 1. **SUBMIT** a more comprehensive Data Breach Notification Report to this Commission following rules laid down in NPC Circular No. 16-03;
> 2. **NOTIFY** the affected data subjects through an appropriate Data Breach Notification following rules laid down in NPC Circular No. 16-03;
> 3. **PROVIDE** identity theft and phishing insurance for affected Filipino data subjects, or in the alternative, **ESTABLISH** a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning GC, located in the Philippines and with a local number, within six (6) months from receipt of the **ORDER**
> 4. **IMPLEMENT** a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing; and
> 5. **PROVIDE** evidence of compliance with the foregoing.

[1] Data Breach Notification Report of GC dated 16 November 2018.

On 16 November 2018, acting on the aforesaid Order, a letter[2] was submitted and was signed by M.K. for and on behalf of GC. The letter further discussed the communication and notification it made with the Filipino users, the steps already taken and further steps planned to take, the help services it provided, the educational campaign initiatives on issues of digital literacy, safety and privacy, and the evidence of compliance with the Order of this Commission.

On 29 September 2018, GC started sending a notification to all potentially affected Filipino users via an in-app important security update. This message set out an explanation of incident as understood by GC in its initial investigation, informed users that GC had contacted law enforcement, and explained the reasons and impact of GC's remedial step of resetting all potentially affected access tokens. This security update was also posted in the GC newsroom. GC also informed affected users of the steps they can take in relation to phishing and how to protect themselves from an attacker.

Starting 13 October 2018, GC updated the smaller subset of users who were found to be affected by the incident. It was done by way of tailored in-app notification that was written in both English and Tagalog. The Tagalog notification were sent to those Filipino users whose GC language was set to Tagalog on 17 October 2020. The in-app notification varied depending on the categories of information about the user that were potentially assessed during the attack. This was explained in the 'update' under the heading 'Personal data Potentially Involved'. Users fell into three (3) different groups and received different in-app notifications accordingly. This also explained what information the attackers were believed to have accessed in relation to such users. The notification also included hyperlinks to tailored Help Center pages where the affected users could find further details about the incident, updates about GC's investigation regarding the incident, and guidance on steps which the user could take to protect themselves from suspicious emails, text messages, or phone calls.

According to GC, if the users have further questions pertaining to the incident, users are invited to follow a link from the Help Center to the GC Security Incident Response Form, through which they are able to submit questions to GC. Those who will submit question to GC will

[2] *Ibid.*

receive an email to which they can reply with any inquiry in their preferred language.

GC stated that it informed the affected data subjects regarding the steps they can take in relation to phishing and other matters. These are provided at the bottom of the tailored Help Center notices and link to pages dedicated for educating users in this regard. In addition to this, GC also provided information about phishing to users affected by the incident. The 'How could the attackers use this information and what can I do to protect myself' part of the tailored Help Center page contains a link to a Help Center page 'Learn more about phishing' that educates users on what phishing is as well as informing them of they may do to avoid getting phished and what they can do if they have been phished on GC.

GC also provided additional resources to assist and educate users and to allow users to report issues to GC or to contact them directly. It also provided other methods of contact available for Filipino users in relation to the aforesaid matters include, but not limited to the following:

1. Email address for phishing. GC is offering an email address from that which the people can report issues.
2. Reporting violations of Community Standards. Users may report messages, posts, and other content for violation of GC's Community Standards.
3. Data conduct form and email alias where people can contact GC with questions about its data policy through a contact form and will receive a response by email. If they have further questions users can reply to that email in a language of their choice.

GC's Help Center content, account setting pages as well as the Support Inbox contents are also available in Tagalog language. GC employed Filipino Tagalog speakers to ensure that it can continue to be responsive to its Tagalog speaking employee who supports Philippines user concerns regarding the violation of its Community Standards.

GC also participated in numerous initiatives of digital literacy, safety, privacy, and critical thinking online. Currently, GC is developing an #IAMDIGITAL campaign, aimed at encouraging responsible digital citizenship. The content will further include phishing and span education. Moreover, GC also have other current and upcoming initiatives aimed at Filipino users to increase awareness about digital literacy *to wit:* Overseas Workers Welfare, Cyber Safety for Teachers, Digital Youth Summit, Cybersecurity Caravan, NPC Privacy, Safety, Security and Trust Campaign, and Tailored Briefings on GC Products and Services.

Issues

i. Whether the National Privacy Commission has jurisdiction over the alleged data breach incident.

ii. Whether GC, Inc. submitted a comprehensive Data Breach Notification Report that follows the rules laid down in NPC Circular No. 16-03.

iii. Whether GC notified the affected data subjects through an appropriate Data Breach Notification following the rules laid down in NPC Circular 16-03.

iv. Whether GC established a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning GC in pursuant to the Order dated 17 October 2018 of this Commission.

v. Whether GC implemented a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing in pursuant to the Order dated 17 October 2018 of this Commission.

vi. Whether GC provided sufficient evidence of compliance.

Discussion

National Privacy Commission has jurisdiction over the alleged data breach incident.

The National Privacy Commission is an independent body mandated to administer and implement the Data Privacy Act of 2012 (DPA), and to monitor and ensure compliance of the country with international standards set for data protection[3]. Section 7 (a) and (d) of the DPA specifically provides that the NPC is mandated to ensure compliance of personal information controllers with the provisions of the act and compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy, respectively.

Corollary to the foregoing, Section 6 of the DPA explicitly provides for the extraterritorial application of the DPA *to wit*:

> SEC. 6. *Extraterritorial Application*. – This Act **applies to an act done or practice engaged in and outside of the Philippines** by an entity if:
>
> (a) **The act, practice or processing relates to personal information about a Philippine citizen or a resident;**
>
> (b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:
>
> (1) A contract is entered in the Philippines;
>
> (2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and
>
> (3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and
>
> (c) The entity has other links in the Philippines such as, but not limited to:
>
> (1) The entity carries on business in the Philippines; and
>
> (2) The personal information was collected or held by an entity in the Philippines.

[3]Data Privacy Act, Sec. 7(2012)

Following the *Extraterritorial Application* provided by the Section 6 of the DPA, the processing of personal information of GC as personal information controller clearly falls within the mandate and jurisdiction of this Commission. Moreover, the Order issued by this Commission is within the ambit of its power and function, thus valid and enforceable against GC.

GC, Inc. submitted a comprehensive Data Breach Notification Report that follows the rules laid down in NPC Circular No. 16-03.

This Commission, upon carefully reviewing the Data Breach Notification Report submitted by GC, finds that GC has complied with the requirements laid down in NPC Circular No. 16-03.

Section 17 of the NPC Circular 16-03[4] provides that the Notification shall include, but not be limited to:

1. Nature of the Breach
   a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
   b. a chronology of the events leading up to the loss of control over the personal data;
   c. approximate number of data subjects or records involved;
   d. description or nature of the personal data breach;
   e. description of the likely consequences of the personal data breach; and
   f. name and contact details of the data protection officer or any other accountable persons.
2. Personal Data Possibly Involved
   a. description of sensitive personal information involved; and
   b. description of other information involved that may be used to enable identity fraud.
3. Measures Taken to Address the Breach
   a. description of the measures taken or proposed to be taken to address the breach;
   b. actions being taken to secure or recover the personal data that were compromised;

[4] Personal Data Breach Management, NPC Circular 16-03 (2016)

c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.

In this case, the contents of the update provided by GC to the Commission dated 13 October 2018 sufficiently complied with the rules laid down in NPC Circular No. 16-03 in relation to Section 17 of the aforesaid. The aforesaid Data Breach Notification Report and the updates submitted by GC already contains the (1) Nature of the breach; (2) Personal data possibly involved; and (3) Measures taken to address the incident.

It is also worth noting that GC, in recognition of the mandate of this Commission, voluntarily informed this Commission pertaining to the breach incident dated 29 September 2019.

GC notified the affected data subjects through an appropriate Data Breach Notification that follows the rules laid down in NPC Circular 16-03.

In the letter submitted by GC dated 16 November 2018, it is stated therein that starting 29 September 2018, GC sent notification to all potentially affected Filipino users via in-app important security update. The message contained the explanation of the incident as understood by GC in its initial investigation, informed the users that GC had contacted law enforcement, and explained the reasons and impact of its remedial step of resetting all potentially affected tokens which was also posted in the GC newsroom.

On 13 October 2018, GC started updating the smaller subset of users who the investigation showed that were affected by the incident by way of tailored in-app notification which as communicated in English

and Tagalog. Tagalog notification were sent to those affected Filipino users whose GC language was set to Tagalog on 17 October 2018.

As a proof of notification, GC, also attached the sample notifications it provided to the affected data subjects.[5]

Therefore, this Commission finds that GC notified the affected data subjects through an appropriate Data Breach Notification following the rules laid down in NPC Circular 16-03.

GC established a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning GC in pursuant to the Order dated 17 October 2018 of this Commission.

The notification made by GC includes hyperlinks to tailored Help Center pages where the affected users could find further details about the incident, updates about GC's investigation regarding the incident, and guidance on steps which the user could take to protect themselves from suspicious emails, text messages, or phone calls. If the users have further questions pertaining to the incident, users are invited to follow a link from the Help Center to the GC Security Incident Response Form, through which they can submit questions to GC. Those who will submit question to GC will receive an email to which they can reply with any inquiry in their preferred language.

Moreover, GC provided additional resources to assist and educate users and to allow users to report issues to GC or to contact them directly. It also provides other methods of contact available for Filipino users in relation to the aforesaid matters include, but not limited to the following:

1. Security Incident Response Form. This is where Filipino users can contact GC in respect to the aforesaid incident.
2. Email address for phishing. GC is offering an email address from that which the people can report issues.

[5] See CID 18-J-162 Case Files at pp. 9 to pp. 15

3. Reporting violations of Community Standards. Users may report messages, posts, and other content for violation of GC's Community Standards.
4. Data conduct form and email alias where people can contact GC with questions about its data policy through a contact form and will receive a response by email. If they have further questions users can reply to that email in a language of their choice.

The Help Center may not be physically located in the Philippines, but this Commission finds that the efforts of GC, as well as the designation of its GC Philippines Head for Public Policy to oversee privacy related matters, sufficiently satisfied the Order dated 17 October 2018 of this Commission.

GC implemented a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing in pursuant to the Order dated 17 October 2018 of this Commission.

GC, through the notification it made, informed the affected data subjects regarding the steps they can take in relation to phishing and other matters. These are provided at the bottom of the tailored Help Center notices and link to pages dedicated for educating users in this regard. In addition to this, GC also provided information about phishing to users affected by the incident. The 'How could the attackers use this information and what can I do to protect myself' part of the tailored Help Center page contains a link to a Help Center page 'Learn more about phishing' that educates users on what phishing is as well as informing them of they may do to avoid getting phished and what they can do if they have been phished on GC.

Moreover, GC also participated in numerous initiatives of digital literacy, safety, privacy, and critical thinking online. Currently, GC is developing an #IAMDIGITAL campaign, aimed at encouraging responsible digital citizenship. The content will further include phishing and span education. GC also have other current and

upcoming initiatives aimed at Filipino users to increase awareness about digital literacy *to wit:* Overseas Workers Welfare, Cyber Safety for Teachers, Digital Youth Summit, Cybersecurity Caravan, NPC Privacy, Safety, Security and Trust Campaign, and Tailored Briefings on GC Products and Services.

Considering the foregoing, this Commission finds that GC implemented a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness in identity theft and phishing.

GC provided sufficient evidence of compliance.

After thorough review of the submitted documents and adjudication of this case, this Commission finds that GC sufficiently provided proof of its compliance to the Order dated 17 October 2018.

WHEREFORE, all premises considered, the Commission resolves that the matter CID 18-J-162 - "In Re: GC, Inc. Forced Logout "is hereby considered **CLOSED**.

SO ORDERED.

Pasay City, Philippines;
19 November 2020.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

(Sgd.)
LEANDRO ANGELO Y. AGUIRE
Deputy Privacy Commissioner

(Sgd.)
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

Copy furnished:

M.K.
Representative of the PIC
GC, Inc.
Attn: Privacy Operations,
xxxxxxxxx
xxxxxxxxx

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