LCQ5: Leakage of personal data by commercial organisations

Following is a question by the Hon Paul Tse and a reply by the Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, in the Legislative Council today (December 12):

Question:

Following the leakage of the personal data of more than 9 million passengers by Cathay Pacific Airways Limited, the Marriott International hotel group has also leaked the personal data of nearly 500 million customers worldwide. Besides, it was revealed that the website of TransUnion Limited (TransUnion), which holds the credit records and personal data of over five million members of the public, had serious information security loopholes. After obtaining the personal data of the Chief Executive and the Financial Secretary, reporters of a media organisation successfully impersonated them and obtained their detailed credit reports from the website. Some members of the information and technology sector have criticised that the identity verification procedure of the website is too lax, making the database therein a "doorless coop" which allows indiscriminate access by anyone, thereby giving lawbreakers opportunities to take advantage of the loopholes. Several members of the public have relayed that the successive occurrence of data leakage incidents has caused them to doubt whether commercial organisations are capable of protecting the security of their customers' data, and whether it is the case that the authorities can do nothing about the situation. In this connection, will the Government inform this Council:

(1) whether it knows the progress of the compliance check on TransUnion conducted by the Office of the Privacy Commissioner for Personal Data (PCPD); whether the scope of the compliance check, apart from TransUnion itself, also covers the personal data security protection for TransUnion's customers implemented by those organisations or companies which have business connections with TransUnion;

(2) given that at least five organisations are providing the public, in collaboration with TransUnion, free service of online enquiry of personal credit information, and some of the websites concerned have requested users to authorise TransUnion to transfer their data to its collaborating organisations or the overseas servers of such organisations, whether the authorities have regulated this type of data transfer; if not, of the follow-up actions; whether the authorities have assessed the impacts on the public when there is a leakage of personal data by the collaborating organisations of TransUnions or by their overseas servers; and

(3) as TransUnion's business is currently not subject to any regulation and PCPD can only deal with the situation after occurrence of incidents of personal data leakage, whether the authorities have assessed if the existing regulatory regime is tantamount to a "toothless tiger", not being able to

protect the personal data privacy of the public; whether the authorities will consider implementing new measures or enacting legislation to actively regulate such situation; if so, of the details; if not, the reasons for that?

Reply:

President,

On the question raised by the Hon Paul Tse, we have consulted the Privacy Commissioner for Personal Data (PCPD), the Hong Kong Monetary Authority (HKMA) and the Financial Services and the Treasury Bureau. Before responding to each parts of the question, I would first like to briefly describe the relevant background information on the arrangements relating to credit reference services.

TransUnion Limited (TransUnion) is an organisation providing credit reference services. In the mid-1990s, the HKMA conducted a study on the customer credit quality of authorised institutions and concluded that a comprehensive credit database with extensive participation of the authorised institutions should be established. The HKMA was of the view that the establishment of a full-fledged credit reference services in Hong Kong with the active participation of all authorised institutions (including licensed banks, restricted licence banks and deposit-taking companies) would allow all authorised institutions and the whole banking sector to better understand, and assess more accurately, the creditworthiness of their customers and better manage the overall credit risk in Hong Kong.

Following the implementation of the Personal Data (Privacy) Ordinance (PDPO) in 1996, in order to provide practical guidance for Credit Reference Agencies (CRAs) in Hong Kong, the PCPD issued the Code of Practice on Consumer Credit Data (Code of Practice) in February 1998 to regulate the handling of personal credit data by CRAs and credit providers. The Code of Practice covers areas on the collection, accuracy, use, security, access and correction of data. Four revisions have been made to it since then, with the latest revision made in January 2013.

As the regulatory authority of banks, the HKMA issued a circular to all authorised institutions in March 1998, suggesting the authorised institutions to participate comprehensively in the sharing and use of credit data through CRAs within the ambit of the Code of Practice. At the same time, the HKMA also stipulated that banks must comply with the relevant supervisory requirements set out in the HKMA's Supervisory Policy Manual (SPM) when providing CRAs with and using credit data. In accordance with the requirements, authorised institutions that use the service of a CRA should enter into a formal contractual agreement with the CRA that requires the CRA to formulate effective control systems to ensure that relevant provisions of the PDPO and the Code of Practice are complied with.

Our reply to the various parts of the question raised by the Hon Paul Tse is as follows:

(1) Upon receiving the data breach notification of TransUnion on November

28, 2018, the PCPD initiated a compliance check on the incident on the same day. In the light of information gathered from the check, the PCPD has reasonable grounds to believe that TransUnion has contravened the requirements under the PDPO. On November 30, the PCPD decided to launch an in-depth compliance investigation into TransUnion in accordance with section 38(b) of the PDPO. On the same day, the PCPD also conducted compliance check on five companies offering web platforms or mobile applications for access to the simplified version of credit reports.

The HKMA and the banking industry are highly concerned over the incident as the security of the personal credit information provided to TransUnion by banks may be involved. The HKMA jointly with the Hong Kong Association of Banks have immediately contacted TransUnion to ascertain the situation, and the Hong Kong Association of Banks and the banking industry have maintained close liaison with TransUnion over the past two weeks. A series of requirements have been raised to TransUnion, amongst which TransUnion has been requested to conduct a full investigation into the incident immediately and to suspend its online enquiry service on personal credit reports immediately until the completion of full investigation and comprehensive upgrade of information security to protect the personal credit information of authorised institutions. TransUnion has now suspended its online enquiry service on personal credit reports. The HKMA will continue to follow up on the matter with the Hong Kong Association of Banks, including requesting TransUnion to thoroughly review all relevant procedures and measures to ensure adequate protection in the collection, handling, storage, security and destruction of personal credit information to meet the security requirements of authorised institutions. The HKMA has also made notifications to the PCPD and expressed concern. The HKMA will continue to maintain close liaison with the PCPD.

(2) According to para. 3.21 of the Code of Practice issued by the PCPD, a CRA shall not transfer consumer credit data held by it to a place outside Hong Kong unless the purpose of use of the data transferred is the same as or directly related to the original purpose of the collection of such data. Irrespective of whether the personal data is stored in Hong Kong or overseas, or transferred to a data processor overseas to act on behalf of a data user, the data user must ensure that the personal data are dealt with properly in accordance with the requirements of the PDPO.

(3) Under the current legal framework, CRAs are not regulated by the HKMA. CRAs (including TransUnion) provide credit reference services to banks in Hong Kong and other credit institutions, and they shall comply with the relevant provisions of the PDPO and the Code of Practice. As the regulatory authority for banks, the HKMA requires banks to comply with the provisions of the PDPO when carrying out relevant businesses, to ensure that personal data of customers are properly safeguarded when providing data to and using the service of CRAs. An authorised institution using the service of any CRA must enter into a formal contractual agreement with the CRA that requires the CRA to formulate effective control systems for personal credit data. An authorised institution may consider whether to terminate its relationship with a CRA if it is aware of unacceptable practices of the CRA, or serious

breaches of the requirements of the PDPO or the Code of Practice.

According to paragraph 3.12 of the Code of Practice issued by the PCPD, a CRA shall take appropriate measures in protecting personal credit data in its daily operations to safeguard against any improper access to personal credit data held by it, including monitoring and reviewing on a regular and frequent basis the usage of the database, with a view to detecting and investigating unusual or irregular patterns of access or use, etc. In response to this incident, we will urge the PCPD to conduct a comprehensive review of the Code of Practice with reference to the findings of the compliance investigation upon its completion, and consider the need for further revisions to improve the operation of the Code.

Thank you, Acting President.