For discussion on
7 January 2019

Legislative Council Panel on Financial Affairs

Personal Data Protection Issues Relating to Credit Reference Agencies

Purpose

This paper briefs Members on the follow-up actions taken by the relevant government agencies and the Office of the Privacy Commissioner for Personal Data ("PCPD") in response to the recent incident concerning online security of consumer credit data maintained by the TransUnion Limited ("TransUnion"), an organisation providing consumer credit reference services.

Regulation of Consumer Credit Data

2. In Hong Kong, the protection of privacy of individuals with respect to personal data is underpinned by the Personal Data (Privacy) Ordinance ("PDPO") (Cap. 486) which came into force in December 1996. The PCPD is an independent statutory body set up to oversee the enforcement of the PDPO. To provide practical guidance for credit reference agencies ("CRAs") in Hong Kong, the PCPD issued a 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 the collection, accuracy, use, security, access and correction of data. It stipulates that a CRA shall take appropriate measures to protect 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. The

PCPD reviews the Code from time to time, and four revisions have been made since its promulgation, with the last revision effected in January 2013.

3. Banks, as credit providers and users of services of CRAs, are required to comply with the requirements of the PDPO and the Code of Practice in their sharing and use of customers' credit data through CRAs. The Hong Kong Monetary Authority ("HKMA"), as a regulator for banks, requires banks to have clear and comprehensive policies and procedures to ensure compliance with the requirements of the PDPO and the Code of Practice. For instance, to protect the confidentiality of CRA data, banks should establish a policy to safeguard customer data obtained from the CRA. Access to CRA credit reports should be granted on a need-to-know basis and there should also be restrictions on how such reports may be duplicated, copied or circulated.

Follow-up on Suspected Breach of the PDPO

4. TransUnion notified the PCPD on 28 November 2018 of a suspected data breach due to possible security loopholes in the application procedures for credit reports maintained by the company, with some personal data on the TransUnion database allegedly accessed by an unauthorised party. On the same day the PCPD took immediate steps to contact TransUnion, initiate a compliance check for fact-finding and assist TransUnion to take remedial actions in order to mitigate any possible losses. The PCPD also suggested TransUnion and the related credit agencies or intermediaries to suspend the application procedures in question, plug the suspected security loopholes, strengthen the authentication procedures and inform the affected individuals once they were identified.

5. Upon receipt of further information from TransUnion, the PCPD noted reasonable grounds to believe that there might be a contravention by the company of requirements under the PDPO. The PCPD decided on 30 November 2018 to commence a compliance investigation against TransUnion pursuant to section 38(b) of the PDPO. The investigation is currently ongoing. Separately, the PCPD has also

commenced compliance check on five companies offering web platforms or mobile applications for access to the simplified version of credit reports maintained by TransUnion.

6. Given that the incident involved the security of personal credit information provided to TransUnion by banks for credit reference purposes, the HKMA together with the Hong Kong Association of Banks liaised closely with TransUnion following the incident. Specifically, TransUnion has been requested to conduct a full and immediate investigation into the incident and to suspend the online enquiry services on personal credit reports until the completion of investigation, comprehensive upgrading of the information security system and an independent review on the enhanced security controls. TransUnion's relevant online services were suspended on 29 November 2018.

7. TransUnion reported the incident to the Police on 29 November 2018. The Cyber Security and Technology Crime Bureau of the Hong Kong Police Force has been investigating the incident and will take follow-up actions as appropriate. Special attention will be paid to cases suffering actual losses possibly due to the incident.

Review of PDPO and Code of Practice

8. Arising from an earlier data breach incident, the Government, in collaboration with the PCPD, is reviewing the relevant stipulations and penalties under the PDPO, and will seriously consider how the regulation of data protection, in particular with respect to data breach notification, could be enhanced. In connection with the TransUnion case, the PCPD will also conduct a comprehensive review of the Code of Practice with reference to the findings of the compliance investigation, and consider the need for further revisions to improve the operation of the Code.

Next Steps

9. The Government attaches great importance to the protection of personal data. The relevant government agencies and the PCPD will

spare no effort in investigating the incident while following up as appropriate having regard to findings from the investigation. Meanwhile, the Office of the Government Chief Information Officer will continue to collaborate with the Hong Kong Computer Emergency Response Team Coordination Centre to educate the public on cyber security issues and promote the adoption of best practices in different business sectors.

Financial Services and the Treasury Bureau
Constitutional and Mainland Affairs Bureau
Innovation and Technology Bureau
Security Bureau
Hong Kong Monetary Authority
December 2018