Data Breach Incident of Kwong's Art Jewellery Trading Company Limited and My Jewelry Management Limited Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance,
Chapter 486 of the Laws of Hong Kong

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) completed its investigation in relation to a data breach incident reported by Kwong's Art Jewellery Trading Company Limited (Kwong's Art Jewellery) and My Jewelry Management Limited (My Jewelry).

The investigation arose from a data breach notification submitted by Kwong's Art Jewellery and My Jewelry to the PCPD on 11 November 2024, reporting abnormalities in their shared information systems and receipt of messages from a threat actor which claimed that the data stored in the information systems of Kwong's Art Jewellery and My Jewelry had been stolen. Upon inspection, Kwong's Art Jewellery and My Jewelry confirmed that the data stored in their database server had been stolen and deleted (Incident).

Kwong's Art Jewellery is the parent company of My Jewelry and is engaged in jewellery manufacturing and wholesale, while My Jewelry is a jewellery retail company which operates the brand "My Jewelry". Kwong's Art Jewellery and My Jewelry have been jointly managing and using the affected information systems, including the servers, applications and databases.

The investigation revealed that the threat actor conducted a brute-force attack to obtain the credentials of an administrator account (Account). The threat actor utilised the Account to gain access to the information systems of the two companies and performed lateral movement within the network, which included implanting a Trojan Horse program on a desktop computer used for internal system development and programming. This allowed

the threat actor to obtain the source code to control the database server, which led to the successful exfiltration and deletion of the personal data stored therein.

According to the information provided by Kwong's Art Jewellery and My Jewelry, approximately 79,400 data subjects were affected by the Incident, including corporate customers and current and former employees of Kwong's Art Jewellery, as well as retail customers and current and former employees of My Jewelry. The personal data affected included the names, Hong Kong Identity Card numbers, dates of birth, telephone numbers, addresses and commencement dates of employment of employees, as well as the names, Hong Kong Identity Card numbers (first four alphanumeric characters), years and months of birth, telephone numbers, email addresses, and membership numbers of customers.

Following the Incident, Kwong's Art Jewellery and My Jewelry implemented various improvement measures to enhance the security of their information systems, which included resetting login passwords for all users, updating operating systems of servers, antivirus software and firewall, as well as deploying "extended detection and response" tools for continuous monitoring of their information systems, etc. In addition, Kwong's Art Jewellery and My Jewelry notified all affected data subjects after the Incident.

Investigation Findings

The PCPD conducted seven rounds of inquiries and reviewed the information provided by Kwong's Art Jewellery and My Jewelry in relation to the Incident, and the follow-up and remedial actions taken by the two companies after the Incident. Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner for Personal Data (Privacy Commissioner), Ms Ada CHUNG Lai-ling, found that the following deficiencies of Kwong's Art Jewellery and My Jewelry contributed to the occurrence of the Incident (See Annex 1 for details):-

1. Failure to delete a former employee's account in a timely manner;
2. Lack of effective security and detection measures in the information systems;
3. Outdated operating systems of servers;
4. Lack of policies and guidelines on information security; and
5. Absence of security assessments and audits of the information systems.

The Privacy Commissioner's Decision

The Privacy Commissioner considered that Kwong's Art Jewellery and My Jewelry failed to adopt adequate and effective security measures at the time of the Incident to safeguard the personal data in their possession. The Privacy Commissioner expressed profound regret that Kwong's Art Jewellery and My Jewelry failed to recognise the security risks in their information systems, resulting in the failure to timely delete the former employee's account, failure to implement effective security and detection measures, the use of outdated operating systems of servers, failure to formulate policies and guidelines on information security, and the absence of security assessments and audits of the information systems, which eventually led to the Incident.

Based on the above, the Privacy Commissioner found that Kwong's Art Jewellery and My Jewelry had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening Data Protection Principle 4(1) of the Personal Data (Privacy) Ordinance concerning the security of personal data.

The Privacy Commissioner has served Enforcement Notices on Kwong's Art Jewellery and My Jewelry, directing them to take measures to remedy the contraventions and prevent recurrence of similar contraventions in future.

Recommendations

Through this report, the Privacy Commissioner recommends organisations to adopt appropriate organisational and technical measures to safeguard their information systems that contain personal data so as to strengthen data security:

- Establish clear internal policies and procedures to safeguard the security of information systems and ensure thorough implementation of the same;
- Implement effective measures to prevent, detect and respond to cyberattacks, including conducting regular vulnerability scans and patching cybersecurity vulnerabilities in a timely manner;
- Cease the use of end-of-support software and upgrade software in a timely manner;

- Enhance password management of information systems and adopt multi-factor authentication;
- Conduct comprehensive security risk reviews and audits for information systems regularly;
- Configure appropriate security functions on service platforms provided by third-party vendors and conduct regular security review;
- Formulate a data breach response plan; and
- Provide appropriate training to employees to improve their data security awareness.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
21 August 2025

Annex 1

Data Breach Incident of Kwong's Art Jewellery Trading Company Limited and My Jewelry Management Limited Deficiencies that Contributed to the Incident

1. **Failure to delete a former employee's account in a timely manner**: The Account was left idle for more than 13 years and the multi-factor authentication and account lockout function were not enabled for the Account at the time of the Incident. The threat actor eventually gained access to the information systems of Kwong's Art Jewellery and My Jewelry via the Account and stole and deleted the personal data stored in the database server;

2. **Lack of effective security and detection measures in the information systems**: The firewall and antivirus software deployed by Kwong's Art Jewellery and My Jewelry were outdated, which led to the failure to effectively defend against the cyberattack. Moreover, Kwong's Art Jewellery and My Jewelry did not implement additional protective measures for effective real-time or regular monitoring of the activities within their information systems;

3. **Outdated operating systems of servers**: The operating system of the affected database server was not up-to-date and the vendor had discontinued support for the relevant operating system for four years. Kwong's Art Jewellery and My Jewelry not only failed to update the operating system of the database server in a timely manner, but also failed to implement any additional security measures at the time of the Incident;

4. **Lack of policies and guidelines on information security**: Kwong's Art Jewellery and My Jewelry did not establish written policies or guidelines on system security, account management, password requirements, activity monitoring, and system updates for staff members to follow. In addition, they failed to formulate response plans and reporting mechanisms for data security incidents; and

5. **Absence of security assessments and audits of the information systems**: Kwong's Art Jewellery and My Jewelry had not conducted any forms of security assessments

and audits on their information systems to identify potential information security risks before the Incident.