Legislative Council Panel on Constitutional Affairs

Suspected Theft of Registration and Electoral Office Computers Containing Personal Data of Registered Voters and Follow-up Measures

This paper briefs Members on the incident of suspected theft of two notebook computers stored inside a locked room at the AsiaWorld-Expo ("AWE"), which was the fallback venue of the 2017 Chief Executive ("CE") Election, and provides Members with information on the situation, preliminary direction of review, and improvement measures regarding the use of electors' information in the CE Election, venue security at the fallback venue, and security measures on information technology ("IT").

2. The Registration and Electoral Office ("REO") sincerely apologises for any inconvenience and distress to the public caused by the incident.

Background

3. In preparing for the CE Election held on 26 March 2017, the REO had to ensure that there would be a fallback venue that could be able to operate at short notice when there is an actual need to do so. As the AWE has been used for setting up the Central Counting Station and the Media Centre for the 2016 Legislative Council ("LegCo") General Election and the 2016 Election Committee ("EC") Subsector Ordinary Elections, the REO chose the AWE as the fallback venue for the 2017 CE Election and arranged for the setting up of the venue and testing of the computer systems at the AWE before the conduct of the election.

Summary of the Incident

4. After the completion of setting up the venue and the testing of computers on 24 March 2017, REO staff left the AWE in the same evening, and notified the control room of AWE to deactivate the card keys to the doors of the store room in which the notebook computers were stored, and turned the door into locked mode. On 27 March 2017, i.e. the day following the 2017 CE

Election, staff from the REO went to the AWE for packing and counting of the IT equipment at around 10:00 am. At around noon, the staff found that the two notebook computers stored in the concerned store room were missing and suspected that they were stolen. After repeated counting of the equipment, the REO staff reported the case to the Police at around 4:30 pm.

5. Of the two notebook computers suspected to be stolen, one contained the names of EC members without any other personal particulars. As the relevant names had already been promulgated through public platforms, there was no risk of data leakage. The other computer contained information of about 3.78 million Geographical Constituencies ("GCs") electors in the 2016 Final Register, including their names, addresses, Hong Kong Identity Card ("HKID") numbers, and the constituencies the electors are registered in. All the information has been encrypted in accordance with the relevant government security requirements. The setting of password has followed the relevant security requirements. Neither telephone numbers of electors nor voting records were stored in these computers.

Immediate Handling, Latest Development and Corresponding Actions Taken

6. The Police has classified the case as theft. The REO is fully assisting in the Police investigation. As the criminal investigation is still ongoing, we are unable to disclose further details on the progress of investigation.

7. The REO also reported the incident on 27 March (the same day which the case was reported to the Police) to the Office of the Privacy Commissioner for Personal Data ("PCPD") and the Government Information Security Incident Response Office, and understand that the PCPD will conduct a compliance check on the incident. The REO will fully and duly follow up on improvement measures and recommendations by the PCPD.

8. The REO issued press releases on 27, 28 and 30 March to inform the public about the suspected theft of the computers. The Constitutional and Mainland Affairs Bureau ("CMAB") and the Electoral Affairs Commission ("EAC") also issued press releases on 27 and 28 March respectively, instructing the REO to fully assist in the Police investigation. The REO will submit an incident report to the CMAB and the EAC, covering the detailed arrangement

for the transportation of IT equipment from REO office to the AWE, security measures on data stored in computers and venue security for the storage of IT equipment, etc.

9. Since 30 March, the REO has also written to government departments and organisations of various sectors, including finance, insurance, telecommunications, retail, estate agents, information technology, etc., to notify them of the incident and appeal to their assistance in adopting appropriate measures to prevent criminals from using the relevant information as a mean of identity theft in criminal activities, so as to protect their own interest and also the interest of the data subjects. We understand that the Hong Kong Monetary Authority has contacted a number of retail banks, who indicated that they follow rigorous loan vetting and approval procedures. An individual cannot obtain any bank loan or apply for credit cards by simply providing his name, HKID number and address. There are also corresponding additional security measures for online banking and telephone banking services. Generally speaking, one cannot access the online banking services by using his or her name and HKID number alone, and high-risk transactions such as third party transfer are not allowed through telephone banking. As for loans, a payment agreement or an interest payment agreement with respect to the loan granted by the money lender shall be prepared in writing as abstract or memorandum in accordance with section 18(1) of the Money Lenders Ordinance (Cap 163), and signed by the borrower in person, otherwise such agreement or guarantee shall not be enforced. We understand that finance companies will only grant loans to the applicants upon the provision of proof of identity. In addition, according to the relevant laws[1], proof of identity is required for the successful completion of property or insurance transactions. We will continue to keep in view the situation and maintain close contact with government departments, the PCPD, and the relevant regulatory authorities, so as to minimise the possible impact of the incident.

10. Following the PCPD's guidelines and advice, the REO informed all GC electors of the incident via email or letters to increase their awareness and to minimise potential damage. About 550 000 electors, who have provided email addresses to the REO, were informed by email starting from 30 March. The

---

[1] Including Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap 615) and Estate Agents Practice (General Duties and Hong Kong Residential Properties) Regulation (Cap 511C).

REO has also started sending letters since 31 March to other electors by post in batches. The letter has also been uploaded onto the REO website (www.reo.gov.hk).

11. The REO has reminded staff to watch out for any unusual or suspicious voter registration and change of particulars applications. For any incomplete or suspicious cases, our staff will clarify with the applicants and ask for written supplementary information, if necessary. If the applicant fails to provide supplementary information, REO will in general not process the application further.

12. The REO also encourages electors to use the Online Voter Information Enquiry System (www.voterinfo.gov.hk) to check their registration status and particulars. If electors have any queries or would like to report any suspicious changes in their registration particulars, they may contact the REO for assistance. In case of suspected identity theft, electors should report to the Police immediately.

Result of Preliminary Review and Proposed Improvement Measures

13. In the light of the suspected theft of notebook computers which contained electors' information at the fallback venue of the CE Election, the REO admits that there are indeed deficiencies in the relevant arrangements, and will consider improvement measures from three aspects, including the use of electors' information in the CE Election, venue security at the fallback site and IT security measures.

Use of electors' information in the Chief Executive Election

14. The computer system storing electors' information in one of the computers is mainly used for checking the registration particulars and voting eligibility of electors. In previous elections, the system concerned would be set up at dedicated polling stations in police stations. If a detainee requests casting vote on the polling day, the polling staff of the dedicated polling station will verify his/her voting eligibility through the system. Given the detainees may be electors of any constituency; the system is designed to store the information of all the electors in Hong Kong to facilitate the verification process.

15. In the CE Election, for security reasons, only EC members and authorised persons were allowed to enter the main polling station. The system was installed at the entrance of the main polling station to facilitate the overall admission arrangement at the venue, so that enquiries regarding voting eligibility at the entrance could be promptly and appropriately handled. This could also help handle cases where EC members might have forgotten to bring along their name badges on the polling day. For instance, if an EC member forgot to bring along his/her name badge, he/she would be requested to produce his/her identity card for verification.. Upon confirming his/her eligibility, the EC member concerned would be issued with a replacement name badge. If any person had any doubt about his/her eligibility to vote, the polling staff could also make use of the system to check the relevant registration particulars and explain the details to the person concerned about his/her voting eligibility.

16. Upon preliminary review of the practice, under the premises of protection of personal data and IT security, the REO considers that adopting the system developed for detainees for use in the LegCo and District Council elections for the CE Election is not appropriate as the bases of the electorate of these elections are different. In the future CE Election, the system will only store information of EC members.

Venue security at the fallback venue

17. As a fallback venue plan is required for the CE Election, the REO is required to conduct sufficient preparation work at the fallback venue. According to the established practice, the REO would arrange the computers required for the fallback venue and ensure that the computer systems concerned have been properly installed and tested before the polling day. In view of the relatively short polling time and the remote location of the AWE, most of the electoral materials are prearranged at the fallback venue so that in case the fallback venue has to be activated, the polling could start at the AWE as soon as practicable.

18. After the testing of computers arranged on 24 March was completed in the evening on that day, according to the relevant procedures, the REO staff had to shut down the computers, store the computers in the concerned room and lock the room.

19. The standing CCTV cameras at various locations of AWE are directly connected to the AWE control room under round-the-clock surveillance by their security personnel. During the period between the commencement of setting up of the fallback venue to the moving out period after the election, the REO arranged for additional security supervisors and security guards to patrol and station at different positions of the venue. The REO also arranged for installation of additional CCTV cameras at designated spots, including the foyer outside the concerned room. The concerned computers were stored in a locked room but no arrangement was made to store them in a locked cabinet. Since criminal investigation is in progress, it would not be appropriate to disclose detailed security arrangements at this stage.

20. After preliminary review, REO considers that there is room for improvement in the storage of notebook computers at the fallback venue. Under the major premises of protection of personal data and IT security, it would be more appropriate to deliver the notebook computers to the fallback venue only when the fallback plan is activated. The REO will revise the procedures of activating the fallback venue, while ensuring that such changes will not substantially lengthen the time needed for the fallback venue to commence operation.

21. Separately, regarding the security arrangements of the venue, the REO considers that such arrangements, including those for the fallback venue, should be approved by staff at the management level, who should also provide sufficient and adequate guidelines and directions to the front-line staff so as to ensure that all security arrangements are properly carried out.

Security measures of information technology

22. On the handling of personal information of members of the public, the REO needs to comply with the relevant policies and regulations of the Government, including the Security Regulations, and the IT security regulations and policies of the Office of the Government Chief Information Officer ("OGCIO"). Such regulations and policies cover areas including access control to information systems and data, office security, software asset management and authorisation requirements for using software not supplied by Government, etc. The regulations, policies and guidelines are developed and reviewed by the OGCIO with reference to the international best practices. The

REO has also drawn up corresponding internal guidelines based on the above regulations, policies and guidelines, and periodically reminds staff, including contract staff, to comply with such information security provisions. Besides, the REO has also drawn up internal guidelines for handling of personal data of electors in accordance with the Personal Data (Privacy) Ordinance.

23. One of the stolen computers contained information of about 3.78 million GCs electors in the 2016 Final Register, including their names, addresses, HKID numbers, and the constituencies the electors are registered in. All the information has been encrypted in accordance with the relevant security requirements and protected by multiple encryptions. The encryption algorithm used in the system conforms to the related guideline of the OGCIO, and is one of the stringent industrial standards in use.

24. In response to the incident, the REO will work with relevant departments and comprehensively review the related arrangements by the REO on the collection, use, processing and storing of the personal information of electors, system requirements and the overall security arrangements, etc., and will fully and duly follow up on the improvement measures and recommendations to be made by PCPD upon the completion of their compliance check.

Next Step

25. The REO is fully assisting the Police in the criminal investigation. The REO will also conduct an internal investigation. Shall there be any evidence of breach of internal administration codes or any regulations, the REO will take disciplinary action in accordance with the established procedures.

26. Once again, the REO sincerely apologises for any distress caused to the electors by the incident. The REO will implement the improvement measures as mentioned above so as to ensure that no similar incident will happen again.

Registration and Electoral Office
April 2017