Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: HENNES & MAURITZ

Initiated as an Independent NPC Investigation into the Possible Data Privacy Violations Committed by the Hennes & Mauritz.

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

NPC BN 18-223
(Formerly CID BN 18-223)

RESOLUTION

LIBORO, *P.C.:*

Before this Commission is the Compliance submitted by Hennes & Mauritz (H&M) with the Commission's directive stated in the Resolution dated 15 April 2021.

Facts

On 15 April 2021, this Commission issued a Resolution with the following dispositive portion:

> **WHEREFORE**, premises considered, this Commission resolves to give Hennes & Mauritz a period of thirty (30) days from receipt of this Resolution to EXPLAIN its failure to report and notify the Commission and the data subject within the required periods under NPC Circular No. 16-03.

The Resolution dated April 15 was received by H&M on 07 May 2021, in the aforesaid Resolution, the Commission determined that H&M failed to comply with the notification requirements pursuant to NPC Circular No. 16- 03 on Personal Data Breach Management. Particularly, H&M failed to promptly notify this Commission within seventy-two (72)-hours about the data breach from the time it figured out the incident on 14 November 2018, when the credit cards owner came back to the store and reported the incident.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

In its letter dated 19 May 2021, H&M stated that they were unable to confirm or even have a reasonable belief that a personal data breach has occurred until a thorough investigation was conducted and completed according to the company's standard operating procedure.

Furthermore, H&M alleged that without due process, there could be many other potential and reasonable causes behind the unknown transactions and therefore may not be linked to an occurrence of data breach stemmed from the lost card found in its store.

Therefore, H&M also argued that the seventy-two (72) hour period shall apply from the time H&M concluded its investigation and not from the time the customer informed them about the incident.

Discussion

This Commission, upon reviewing the breach report and explanation submitted by H&M, finds that H&M has complied with the directive in the previous Resolution dated 15 April 2021 of the Commission and consider this matter closed.

However, this Commission would like to reiterate that Section 11 of the NPC Circular No. 16-03 provides for the requirements of notification to this Commission and to the affected data subjects regarding the existence of a data breach, *to wit:*

> 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.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> 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.

Corollary to this, Section 17 of the same Circular 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 personal data breach has occurred.
>
> xxx
>
> C. *When delay is prohibited.* There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless the personal information controller is granted additional time by the Commission to comply.

This Commission would like to note that the counting of the seventy-two (72) hours shall be reckoned from the time the breach itself was made known to H&M. It must be noted that the breach was made known to H&M when the credit card owner came back to the store and reported the incident on 14 November 2018, a day after the breach occurred. H&M only submitted its report to its HR on 20 November 2018, and to this Commission on 28 November 2018, fourteen (14) days after the incident ensued.

It must be pointed out that the manager on duty discovered said credit card in the drawer on the night of 13 November 2018 and just recorded the same on their Lost and Found register before finally storing it in their safe/vault for security. It is understandable that any supposed subsequent actions to find and contact the data subject the next day might have been preempted by the card owner herself who went back

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

to the store on 14 November 2018, nevertheless, H&M should have still reported the breach to this Commission as part of the obligations as a PIC.

It is also worth noting that records show that the H&M concluded its investigation on 20 November 2018 but still belatedly notified the Commission on 28 November 2018.

At this juncture, this Commission wants to emphasize that in case of a mandatory data breach , Personal Information Controllers (PICs) have the obligation to notify the Commission and the affected data subject within the periods mandated under NPC Circular No. 16-03.

This Commission would like to note that H&M was able to demonstrate that it implemented reasonable and appropriate security measures to uphold data privacy and protection.

H&M undertook the following measures to address the data breach incident:

1. The Store Management and its Security Department investigated the facts and circumstances surrounding the incident.

2. After the completion of the investigation report, H&M through its Human Resource Department (HR) issued a Notice to Explain (NTE) letter to N.A. and M.D. to hear each side of their story.

3. Final Written Warning was served to N.A. due to neglect of duty, while dismissal from service was also served to M.D. grounded in an unauthorized taking of credit card's information for the purpose of removing funds from it.

Moreover, H&M was able to investigate and determine the circumstances of the data breach using its CCTV recordings. H&M also immediately imposed a penalty to both erring employees. A Final Written Warning was issued against the erring employee and grounded on his failure to return the credit card to the customer while on the other hand, dismissal of service was served against the other

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

erring employee for just cause, grounded on the unauthorized taking of credit card information and for the violation of company's Code of Conduct.

In view of the foregoing, it is therefore recognized that the security measures undertaken by H&M were sufficient in addressing the subject breach.

WHEREFORE, premises considered, this Commission **NOTES** the explanation given by Hennes & Mauritz as to its failure to report and notify the Commission and the data subject within the required periods under NPC Circular No. 16-03.

Further, this Commission resolves that the matter NPC BN 18-223 – "In re: Hennes & Mauritz" is hereby considered **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
01 June 2021.

(Sgd.)
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

WE CONCUR:

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

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

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

Copy furnished:

A.G.Z.
Data Protection Officer
H&M Hennes & Mauritz Inc.

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 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228