IN RE: HC CONSUMER FINANCE PHILIPPINES, INC.

NPC BN 18-029

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

RESOLUTION

AGUIRRE, *D.P.C.;*

Before the Commission is a breach notification submitted by HC Consumer Finance Philippines, Inc. (HCPH) involving a missing laptop from its Point-of-Sale (POS) terminal.

Facts

On 02 March 2018, HCPH notified the National Privacy Commission (NPC) of a breach:

> Pursuant to the requirement of NPC Circular 16-03 which requires personal information controllers to notify the National Privacy Commission (Commission) within seventy-two (72) hours upon knowledge of or reasonable belief by the Personal Information Controller or Personal Information Processer [sic] that a personal data breach has occurred, HC Consumer Finance Philippines, Inc. (HCPH) hereby submits the following breach notification:
>
> 1. Data Breach Notification 2018-001 Stolen Laptop[1]

In its data breach notification, HCPH informed the NPC that the breach involves a "stolen laptop resulting to possible unauthorized disclosure of or access to personal data contained in the equipment."[2] According to HCPH, on 14 February 2018, its security department received an incident report from District Sales Manager MJE regarding

[1] Email, 02 March 2018, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[2] Data Breach Notification, 01 March 2018, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).

the stolen laptop.[3] HCPH added that on 16 February 2018, its security department investigated and identified the circumstances surrounding the theft of the laptop.[4] On 22 February 2018, HCPH's IT Department received a report about the stolen laptop.[5] The IT Department verified that the stolen laptop was connected to the Puppet Server on 21 February 2018 at 4:20 p.m.[6] It deployed a script to wipe the data and files in the stolen laptop and to reformat the laptop the next time it connects to the internet.[7] On 27 February 2018, HCPH's Data Protection Officer (DPO) was notified of the incident.[8]

HCPH reported that the breach possibly affected three hundred ninety-five (395) data subjects.[9] According to HCPH, the breach involves its customers' names, dates of birth, home addresses, permanent addresses, email addresses, landline numbers, mobile numbers, identification document numbers and copies of identification documents.[10]

To address the breach, HCPH subjected the sales associate in charge of the stolen laptop to disciplinary action.[11] HCPH also conducted an investigation through its Security Department and identified the customers whose information was processed through the stolen laptop.[12] To mitigate possible harm to the data subjects, HCPH deployed a script to wipe the laptop data once the laptop is connected to the internet.[13] HCPH also initiated an account password reset for all Sales Associates assigned to POS terminals.[14]

HCPH also took measures to prevent the recurrence of the incident. It deployed a script to periodically wipe data and files every 10:00 p.m. on POS issued laptops.[15] HCPH implemented this measure on a company-wide basis beginning 23 February 2018.[16] HCPH also streamlined the process for identifying and reporting stolen or lost

---

[3] *Id.* at 3.
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] Data Breach Notification, 01 March 2018, at 4, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] Data Breach Notification, 01 March 2018, at 4, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[15] *Id.*
[16] *Id.*

laptops.[17] It also raised an IT ticket for the enhancement of access control and to secure log files.[18]

To assist the data subjects who may have been negatively affected by the breach, HCPH engaged its Security Department and Anti-Fraud Team of its Risk Department to monitor and resolve any potential harm caused by the data breach.[19]

HCPH also applied for exemption from data subject notification:

> In addition, HCPH would like to apply for an exemptive relief of the requirement of Section 38(c) of the Implementing Rules and Regulations (IRR) which states that the Personal Information Controller (PIC) shall notify the affected data subjects within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the PIC that a personal data breach requiring notification has occurred. Our request is based on the following premises:
>
> 1. Immediately after the breach, HCPH has applied appropriate technical and organization measures to protect the personal data and to ensure that high risk posed to data subjects is no longer likely to materialize. Actions taken are as follows:
>   a. Deployed a script to wipe data/files the next time the stolen laptop connects to the internet and it will be reformatted automatically; and
>   b. Initiated account password reset for all Sales Associates assigned to Point-of-Sale terminals.
>
> 2. It would involve disproportionate effort to identify the number of affected individuals.
>
> Based on the foregoing premises, it is deemed by HCPH that notification to data subjects is no longer necessary given that appropriate measures had already been instituted to prevent adverse impact on our customers and there is no reasonable degree of certainty that the thief had accessed(sic) to data/files in the stolen laptop.[20]

[17] *Id.*
[18] *Id.*
[19] *Id.* at 5.
[20] Email, 02 March 2018, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).

On 17 March 2022, the Complaints and Investigations Division (CID) of the NPC directed HCPH to submit a post-breach report containing proper documentation on the actions it took to address the breach.[21]

On 18 April 2022, HCPH submitted its Post-Breach Report.[22] In its Post-Breach Report, HCPH discussed the nature and summary of the breach, the measures it took to address and mitigate the consequences of the breach, the outcome of the breach management, and the assistance it provided to affected data subjects.[23]

On 23 March 2023, the CID directed HCPH to submit proof to support its Post-Breach Report.[24] Specifically, the CID required HCPH to furnish the following information or documentation:

1. Proof of any subsequent connections made by the laptop to the network after the connection to the Puppet Server on 21 February 2018;
2. Proof of Deletion/Wipeout of the data contained in the missing laptop;
3. Types of identification documents involved;
4. Data Privacy Policy at the time of the incident.[25]

On 03 April 2023, HCPH, through its DPO, submitted its compliance with the Order issued on 23 March 2023.[26]

HCPH submitted as proof, the affidavit of JNL, Head of its IT Online Infrastructure and Platform.[27] JNL attested that there had been no subsequent connections made through the stolen laptop after its connection to the Puppet Server on 21 February 2018.[28]

---

[21] Order (To Submit Post Breach Report), 17 March 2022, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[22] Post-Breach Report, 18 April 2022, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[23] *Id.* at 3-5.
[24] Order (To Submit Proof in Support of the Post-Breach Report), 23 March 2023, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[25] *Id.* at 1.
[26] Email, 03 April 2023, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[27] Letter, 03 April 2023, Annex A, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[28] *Id.*

HCPH also provided the affidavit of PJM, its Information Security Officer.[29] PJM attested to the process followed by HCPH in handling lost or stolen IT equipment where IT Security performs a wipe out of the data contained in the stolen laptops and mobile phones.[30]

In addition to these, HCPH identified the types of IDs involved in the breach:

> Identification documents involved can range from Voter's ID, Passport, UMID, SSS ID, Driver's License, among others. These documents are however not saved in the laptop's storage itself but accessible when the user logs in to Home Credit's loan processing system accessible to Sales Associates.[31]

HCPH also attached copies of the process it follows when dealing with lost and stolen IT equipment[32] and its Data Privacy Policy at the time of the incident.[33]

Issue

I. Whether the matter falls under mandatory breach notification under Section 11 of NPC Circular 16-03 (Personal Data Breach Management); and

II. Whether HCPH 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. Nevertheless, HCPH sufficiently addressed the breach and implemented security measures to prevent its recurrence.

I. The matter does not fall under mandatory breach notification under Section 11 of NPC Circular 16-03.

---

[29] Letter, 03 April 2023, Annex B, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[30] *Id.*
[31] *Id.* at 1.
[32] *Id.* Annex C.
[33] *Id.* Annex D.

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]

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]

---

[34] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 11 (15 December 2016).
[35] 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 December 2024).
[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 25 September 2024).

Here, the first requisite is present. The breach involves sensitive personal information, or information that may, under the circumstances, be used to enable identity fraud.

According to HCPH, the information involved consists of HCPH customers' dates of birth and copies of their identification documents such as Voter's ID, Passport, UMID, SSS ID, and Driver's License.[37] These contain sensitive personal information under Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA).

Section 3 (l) of the DPA provides:

> Section 3. *Definition of Terms*. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> . . .
>
> (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.[38]

Here, the HCPH customers' respective dates of birth are considered sensitive personal information because the age of each HCPH customer may be determined from this information. As to the copies of the HCPH customers' government-issued IDs, these contain ID

[37] Data Breach Notification, 01 March 2018, at 4, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (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). Emphasis supplied.

numbers issued by government agencies peculiar to each HCPH customer. As such, the breach involves sensitive personal information as defined under the DPA.

In addition to this, HCPH stated that the breach involved its customers' full names, home addresses, permanent addresses and email addresses.[39] These may be considered as other information that, under the circumstances, may enable identity fraud.

In determining whether other information involved in a breach may enable identity fraud, Section 11 of NPC Circular 16-03 should be read together with Section 20 (f) of DPA. Section 20 (f) expressly requires the consideration of the specific circumstances of a 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.[40]

The Commission previously held that a data subject's name and email address may be considered under other information that may enable identity fraud.[41] The Commission explained:

> This Commission takes this opportunity to stress that information that may be used to enable identity fraud under

---

[39] Data Breach Notification, 01 March 2018, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[40] Data Privacy Act of 2012, § 20 (f). Emphasis supplied.
[41] 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 December 2024).

> 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.**[42]

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.[43] The Personal Information Controller (PIC) reported that a hacker accessed and implanted ransomware in an online database.[44] Because of these particular circumstances, the Commission concluded that the hacker may contact and send malicious emails directly to the data subjects.[45]

Here, the information accessible through the stolen laptop may be used to enable identity fraud. In its Data Breach Notification, HCPH stated that the breach involves HCPH customers' full names, home addresses, permanent addresses and email addresses.[46] As earlier discussed, the breach also involves sensitive personal information including the HCPH customers' dates of birth, and copies of their government issued IDs.[47] HCPH stated in its letter dated 03 April 2023 that these IDs include voter's IDs, Passports, UMIDs, SSS IDs, Driver's Licenses, among others.[48]

---

[42] *Id.* Emphasis supplied.
[43] *Id.* at 4.
[44] *Id.*
[45] *Id.*
[46] Data Breach Notification, 01 March 2018, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[47] *Id.* at 4.
[48] Letter, 03 April 2023, Annex A, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2023).

In this case, the laptop was stolen from one of HCPH's POS terminals.[49] The stolen laptop may be used to access the personal data involved through the HCPH loan processing system.[50] While HCPH was unable to identify the person who stole the laptop, the nature of the personal information involved shows that it may be used by a malicious party to commit identity fraud. In addition to this, although HCPH deployed a script to wipe the data off the stolen laptop, it was never able to regain control over the laptop.[51]

Given the specific circumstances of this matter, the names, email addresses, home addresses, permanent addresses, birthdates, and government-issued IDs of the HCPH customers provide adequate means of committing identity fraud. Notably, the information involved may be used by the malicious actor to impersonate the HCPH customers or to gain access to the HCPH customers' accounts. As such, the breach involves information that may, under the circumstances, be used to enable identity fraud.

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

The second requisite is present in this case. An unauthorized person acquired the information when the laptop was stolen.

The Commission previously held that a loss of control over personal data held in custody is enough for a PIC to have "reason to believe that the information may have been acquired by an unauthorized person."[52]

In this case, HCPH alleged that the laptop from which the personal data of the HCPH customers may be accessed was stolen from one of HCPH's POS terminals.[53] HCPH also stated that after the laptop was

---

[49] Data Breach Notification, 01 March 2018, at 3, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[50] Letter, 03 April 2023, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2023).
[51] Data Breach Notification, 01 March 2018, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[52] In re: Office Warehouse, Inc., NPC BN 18-144, 21 March 2024, at 8, *available at* https://privacy.gov.ph/wp-content/uploads/2024/09/NPC-BN-18-144-2024.03.21-In-re-Office-Warehouse-Inc.-Resolution.pdf (last accessed 03 December 2024).
[53] Data Breach Notification, 01 March 2018, at 3, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).

stolen, it was used to connect to the Puppet Server.[54] The foregoing shows that there is reasonable belief that an unauthorized person acquired the information involved in the breach.[55] Thus, the second requisite is present.

The third requisite, however, is absent. There is no 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 (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.[56]

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.[57] The risk must be apparent and not the product of mere speculation.[58] Serious harm means that the consequences and effects to any affected data subject are significant based on the surrounding circumstances of the breach.[59]

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 that has lapsed since the breach,

---

[54] *Id.*
[55] In re: Office Warehouse, Inc., NPC BN 18-144, 21 March 2024, at 8, *available at* https://privacy.gov.ph/wp-content/uploads/2024/09/NPC-BN-18-144-2024.03.21-In-re-Office-Warehouse-Inc.-Resolution.pdf (last accessed 03 December 2024).
[56] NPC Circ. No. 16-03, § 11.
[57] 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 December 2024).
[58] *Id.*
[59] *Id.*

objective of the unauthorized acquisition, security measures implemented on the information, and extent of potential misuse and exposure of the information.[60]

In this case, the laptop was taken from HCPH's POS terminal by an unauthorized individual.[61] According to HCPH, however, the information could only be accessed by the thief through HCPH's loan processing system, which is accessible to Sales Associates.[62] Based on HCPH's investigation, there was no indication of a system log-in that could have compromised the HCPH customers' information.[63]

According to HCPH, it immediately employed technical and organizational measures to protect the information involved in the breach.[64] HCPH deployed a script that would wipe the data and files stored in the stolen laptop and reformat it once it connects to the internet.[65] HCPH also conducted its own investigation on the matter and identified all the customers whose information was processed in the stolen laptop.[66] According to HCPH, no subsequent connections through the laptop were made after 21 February 2018.[67] It also provided as proof, the affidavit of its Information Security Officer who attested to the procedure followed by the HCPH IT Department which resulted in the wiping out of data stored in stolen IT equipment.[68]

HCPH also employed measures to prevent the recurrence of the incident. HCPH instituted a script to periodically wipe data and files from its POS laptops every 10:00 p.m.[69] It also implemented changes to improve its IT security such as the taking of client photos and supporting documents within its application so that files are not locally saved on the POS laptops, the enforcement of secure password requirements and the capturing of the last login timestamps on its POS

---

[60] *Id.*
[61] Data Breach Notification, 01 March 2018, at 3, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[62] Letter, 03 April 2023, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2023).
[63] Post-Breach Report, 18 April 2022, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2022).
[64] Data Breach Notification, 01 March 2018, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[65] *Id.*
[66] *Id.* at 4.
[67] Letter, 03 April 2023, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2023).
[68] *Id.* Annex B.
[69] Post-Breach Report, 18 April 2022, at 2, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2022).

laptops through the Foreman/Puppet server.[70] HCPH also continuously improved its data breach handling procedures and has made regular revisions in its Data Privacy Manual.[71]

Further, HCPH engaged its Security Department and the Anti-Fraud Team of its Risk Department to monitor and resolve any potential harm arising from the breach.[72]

Based on the foregoing factors and the remedial measures taken by HCPH, 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 third requisite is absent, the matter does not fall under mandatory breach notification.

II. HCPH sufficiently addressed the breach and implemented security measures to prevent its recurrence.

While mandatory breach notification is not required in this matter, HCPH notified the NPC of the breach. HCPH also sufficiently addressed the breach and implemented security measures to prevent its recurrence.

As previously discussed, HCPH monitored the activity on the stolen laptop and found that there was no indication of a system log-in that could have compromised the HCPH customers' information.[73] As a preventive measure, HCPH also instituted a script to periodically wipe data and files from its POS laptops every 10:00 p.m.[74] It also implemented changes in its processes, such as the taking of client photos and supporting documents within its application so that files are not locally saved on the POS laptops, the enforcement of secure password requirements and the capturing of the last login timestamps

---

[70] *Id.*
[71] *Id.*
[72] Data Breach Notification, 01 March 2018, at 3, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2018).
[73] Post-Breach Report, 18 April 2022, at 1, *in* In re: HC Consumer Finance Philippines, Inc., NPC BN 18-029 (NPC 2022).
[74] *Id.* at 2.

on its POS laptops through the Foreman/Puppet server.[75] Finally, HCPH also updated its internal policies concerning data breaches.[76]

Thus, HCPH sufficiently addressed the breach and implemented security measures to prevent its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 18-029 In re: HC Consumer Finance Philippines, Inc. is **CLOSED.**

SO ORDERED.

City of Pasay, Philippines.
04 September 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:

RBI
Data Protection Officer

[75] *Id.*
[76] *Id.*

HC Consumer Finance Philippines, Inc.

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