IN RE: PJ LHUILLIER INCORPORATED **NPC BN 19-002**

x---x

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is PJ Lhuillier Incorporated's (PJLI) breach notification and management in compliance with NPC Circular 16-03 (Personal Data Breach Management).

Facts

On 18 January 2019, PJLI reported a confidentiality breach involving its email marketing tool platform server.[1] PJLI stated that the server is used to send marketing emails to a subset of its clients and operates on an isolated network with its own ISP connection.[2]

According to PJLI, on 10 January 2019, an employee received a spam email and alerted PJLI's Information Security Department.[3] On the same date, PJLI discovered that the spam email had been sent using their Email Marketing Tool Platform.[4]

PJLI initially reported the breach as a series of spam emails, but further investigation traced them back to the email blast server.[5] The investigation allegedly revealed that "a non-standard email blast campaign job has been defined."[6] An Incident Response (IR) investigation subsequently identified a vulnerability in the web

[1] Initial Report, 18 January 2019, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[2] *Id.*
[3] Supporting Details June 2021 Updates for NPC, 18 June 2021, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[4] *Id.*
[5] Initial Report, 18 January 2019, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[6] *Id.*

application used for email blasts, which PJLI claims was exploited to gain unauthorized access to the server.[7]

The IR team conducted an examination of the server logs to check for other potential malicious activities exploiting the same vulnerability.[8] Based on its findings, in addition to the server being used to send spam emails, there were unauthorized attempts to export recipient lists from an undetermined number of contact lists.[9]

PJLI reported that the extent of exposed "Personally Identifiable Information (PII)" varies.[10] Some campaigns allegedly involved only the exposure of email addresses or mobile numbers, while others potentially included information such as names, birthdates, and income details.[11]

In response to the breach, PJLI claimed that it took the following steps:

(1) Removed the server from the network;

(2) Engaged a third-party for an IR investigation and validation of internal results;

(3) Revisited the regular vulnerability scans performed on the server, noting that the CVE used was not detected in previous scans;

(4) Continued the process of de-duplicating records; and

(5) Prepared notifications for affected data subjects.[12]

On 23 January 2019, PJLI submitted a supplemental report with the subject, "Data Breach Notification - Email Marketing Tool Platform Web App Report."[13] In the report, PJLI reiterated that the breach involved the exploitation of a vulnerability within the Interspire Email Marketing Web Application.[14] This vulnerability allegedly allowed unauthorized parties to bypass authentication of the web application, gain access to, and subsequently download recipient mailing lists originally compiled for marketing email campaigns.[15]

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] Initial Report, 18 January 2019, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).

[12] *Id.*

[13] Supplemental Report, 23 January 2019, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).

[14] *Id.* at 1.

[15] *Id.*

PJLI reiterated that the investigation suggests that the compromised "personally identifiable information (PII)" may include the following: (a) Email addresses; (b) Full names; (c) Birthdates; (d) Mobile numbers; and (e) Income ranges.[16]

PJLI claimed that it immediately disconnected the system upon discovery of the breach on 15 January 2019.[17] Further, PJLI engaged Red Rock Security, a third-party Information Security firm, to assist in preparing the incident report.[18]

PJLI provided the sequence of events from the initial report of a spam email to the submission of the initial report:[19]

January 10, 2019	Report of SPAM in a foreign language. Processed as per SOP as SPAM.
January 10, 2019	Discovery that SPAM source was the departmental web application used for marketing email blasts.
January 11, 2019	System configuration was updated to prevent its use to send out relays.
January 13, 2019	Recurrence of spamming relay. Campaign used to send out spam was disabled. Contacted business units to determine who created the campaign.
January 14, 2019	Changed password of account of server.
January 15, 2019	• Relaying persisted. Called in 3rd Party IR assistance to review collected evidence and initial internal investigation. • Confirmation of exploit used to send relay. Algerian IP 105.111.116.105 connected via Bing.com. This was then followed by a connection from AWS Germany 35.157.92.39 which loaded the spamming campaign. • Compromised Web application was immediately shut down. • Conducted log analysis to see if there were other activities aside from the relaying incident.
January 15, 2019	Confirmation of unauthorized downloads.

[16] *Id.*
[17] *Id.*
[18] Compliance, 18 June 2021, *Supporting Details June 2021 Updates for NPC*, in In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[19] Supplemental Report, 23 January 2019, at 1-2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).

<table>
<tr><td></td><td><table><tr><td>August 5, 2018
7:03 AM
11:30 PM
144.217.241.249
Canada</td><td>August 12, 2018
7:56 PM
3:56 AM
105. 157.205.190
Morocco</td></tr></table>
<i>Please refer to attached 3rd Party for additional details.</i></td></tr>
<tr><td>January 16, 2019</td><td>Activation of PJLI Data Breach Team / Corporate Crisis Team</td></tr>
<tr><td>January 17, 2019</td><td>Reported to PJLI Management Committee and Board of Directors</td></tr>
<tr><td>January 18, 2019</td><td>Initial meeting with the NPC to discuss the incident and ask for guidance regarding the next steps.</td></tr>
<tr><td>January 18, 2019</td><td>Submission of initial report. Start of client notification-related activities. Sourced out email marketing tool after NPC meeting since our email marketing web app was disabled.</td></tr>
</table>

PJLI initially claimed that according to the investigation, a total of nine hundred thirteen thousand three hundred seventy-one (913,371) data subjects were possibly affected.[20] PJLI alleged that the compromised "contact lists can be commoditized and sold [to be used] for malicious activities such as spam campaigns, phishing attacks, and similar threats."[21]

PJLI claimed that it took several measures to address the incident.[22] The email marketing web application involved was removed from the network, and logs were reviewed to identify other indicators of compromise to make sure that the incident was limited to the web application.[23]

To secure or recover the compromised personal data, PJLI stated that it "notified possibly affected data subjects" and "provided reminders on how to minimize [the risks of] password guessing attacks, phishing, and the likes."[24] Additionally, PJLI alleged that it has taken steps to mitigate possible harm and limit the damage and distress to those affected by the incident by providing contact details for feedback or

[20] *Id.* at 2.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*

inquiries and confirming that the incident was isolated to the email marketing web app with no transactional data exposed.[25]

To prevent a recurrence of the incident, PJLI states that it has discontinued the use of the email marketing web app and permanently removed it from their list of solutions.[26] It also engaged a third party to perform an independent vulnerability assessment to validate internal test results conducted regularly.[27] Further, PJLI reported the Common Vulnerabilities and Exposures (CVE) System used in the exploit to the Pen Testing Tool provider to ensure it can be detected in future versions.[28] It also claimed that it "[a]ugment[ed] existing information security controls by implementing a security operations center" and "deploying a Security Analytics and Intelligence solution to further improve proactive responses to security attacks as per their approved 2019 plans."[29]

On 10 May 2021, the NPC, through the Complaints and Investigation Division (CID), directed PJLI to submit additional details on the incident within fifteen (15) days from the receipt of the Order.[30] The CID instructed PJLI to submit the following:

> a. A copy of the notification to the affected data subjects, as well as the manner of sending the same and proof of receipt thereof;
>
> b. Proof of actions taken to mitigate the harm or negative consequences and limit the damage and distress of the affected data subjects;
>
> c. Full Investigation Report of the Company resulting from its own internal investigation on the breach incident;
>
> d. Detailed Investigation Report of the third-party service provider;
>
> e. Results of the vulnerability assessments and penetration tests conducted by third-party service providers;
>
> f. Results of the vulnerability assessments/scans and penetration tests conducted by the Company; and

[25] Supplemental Report, 23 January 2019, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2019).
[26] *Id.*
[27] *Id.* at 3.
[28] *Id.*
[29] *Id.*
[30] Order, 10 May 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

g. Network diagram/Topography at the time of the incident.[31]

On 18 June 2021, PJLI submitted its Compliance which included a Response to the Order dated 10 May 2021, and annexes containing the details of the incident as directed by the CID.[32] In contrast to its initial submissions, PJLI reported in its Compliance report that the number of affected data subjects totaled 912,015.[33]

PJLI included an incident report[34] and a 3rd Party Host Analysis Report of the incident[35] in its Compliance. PJLI stated that they use the Interspire Email Marketer version 6.1.2, which they installed on 22 July 2014, as their email marketing tool.[36] A vulnerability identified in this email marketing tool, titled "CVE-2017-14322," allows remote attackers to bypass authentication and gain administrative access.[37] This issue affects versions of Interspire Email Marketer prior to 6.1.6.[38]

As part of its Compliance, PJLI also submitted a copy of the notification template sent to the affected data subjects:

> Dear Valued Client,
>
> We are writing to inform you of a security incident which may have affected your personal data stored in one of our email marketing tool servers.
>
> On January 15, 2019, we detected attempts to use one of our email servers as a relay to send out spam to other domains. Follow-up investigation resulted in the discovery of unauthorized downloading of contact lists used as recipients for email campaigns. These unauthorized downloads took place on August 5, 8, and 12, 2018. Your personal information (name, birth date, email address, mobile number and in some cases, income information) may have been exposed in this incident. Upon discovery, remedial actions were taken to reduce the harm. The server was immediately disconnected from the network after confirmation of breach. The incident was likewise reported to the National Privacy Commission.

[31] *Id.* at 2.
[32] Compliance, 18 June 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[33] *Id. PJLI response to NPC 19 002 Received June 4 2021.*
[34] *Id. IR011-011019 Report.*
[35]*Id. 3rd Party Incident Review Report.*
[36] *Id.*
[37] Technical Report, 30 June 2021, at 1, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[38] *Id.*

> We value your patronage and respect the privacy of your personal information, and we are committed in our role in keeping your personal data safe and secure. As a precautionary measure, please observe the following steps in order to fully protect your user information:
>
> - Immediately change the passwords of all user accounts in which personal information details or portions of it are used as passwords.
> - Do not use the same password across multiple accounts. Use strong passwords. Change passwords regularly.
> - Regularly check your accounts for suspicious transactions.
> - Take advantage of available two-factor authentication features of applications that you use. For example. you can configure your account to require a one-time passcode (sent to your phone or other email) in addition to your password before you can access.
> - Be very cautious about providing personal information which will require you to click on links or download attachments contained in email, SMS or private messages. Take time to validate these requests for personal information through other communications channels (e.g. contact numbers in billing notices) with your online services providers.
>
> For any inquiries, please contact our Data Protection Officer thru the email emailprivacy@pjlhuillier.com or SMS only numbers 09188122737 or 09178122737. We will do our best to provide feedback to you as soon as possible.
>
> We undertake to provide more information to you as soon as they become available.[39]

Additionally, PJLI submitted the results of an internal vulnerability assessment test covering the affected server, [40] as well as a network diagram depicting the state of the network at the time of the incident.[41] PJLI has also provided evidence of the implementation of both organizational[42] and technical measures[43] within the organization.

As to PJLI's organizational measures, it attached proof that it observes Privacy Awareness Week (PAW) and Information Security Month.[44] PJLI also hosted activities such as "Defend the Flag" competitions in order to improve the skills of its information security team and "Catch

[39] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[40] *Id. IR011-011019 Report.*
[41] *Id. Network Diagram During Time of Incident.*
[42] *Id. Proof of Implementation – Organizational.*
[43] *Id. Proof of Implementation – Technical.*
[44] *Id. Proof of Implementation – Organizational.*

the Phish Quiz/Test" which aims to educate employees about phishing threats and how to identify them.[45]

PJLI also included proof of its technical measures.[46] It has a Host-based Intrusion Protection System (HIPS)[47] that analyzes detailed activities on monitored hosts, identifying malicious processes or users and accessing data files and system processes to monitor attack outcomes.[48]

PJLI also uses a Security Information and Event Management (SIEM) system[49] to collect, categorize, and analyze log and event data from applications, security devices, and host systems, generating alerts and threat levels based on predefined rules.[50] Additionally, Honeypot monitoring is in place,[51] using deception technology to lure cybercriminals into exploiting vulnerabilities, allowing the security team to study attacker behaviors and improve security policies.[52]

Moreover, PJLI employs Akamai Enterprise Threat Protector,[53] a cloud-based secure web gateway, later transitioned to Cloudflare in 2020,[54] ensuring safe internet connections for users and devices.[55] It also has a Sophos Web Appliance[56] to block web threats at the source, enforce acceptable use policies, and safeguard against data loss.[57] PJLI also has Imperva Database Firewall,[58] a database firewall that monitors databases to protect against attacks targeting sensitive information.[59] In 2020, PJLI installed anti-exploit/ransomware software,[60] adding an extra layer of security by blocking attacker techniques, including new

[45] Compliance, 18 June 2021, *Proof of Implementation - Organizational*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[46] *Id. Proof of Implementation – Technical*.
[47] *Id. Proof of controls prior to incident*.
[48] Technical Report, 30 June 2021, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[49] Compliance, 18 June 2021, at *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[50] Technical Report, 30 June 2021, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[51] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[52] Technical Report, 30 June 2021, at 2, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[53] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[54] *Id. Proof of Implementation – Technical.*
[55] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[56] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[57] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[58] Compliance, 18 June 2021, *Proof of Implementation - Technical*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[59] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[60] Compliance, 18 June 2021, *Proof of Implementation - Technical, in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

exploits and ransomware that threaten to block access to data unless a ransom is paid.[61]

On 24 September 2021, the CID directed PJLI to clarify the following statements made by the latter in its submissions:

> 1. At the time of the contract with Web Solutions Inc, the latest version of Interspire Email Marketer available is version 6.1.4, Why did PJLI chose the prior version of 6.1.2?
>
> 2. As to the number of affected data subjects, clarify the breakdown of the nine hundred twelve thousand and fifteen (912,015).
>
> 3. On 10 Ianuary 2019, PJLI updated its CLAM AV. When was the last update of Clam AV prior to this date, as well as the frequency of updates?
>
> 4. The vulnerability assessment was noted to have a change as to frequency, what brought about the change?
>
> 5. Upon investigation, what caused the non-detection of the published vulnerability?
>
> 6. Attach proof of receipt/ sending of the notification to the data subjects[62]

On 29 September 2021 PJLI submitted its response.[63] It claimed that at the time of deployment, its vendor recommended version 6.1.2 of Interspire Email Marketer as the stated and stable version.[64] PJLI also attached a breakdown of the 912,015 affected data subjects:[65]

912,015	Represents master list of recipients for email notifications. Since investigation was still ongoing at this point, PJLI decided to notify all clients in its email database list to ensure that we can comply with the prescribed notification deadline of within 72 hours.
10,697	Represents subset of records created after August 13 which was after the reported breach.

[61] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[62] Additional Questions from CID, 24 September 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[63] PJLI Response dated 29 September 2021, 29 September 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[64] *Id.* at 1.
[65] *Id.*

901, 318	Represents records which were possibly included in the breach
121,059	Hard bounced emails as reported by mailchimp.com
780,259	Emails not included in the hard bounced list which means they were notified accordingly
Breakdown using email address as the main identifier	
260,190	number of records containing email details only
1,761	number of records containing email and name details only
70,171	number of records containing email, name, and bday
71,485	number of records containing email, name, bday and possibly other PIIs such as of age, gender, educational attainment, civil status or income bracket value estimates
377,495	number of records containing email, and possibly other PIIs such as of age, gender, educational attainment, civil status or income bracket value estimates

As part of its response, PJLI included an Email Campaign Report as proof of sending the notification to the affected data subjects:[66]

Email Campaign Report	
Title:	Privacy Notice
Subject Line:	Notice from Cebuana Lhuillier Data Privacy Officer
Delivery Date/Time:	Sat, Jan 19, 2019 8:00 am
Overall Stats	
Total Recipients:	912,015
Successful Deliveries:	787,335
Bounces:	124,680 (13.7%)
Recipients Who Opened:	119,635 (15.2%)
Total Opens:	177,468
Last Open Date:	6/16/21 9:33AM
Total Unsubs:	1,062

On 1 October 2021, the CID directed PJLI to clarify the number of affected data subjects.[67] The CID noted that nine hundred one thousand three hundred eighteen (901,318) records were compromised.[68] There, however, was a discrepancy of one hundred

[66] *Id.* at 2.
[67] Order, 01 October 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[68] *Id.*

twenty thousand two hundred sixteen (120,216) records in the breakdown of compromised personal data.[69] Thus, CID directed PJLI to clarify the specific personal data compromised for the one hundred twenty thousand two hundred sixteen (120,216) data subjects identified in the discrepancy.[70]

The CID also observed that one hundred twenty-four thousand six hundred eighty (124,680) notifications to affected data subjects bounced, meaning those individuals did not receive the notification.[71] Since not only email addresses but other personal data were compromised, the CID requested details on how PJLI notified these data subjects and the specific personal data compromised.[72]

PJLI clarified that there was a line item that was mistakenly omitted in the breakdown included in their previous submission.[73] Thus, PJLI attached an updated breakdown of affected data subjects:[74]

901,318	Total records on or before 13 August 2018
BREAKDOWN	
260,190	Email Only
1,761	Email and name
70,171	Email, name and birthday
71,485	Email, name, birthday and other PIIs such as the age, gender, mobile number, educational attainment, civil status and income bracket values
377,495	Email and other PIIs such as the age, gender, mobile number, educational attainment, civil status and income bracket values
120,216	Email and other PIIs possibly with Age, Town, City, Civil Status, Gender, NumChild, Education, House, source fund

For the one hundred twenty-four thousand six hundred eighty (124,680) data subjects whose notifications bounced, PJLI indicated that there were no other means of notification because there were no mobile numbers or complete addresses available for use.[75] Regarding the specific personal data compromised, PJLI claimed that thirteen

[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] PJLI Response dated 06 October 2021, at 1, 06 October 2021, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[74] *Id.*
[75] *Id.*

thousand six hundred eight (13,608) involved only email addresses while one hundred eleven thousand seventy-two (111,072) included email addresses, age, town, city, civil status, gender, number of children, education, house, and source of funds.[76]

Issue

Whether PJLI notified its affected data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. PJLI's submissions show that it properly notified its affected data subjects, sufficiently addressed the breach, and implemented measures to prevent its recurrence.

It is the obligation of a Personal Information Controller (PIC), such as PJLI, to ensure that affected data subjects of the breach are promptly and properly notified.[77] The Commission has consistently emphasized that the purpose of the required notification to the data subjects of a breach is to allow them to take the necessary precautions or other measures to protect themselves against its possible effects.[78]

Section 18 of NPC Circular 16-03 provides the requirements as to the content and form of the notification of data subjects:

> Section 18. *Notification of Data Subjects*. The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> . . .
>
> C. *Content of Notification*. The notification shall include, but not be limited to:
>
> 1. nature of the breach;
> 2. personal data possibly involved;
> 3. measures taken to address the breach;

[76] *Id.*
[77] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[78] NPC Circ. No. 16-03, § 18 (A).

> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
> 6. any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.
>
> D. *Form.* Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.
>
> The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller 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: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.[79]

In this case, PJLI notified the affected data subjects about the security incident through a letter sent by email.[80]

PJLI identified the nature of the breach by informing the recipients of a security incident involving unauthorized attempts to use their email server to send spam and unauthorized downloading of contact lists.[81] This fulfilled the requirement to describe the nature of the breach. [82]

[79] NPC Circ. No. 16-03, § 18 (C) & (D).
[80] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[81] *Id.*
[82] NPC Circ. No. 16-03, § 18 (C).

The notification specified the types of personal data that may have been exposed, including name, birth date, email address, mobile number, and, in some cases, income information.[83]

The notification also outlined the immediate actions taken to address the breach, such as disconnecting the affected server from the network and reporting the incident to the National Privacy Commission.[84] Additionally, the notification described the steps PJLI took to reduce harm, including server disconnection and actions to prevent further unauthorized access.[85]

PJLI provided the Data Protection Officer's (DPO) contact information, including an email address and phone numbers, allowing data subjects to obtain additional information regarding the breach.[86] This satisfied the requirement to include contact information of a representative from whom more information could be obtained.[87] The notification also included practical advice for data subjects to protect their information, such as changing passwords, using strong passwords, enabling two-factor authentication, and being cautious about phishing attempts.[88]

In addition, PJLI took measures to sufficiently address the breach and adopted measures to prevent its recurrence.

Section 20 of the DPA provides that 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

[83] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] NPC Circ. No. 16-03, § 18 (C).
[88] Compliance, 18 June 2021, *Notification to Affected Data Subjects*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

> accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[89]

As part of its organizational measures, PJLI took several significant steps to ensure data protection and security. PJLI designated a DPO whose name and business contact information are registered with the NPC. Further, PJLI established a Data Breach Management and Corporate Crisis Team.

Additionally, PJLI engaged in various activities to bolster its data security practices. It participated in and hosted a "Defend the Flag" competition designed to enhance the skills of its information security team by simulating real-world cyber-attack scenarios.[90] PJLI developed the "Catch the Phish Quiz/Test," an initiative aimed at educating employees about phishing threats and how to identify and avoid them.[91]

Moreover, PJLI's Information and Communication Technology (ICT) service provider, Networld Capital Ventures Incorporated (NCVI), is certified to be compliant with the requirements of ISO 27001:2013, a globally recognized standard for information security management systems.

As to its technical security measures, PJLI employed multiple vulnerability assessment and penetration test providers to ensure comprehensive detection and mitigation of all potential vulnerabilities in their system. This includes a Host-based Intrusion Protection System (HIPS) to monitor host activities and identify malicious processes,[92] and a Security Information and Event Management (SIEM) system to analyze log data and generate alerts based on predefined rules.[93] PJLI also uses Honeypot monitoring to study attacker behaviors,[94] Akamai Enterprise Threat Protector (transitioned to Cloudflare in 2020) for secure web connections,[95] and a Sophos Web

[89] 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 § 20 (a) (2012).
[90] Compliance, 18 June 2021, *Proof of Implementation - Organizational*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[91] *Id.*
[92] *Id. Proof of controls prior to incident.*
[93] *Id.*
[94] *Id.*
[95] *Id.*

Appliance to block web threats and enforce acceptable use policies.[96] Additionally, they employ the Imperva Database Firewall to protect databases[97] and have installed anti-exploit/ransomware software to block new exploits and ransomware threats.[98]

Given the foregoing, the Commission finds that the measures undertaken by PJLI have sufficiently addressed the incident and prevented its recurrence.

WHEREFORE, premises considered, this Commission resolves that the matter of NPC BN 19-002 In re: PJ Lhuillier Incorporated 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

[96] Compliance, 18 June 2021, *Proof of controls prior to incident*, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).
[97] *Id. Proof of Implementation – Technical.*
[98] Technical Report, 30 June 2021, at 3, *in* In re: PJ Lhuillier, Inc., NPC BN 19-002 (NPC 2021).

Copy furnished:

APM
Data Protection Officer
PJ Lhuillier Incorporated

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission