EMSD responds to PCPD report

The Electrical and Mechanical Services Department (EMSD) noted that the Office of the Privacy Commissioner for Personal Data (PCPD) has completed its investigation of the leakage of personal data from an online server platform of the EMSD's contractor, and released the investigation report today (December 9). The personal data were collected by the EMSD in "restriction-testing declaration" operations to combat COVID-19 in 2022. The EMSD will study the report in detail for stringent and appropriate follow-up actions.

The EMSD attaches great importance to information security and personal data privacy. Relevant policies and guidelines (including the retention period of personal data) have been formulated and circulated to staff regularly. The procurement terms between the EMSD and the contractor providing the online server platform stated that the relevant data would be deleted after termination of the service, and the EMSD had clearly informed the contractor of the expiry of the service by the end of February 2023. Since noticing the leakage of the data on April 30, 2024, the EMSD has been acting in a proactive and responsible manner in reporting the case to law enforcement agencies, and has been co-operating with the PCPD on the investigation. Noting that the PCPD has announced earlier that there were cases of leakage of personal data involving the same online server platform provided by the contractor during the same period, the EMSD immediately conducted an in-depth enquiry with the contractor about the operational details of the server platform to ensure the complete removal of the relevant data.

Having consolidated the experience from this incident, the EMSD is committed to establishing a more robust privacy security framework and a corporate culture for personal data protection to prevent the recurrence of similar incidents. It has since taken a series of measures, including reinforcement of privacy management, holistically reviewing and enhancing guidelines in handling personal data, stepping up staff training, and monitoring contractors of online server platforms. It will also enhance computer system support, including developing a dedicated platform to store personal data in its own server. For outsourced services involving the handling of personal data, the EMSD will remind the contractor to delete the relevant data by the end of the retention period, and will proactively check with the contractor to confirm that the deletion of personal data has been completed.

Company and its director fined $60,000

for contravening Employment Ordinance

Ready To Cook Limited and its director were prosecuted by the Labour Department (LD) for violation of the requirements under the Employment Ordinance (EO). The company and its director pleaded guilty at Kowloon City Magistrates' Courts today (December 9) and were fined a total sum of $60,000. The company was also ordered to pay an outstanding sum of about $34,000 to the employee concerned.

The company wilfully and without reasonable excuse contravened the requirements of the EO, failing to pay an employee wages within seven days after the expiry of wage periods and termination of an employment contract totalling about $34,000, as well as the awarded sum of about $34,000, within 14 days after the date set by the Labour Tribunal (LT). The director concerned was prosecuted and convicted for his consent, connivance or neglect in the above offences.

"The ruling will disseminate a strong message to all employers, directors and responsible officers of companies that they have to pay wages to employees within the statutory time limit stipulated in the EO, as well as the sums awarded by the LT or the Minor Employment Claims Adjudication Board," a spokesman for the LD said.

"The LD will not tolerate these offences and will spare no effort in enforcing the law and safeguarding employees’ statutory rights," the spokesman added.

Fraudulent website and internet banking login screen related to China CITIC Bank International Limited

The following is issued on behalf of the Hong Kong Monetary Authority:

The Hong Kong Monetary Authority (HKMA) wishes to alert members of the public to a press release issued by China CITIC Bank International Limited relating to a fraudulent website and an internet banking login screen, which have been reported to the HKMA. A hyperlink to the press release is available on the HKMA website.

The HKMA wishes to remind the public that banks will not send SMS or emails with embedded hyperlinks which direct them to the banks' websites to carry out transactions. They will not ask customers for sensitive personal information, such as login passwords or one-time password, by phone, email or

SMS (including via embedded hyperlinks).

Anyone who has provided his or her personal information, or who has conducted any financial transactions, through or in response to the website or login screen concerned, should contact the bank using the contact information provided in the press release, and report the matter to the Police by contacting the Crime Wing Information Centre of the Hong Kong Police Force at 2860 5012.

Fraudulent website and internet banking login screen related to Industrial and Commercial Bank of China (Asia) Limited

The following is issued on behalf of the Hong Kong Monetary Authority:

The Hong Kong Monetary Authority (HKMA) wishes to alert members of the public to a press release issued by Industrial and Commercial Bank of China (Asia) Limited relating to a fraudulent website and an internet banking login screen, which have been reported to the HKMA. A hyperlink to the press release is available on the HKMA website.

The HKMA wishes to remind the public that banks will not send SMS or emails with embedded hyperlinks which direct them to the banks' websites to carry out transactions. They will not ask customers for sensitive personal information, such as login passwords or one-time password, by phone, email or SMS (including via embedded hyperlinks).

Anyone who has provided his or her personal information, or who has conducted any financial transactions, through or in response to the website or login screen concerned, should contact the bank using the contact information provided in the press release, and report the matter to the Police by contacting the Crime Wing Information Centre of the Hong Kong Police Force at 2860 5012.

Fraudulent website and internet

banking login screen related to China Construction Bank (Asia) Corporation Limited

The following is issued on behalf of the Hong Kong Monetary Authority:

The Hong Kong Monetary Authority (HKMA) wishes to alert members of the public to a press release issued by China Construction Bank (Asia) Corporation Limited relating to a fraudulent website and an internet banking login screen, which have been reported to the HKMA. A hyperlink to the press release is available on the HKMA website.

The HKMA wishes to remind the public that banks will not send SMS or emails with embedded hyperlinks which direct them to the banks' websites to carry out transactions. They will not ask customers for sensitive personal information, such as login passwords or one-time password, by phone, email or SMS (including via embedded hyperlinks).

Anyone who has provided his or her personal information, or who has conducted any financial transactions, through or in response to the website or login screen concerned, should contact the bank using the contact information provided in the press release, and report the matter to the Police by contacting the Crime Wing Information Centre of the Hong Kong Police Force at 2860 5012.