IN RE: COSTA CROCIERE S.p.A. **NPC BN 21-185**

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

RESOLUTION

NAGA, *D. P.C.;*

Before the Commission is a Breach Notification filed by Costa Crociere S.p.A. (Costa) with a request for exemption from individual data subject notification dated 09 September 2021.

Facts

On 25 December 2020, Costa detected an unauthorized third-party access to portions of its information technology (IT) systems and the IT systems of its subsidiaries, AIDA Cruises (Aida), AIDA Kundencenter GmbH, and Carnival Maritime GmbH.[1]

According to Costa, the Costa Cruises domain (Costa Network) and Aida Cruises domain (Aida Network) are on separate but connected networks. Based on a comprehensive analysis of the available logs and artifacts, they believe that the event began via multiple malicious Excel document(s), sent via email, containing SDBot remote access tooling which was opened by employees at Aida.[2]

Costa stated that on 21 December 2020, the threat actor was able to use their access to the Aida Network to gain access to the Costa Network. On the succeeding days, the threat actor gradually exfiltrated approximately 329 GB of data then 719 GB of data using the Rclone tool.[3]

[1] Costa Crociere S.p.A Data Breach Notification dated 09 September 2021
[2] Id. at page 2.
[3] 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

On 24 December 2020, the threat actor disabled both the Costa anti-virus software, TrendMicro and Aida anti-virus software, Windows Defender. The threat actor then launched DoppelPaymer ransomware onto the Costa Network and the Aida Network. Such activity was detected by Costa at CET 00:21 a.m. on 25 December 2020.[4]

The unauthorized access was used to launch a malware that encrypted a number of IT systems. The unauthorized persons then demanded a ransom from Costa to restore access to those systems. Further, the unauthorized persons exfiltrated approximately 1.1 TB of unstructured data from Costa and its subsidiaries' domains.

Costa, its subsidiaries, and their IT systems are all located outside of the Philippines.

In terms of the security measures Costa implemented to address the breach, it stated that it shut down the intrusion, restored operations, performed measures to prevent further unauthorized access to other parts of its IT systems, and will conduct a technical and forensic investigation.

Further, Costa also stated that it informed and notified following authorities:

1. Italian Data Protection Authority, Garante per la protezione dei dati personali (Garante) as the lead supervisory authority in the European Economic Area (EEA);
2. Italian Ministero delle Infrastrutture e dei Trasporti (MIT) and CSIRT Italia (CSIRT) of in accordance with the Costa's obligations as a designated Operator of Essential Services (OES) under the Italian NIS Directive and Legislative Decree no. 65/2018;
3. Polizia Postale e delle Comunicazioni (Polizia Postale) on 12 January 2021;

[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

4. State Commissioner for Data Protection and Freedom of Information of Mecklenburg-Vorpommern and the Hamburg Commissioner for Data Protection and Freedom of Information in Germany due to the involvement of AIDA Cruises; and
5. German law enforcement authorities where it have cooperated with their investigation.[5]

Moreover, Costa stated that at the time the reports were submitted to the Garante and other Italian and German authorities, it was not aware that Filipino data subjects were affected by the breach. It was only recently that Costa determined the possibility that the unauthorized persons who accessed its IT systems may have been able to access limited amount of personal data relating to approximately seventy-four thousand (74,000) Filipino data subjects.

The Filipino data subjects are either guests of Costa's cruise lines or its employees or crew members. The personal data that may have been possibly affected by the breach includes name, date of birth, passport number, nationality, and cruise trip information.

With this, Costa stated that it has been conducting comprehensive dark web monitoring to mitigate any harm that the said breach may cause to the data subjects.[6] According to Costa, no evidence suggests that the data has been made available for sale or misused. Hence, it believes that the breach has a low risk of harm to the Filipino data subjects.

Additionally, Costa stated that it is regularly reviewing its security and privacy policies and procedures. It is also implementing changes when needed to enhance its information security and privacy program and controls and to prevent a recurrence of any incident similar to the breach.

Further, Costa has administrative and technical measures in place to further secure personal data such as: global identity standardization and synchronization; improvement of key security tools, such as

[5] Id. at page 1 to 2.
[6] Id. at page 2 to 3.

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

Carbon Black, and antivirus solutions; implemented firewall rule adjustments and governance; and optimized alert logging process to allow for earlier detection and remediation. It also has a suite of data protection programs, trainings, and several online training courses focused on cybersecurity and privacy.[7]

Costa stated that it already published the notices regarding the breach on its websites beginning March 2021 in the languages most commonly served by Costa and its subsidiaries, namely on its Italian, French, Spanish, Brazilian, Chinese and Japanese websites. Further, Aida also published notifications on its website. Each notice contained an email address, to enable any individual who had any question or concerns regarding the breach to communicate directly with the company's privacy team.[8]

With the measures undertaken to address the breach and protect the information of its data subjects, and the fact that to its knowledge no data subject has filed a complaint in connection with the breach, Costa then respectfully requests that it be exempted from sending individual notification to data subjects.[9]

Discussion

This Commission finds that the case falls under the mandatory breach notification requirement and the notification of the affected data subjects is necessary in order to protect them from the risk of serious harm. Section 11 of the NPC Circular No. 16-03 (Personal Data Breach Management) 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:

[7] Id at page 3.
[8] Id.
[9] 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

A. The personal data involves **sensitive personal information or any other information that may be used to enable identity fraud**.
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.[10] (Emphasis Supplied)

Moreover, Section 13 of the same Circular states:

> **SECTION 13.** ***Determination of the Need to Notify.*** Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred. The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:
>
> A. Information that would likely affect national security, public safety, public order, or public health;
> B. **At least one hundred (100) individuals;**
> C. **Information required by applicable laws or rules to be confidential**; or
> D. Personal data of vulnerable groups.[11] (Emphasis supplied)

In Costa's initial breach notification, it stated that the total number of affected Filipino data subjects is approximately seventy-four thousand (74,000). Further, the breach involves both personal information and sensitive personal information including name, date of birth, passport number, nationality, and cruise trip information.[12]

Considering that the breach involves more than one hundred (100) individuals and includes sensitive personal information, the incident herein is covered by the mandatory breach notification rule. This

[10] Section 11 of the NPC Circular No. 16-03.
[11] Section 13 of the NPC Circular 16-03.
[12] Costa Crociere S.p.A Data Breach Notification dated 09 September 2021 at page 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

Commission reiterates the importance of the obligation of Personal Information Controllers (PICs) to notify to the affected data subjects in cases of breach that falls under the mandatory notification rule.

This Commission emphasizes that the notification to the affected data subjects is fundamental in order to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.[13]

This Commission also recognizes that Costa's request for exemption from individual notification of the affected data subjects is based on its report that it already published the notices regarding the breach on its websites. However, it must be emphasized that it only published the notices on its Italian, French, Spanish, Brazilian, Chinese and Japanese websites. With this, the affected Filipino data subjects may not be fully informed of the breach since it is not in the language commonly known to Filipinos, such as English or Filipino.

In view of the foregoing, this Commission deems the notification to the affected data subjects as urgent and necessary while also taking into consideration the number of the affected data subjects and the disproportionate effort that Costa may have to undertake in order to notify them.

Section 18(D) of NPC Circular No. 16-03 provides that, where individual notification is not possible or would require a disproportionate effort, the PIC may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner.[14] Accordingly, Section 4(c), Rule XI of the 2021 NPC Rules of Procedure, for the Commission to grant the use of alternative means of notification, a request has to be made by the PIC.[15]

However, in this case, considering the large number of the affected data subjects and the urgency to notify them, the Commission orders

[13] Section 18(A) of the NPC Circular 16-03.
[14] Section 18(D) of the NPC Circular No. 16-03
[15] Section 4(c), Rule XI of the NPC Circular No. 2021-01

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

Costa to use alternative modes of notification for a portion of the affected data subjects to enable Costa to comply with the orders of the Commission. For the affected data subjects with e-mail addresses, Costa shall individually notify them through e-mail. As for the affected data subjects without e-mail addresses, Costa shall notify the affected data subjects through publication in a newspaper of general circulation in the Philippines.

This Commission also notes that Costa anchored its request on the security measures it has implemented to address the breach and prevent its reoccurrence. However, Costa failed to include any proof of such security measures it implemented to address the breach and ensure that the risk of harm or negative consequence to the data subjects will not materialize as indicated in its initial breach notification.

In addition, the Commission has yet to receive the Full Breach Report from Costa. The Commission finds that Costa failed to provide within five (5) days from the initial report the Full Breach Report[16] that contains the complete and necessary information as prescribed under Section 9 and Section 17(D) of the NPC Circular No. 16-03.

WHEREFORE, premises considered, this Commission resolves that the request for exemption from individual data subject notification filed by Costa Crociere S.p.A is hereby **DENIED**.

Costa Crociere S.p.A is hereby **ORDERED** to comply with the following **within ten (10) days** from receipt of this Resolution:

1. **NOTIFY** the affected data subjects. The affected data subjects with e-mail addresses shall be notified pursuant to Section 18 of the NPC Circular No. 16-03. The notification shall be done individually using secure means of communication, through e-mail. Costa shall submit proof of compliance, including the proof of receipt of the data subjects of such notification.

[16] Section 17(C) of the NPC Circular No. 16-03

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

The affected data subjects without e-mail addresses shall be notified through alternative means pursuant to Section 18(D) of the NPC Circular No. 16-03, through publication in a newspaper of general circulation in the Philippines. Costa shall also provide proof of compliance, including proof of notification / publication

2. **SUBMIT** its Full Breach Report pursuant to Section 9 and Section 17(D) of the NPC Circular No. 16-03;

3. **SUBMIT** proof of the security measures Costa implemented to address the breach; and

4. **SHOW CAUSE** in writing why it should not be subjected to contempt proceedings, as permitted by law, before the appropriate court, and other actions as may be available to the Commission, for its failure to submit its Full Breach Report within the required period.

SO ORDERED.

City of Pasay, Philippines.
23 September 2021.

SGD.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

SGD.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

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

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

CP
General Counsel

KB

COMPLIANCE AND MONITORING 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