

Data Breach Incident Investigation Report

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

TransUnion Limited

Unauthorised online access to credit reports

Report Number : R19 - 17497

Date Issued: 9 December 2019

TransUnion Limited

**Data Breach Incident
Unauthorised online access to credit reports**

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (**Ordinance**) provides that “*the [Privacy] Commissioner [for Personal Data, Hong Kong] may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report -*

(a) *setting out -*

(i) *the result of the investigation;*

(ii) *any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and*

(iii) *such other comments arising from the investigation as he thinks fit to make; and*

(b) *in such manner as he thinks fit.”*

This investigation report is hereby published in discharge of the powers and duties under section 48(2) of the Ordinance.

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
9 December 2019

Table of Contents

Executive Summary.....	1
I. Introduction.....	4
II. Facts and Circumstances relevant to the Incident.....	9
III. Legal Issues and Regulatory Framework	27
IV. Views, Findings and Contraventions.....	36
V. Enforcement Action.....	45
VI. Comments	46
Appendix A: Extracts from TransUnion’s Privacy Policy	51
Appendix B: Information Displayed in Credit Reports Obtained from Online Platforms	54
Appendix C: Online Application for a Credit Report at TransUnion’s Website.....	56
Appendix D: Joint Operation between TransUnion and the Five Partners	59
Appendix E: Clauses 2.8 to 2.12 of the Code of Practice on Consumer Credit Data - Access by credit provider to consumer credit data held by CRA.....	82
Appendix F: Supervision of CRA and Credit Report Charges in Five Jurisdictions ..	85

Data Breach Incident Investigation Report

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

TransUnion Limited

Unauthorised online access to credit reports

Executive Summary

Background

On 26 November 2018, the Privacy Commissioner for Personal Data, Hong Kong (**Commissioner**) was informed by the local newspaper Ming Pao through email that it was able to pass through the online authentication procedures of TransUnion Limited (**TransUnion**) and obtain the credit reports of a number of public figures (**Incident**). On 28 November 2018, the Commissioner received a data breach notification (**DBN**) lodged by TransUnion in respect of the suspected unauthorised access. The Commissioner carried out a compliance investigation on 30 November 2018. (paras. 1-4)

At the time of the Incident, online application for and access to credit reports by individuals was available through TransUnion's website and its five partners' websites / mobile application. The five partners were (1) MoneyHero Global Limited (**MoneyHero**); (2) Mtel Limited (**Mtel**); (3) Standard Chartered Bank (Hong Kong) Limited (**Standard Chartered**); (4) i-Choice Limited (**i-Choice**) and (5) MoneySQ Limited (**MoneySQ**), (collectively, the **Five Partners**). (para. 16)

TransUnion set and verified the online authentication procedures for application for and access to credit reports, and applied the same procedures and standards across its own website and the Five Partners' websites / mobile application. It was TransUnion that made the authentication decision. (para.17)

The online authentication procedures covered (1) the matching of the full name, date of birth and Hong Kong Identity Card number inputted by the individual against TransUnion's database; (2) the assessment of the risk associated with the device used to access the system; (3) a set of three or five multiple choice knowledge-based authentication (**KBA**) questions; and (4) the sending of a one-time password (**OTP**) to the individual's mobile number for high risk cases. (para.18)

In the joint operation with the Five Partners, TransUnion used the personal data it held to authenticate an individual's identity and display the credit data at the website(s) / mobile application chosen by the individuals. TransUnion also transferred the individuals' personal data to MoneyHero, Mtel and Standard Chartered. (para. 40)

Views, Findings and Contraventions

As a data user and a Credit Reference Agency (**CRA**), TransUnion is required to comply with the six Data Protection Principles (**DPP**) of Schedule 1 to the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (**Ordinance**) and the guidelines under the Code of Practice on Consumer Credit Data (**Code**) issued by the Commissioner. (para. 60)

Data Use – Data Display and Transfer of Data to Partners – No Contravention

The Commissioner considers the use of personal data for identity authentication and display of credit data to the individual was a purpose consistent with the purpose for which the data was collected. The purpose of transferring personal data to MoneyHero, Mtel and Standard Chartered, on the other hand, did not fall within the original purpose or a directly related purpose for which TransUnion collected the concerned data, and such transfer would therefore call for the individual's prescribed consent as required under DPP 3(1) of Schedule 1 to the Ordinance (Data Use). The Commissioner went through the application procedures step by step. No contravention of DPP 3(1) of Schedule 1 to the Ordinance (Data Use) is found on such transfers. (paras. 80, 89 and 90)

Data Security – Vulnerabilities in Online Authentication Procedures

The Commissioner finds TransUnion contravened DPP 4(1) of Schedule 1 to the Ordinance (Data Security) in respect of its online authentication procedures in that it failed to take all practicable steps to ensure that the personal data held was protected against unauthorised or accidental access or use, on the grounds that (1) an exact

match of the full name and date of birth inputted by an individual against the records of TransUnion's database was not required; (2) the KBA used (a) questions that asked about the age range and Chinese zodiac sign of the individuals instead of unique dealings with TransUnion, and (b) outdated answers that could be easily screened out; (3) access through other websites / mobile application was not blocked after an individual failed the authentication procedures on one website / mobile application; and (4) two-factor authentication was not applied to all applications. (paras. 96-105)

Enforcement Action

The Commissioner exercises his power pursuant to section 50(1) of the Ordinance to serve an Enforcement Notice (**EN**) on TransUnion directing TransUnion to remedy and prevent any recurrence of the contravention in relation to data security. (paras. 111 and 112)

I. Introduction

1. On 26 November 2018, the Commissioner was informed by the local newspaper Ming Pao through email that it was able to pass through the online authentication procedures of TransUnion and obtain the credit reports of a number of public figures by inputting their names, dates of birth, Hong Kong Identity Card numbers (which were available from public sources), email addresses and phone numbers, and answering three simple questions.
2. On 28 November 2018, upon receipt of a DBN from TransUnion in respect of suspected unauthorised access, the Commissioner commenced a compliance check against TransUnion forthwith to find out the facts¹. The Commissioner appealed to TransUnion and other companies concerned² to suspend the application procedures in question, plug the suspected security loopholes, review the authentication procedures and inform the affected individuals once they were identified.
3. On 29 November 2018, TransUnion suspended its online credit report ordering services.
4. On 30 November 2018, the Commissioner, based on the test findings of the online authentication procedures and the actions taken by TransUnion, had reasonable grounds to believe that there might be contravention of the requirements under the Ordinance, and commenced a compliance investigation against TransUnion, pursuant to section 38(b)³ of the Ordinance in relation to the Incident.

¹ See media statement of 28 November 2018 entitled “Privacy Commissioner Receives Credit Data Breach Notification” (https://www.pcpd.org.hk/english/news_events/media_statements/press_20181128.html).

² These were companies that offered online access to credit reports. Please see paragraph 5 for the names of the companies.

³ Section 38 of the Ordinance provides that “*Investigations by Commissioner - Where the Commissioner (a) receives a complaint; or (b) has reasonable grounds to believe that an act or practice (i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user; (ii) relates to personal data; and (iii) may be a contravention of a requirement under this Ordinance, then (i) where paragraph (a) is applicable, the Commissioner shall, subject to section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in the complaint is a contravention of a requirement under this Ordinance; (ii) where paragraph (b) is applicable, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice referred to in that paragraph is a contravention of a requirement under this Ordinance.*”

(<https://www.elegislation.gov.hk/hk/cap486!en@2013-04-25T00:00:00/s38?elpid=153325>)

5. Separately, the Commissioner also commenced compliance checks on five companies offering websites / mobile application for online access to the simplified version⁴ of credit reports maintained by TransUnion on the basis that the same online authentication procedures applied. The five companies were CompareAsia Group Limited (CAG) (being the parent company of MoneyHero), Mtel, Standard Chartered, i-Choice and MoneySQ.

The Legislative Council Meeting

6. The Panel on Financial Affairs of the Legislative Council, Hong Kong Special Administrative Region discussed “*Personal data protection issues relating to credit reference agencies*” at a meeting on 7 January 2019 (**Panel Meeting**). Members of the Panel on Constitutional Affairs and the Panel on Information Technology and Broadcasting were invited to join.
7. In the written submission⁵, TransUnion gave a brief account of its services, business model and the Incident, as extracted below:-

“... TransUnion has been serving Hong Kong financial institutions and the people of Hong Kong for over 30 years...”

We provide credit reports and credit education to the people of Hong Kong. This information helps individuals be financially responsible and to make informed financial decisions.

We also provide every major consumer financial services institution in Hong Kong with consumer credit information that enables them to have the confidence to lend to people and take efficient, risk-based decisions across the consumer credit lifecycle, from acquisition, underwriting, identity verification, to portfolio management and collection. TransUnion’s services help support a strong, healthy and stable Hong Kong credit economy. This consumer credit information, combined with the analytics we also provide to financial institutions, facilitates financial inclusion by giving these institutions the confidence to bring under-served people into the credit economy...

⁴ The credit report obtained through the websites / mobile application of the five companies contained less information than the credit report obtained through TransUnion’s website. Please refer to **Appendix B** for the items of information obtained through TransUnion and the five companies.

⁵ <https://www.legco.gov.hk/yr18-19/english/panels/fa/papers/fa20190107cb1-403-1-e.pdf>

An instance of unauthorised access to our online consumer platform was recently reported in the media. Upon learning of the issue, we immediately alerted the relevant authorities and government departments and increased security layers across our online system. This incident is not a data leak; it was a focussed and intentional incursion. We regret that our platform was accessed in this way and have extended our apologies to the individuals concerned. We also regret any concern that this situation may have created among people in Hong Kong. We are working on several enhancements to the security measures on our online consumer services, which we have suspended in the meantime.

Our business model

As the unauthorised access incident relates to our consumer business model, we will explain this model now. TransUnion provides consumers access to their credit data through two channels: (1) directly by TransUnion and (2) indirectly through a select number of business partners.

We believe that enabling consumers to access their credit information is beneficial to the people of Hong Kong and the wider economy. When people have access to their credit, they are more educated, more empowered, and more likely to behave in a financially prudent way. For the economy, this helps to improve levels of financial literacy overall and promote smarter and more responsible borrowing by people.

TransUnion provides people in Hong Kong with direct access to their credit data through an online platform which it operates directly as well as an in-person service at TransUnion's office. Consumers can pay a one-time fee for their credit reports, or they can subscribe to an on-going service that allows them continuous access to their records, credit scores and features which help them understand and manage their credit.

Alternatively, a consumer can obtain his or her credit data online through our business partners. In Hong Kong, we work with five carefully-selected and credentialed business partners. Through these partners, people are offered another channel to access their credit information. These partners enable consumer access by subsidising the credit report for a consumer in exchange for the ability to contact, market, or match people with the best and lowest-cost financial products available to them based on their credit information. A

consumer's access to their report and agreement to be matched with relevant financial products is done with each individual's express consent.

We believe that these partner channels benefit people by giving them another option to access their credit information and understand how their credit history impacts their ability to access financial products, and by providing them tailored and targeted financial products to choose from.

TransUnion performs due diligence on business partners including the imposition of security requirements and the right to audit. Business partners are audited for their ability to meet TransUnion's standards and are continuously monitored between audits. Any risks identified are tracked for remediation, with governance processes to monitor progress at all levels of management.

In its dealings with consumers and business partners in Hong Kong, TransUnion is guided by the data protection principles in the Personal Data (Privacy) Ordinance and the Code of Practice on Consumer Credit Data under the Ordinance. We also receive a compliance assessment every year by an independent party for our handling of consumer credit data as a credit reference agency under Part III of the Code of Practice on Consumer Credit Data. The latest assessment resulted in a finding of "no relevant exception was noted". We are committed to the protection of consumer credit data, and we are continually reviewing and evolving our security measures to identify and combat increasingly sophisticated activities by criminals.

The unauthorised access incident

We were contacted on 26 November by the Ming Pao newspaper and informed that they had managed to secure unauthorised access to certain consumer credit records via our online platform. We immediately launched an investigation which was closely overseen by both our global and local leadership, in line with TransUnion's data issue response protocol. At the same time, we immediately implemented additional security measures, and we notified the Privacy Commissioner and affected individuals on 28 November. We also temporarily suspended our online services on 29 November.

Our investigation quickly established that over a period of about four weeks covering the last two weeks of October 2018 and the first two weeks of November 2018, a reporter from Ming Pao had compromised three consumer

identities through a combination of TransUnion's direct channel and its business partners.

In the interest of keeping our protocols secure, we are not making public further details about how the reporter navigated the security and other protocols that were in place. If the Panel would like to hear more about our investigations in private, then we would be happy to share our findings on a confidential basis.

We wish to assure the Panel and the public of Hong Kong that our investigations have found no evidence of other unauthorised access by the reporter and that our remedial actions should prevent such future attempts.

Remedial Actions

While our consumer online services remain suspended, we have already implemented additional security measures. In addition, we are re-verifying our existing customer base leveraging one-time passwords and an updated account enrolment process and also implementing a two-factor authentication for account login.

Furthermore, we have engaged a well-recognised, established and independent third party to conduct a review of our security and application architecture and implementation. The review report is estimated to take about 3-4 weeks and we will not resume our online system until the review is complete and we are satisfied that all relevant security issues have been addressed ...”

8. Up to the date of publication of this report, the Commissioner received 11 enquiries⁶ and two complaints⁷ from the public in relation to the Incident.

⁶ Primarily about dissatisfaction with the data breach and self-protection methods.

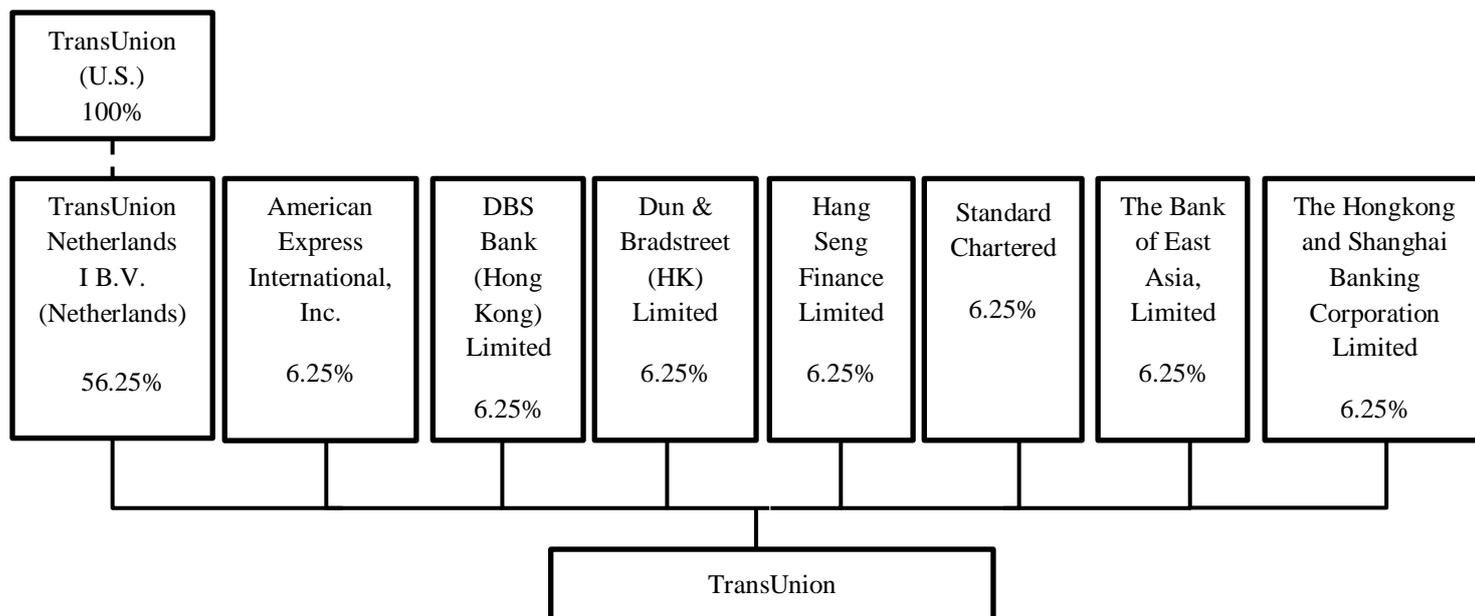
⁷ Primarily about the inadequate security measures taken by TransUnion.

II. Facts and Circumstances relevant to the Incident

9. In the course of the compliance checks and compliance investigation, the Commissioner reviewed the online application procedures for credit reports on TransUnion's website and the simplified version of credit reports on its partners' websites / mobile application, made enquiries with TransUnion and the five companies offering websites or mobile application for access to the simplified version of credit reports maintained by TransUnion, examined the documentary evidence referred to in the DBN, Panel Meeting and replies to the enquiries raised.

Background of TransUnion

10. TransUnion was a CRA incorporated and operating in Hong Kong. It held consumer credit records of over 5.5 million individuals as of 30 November 2018. The majority of its shares (56.25%) was held by TransUnion Netherlands I B.V., which was ultimately owned by TransUnion incorporated in the United States. The other seven shareholders, each holding 6.25% of the shares of TransUnion, were American Express International Inc., DBS Bank (Hong Kong) Limited, Dun & Bradstreet (HK) Limited, Hang Seng Finance Limited, Standard Chartered, The Bank of East Asia, Limited, and the Hongkong and Shanghai Banking Corporation Limited.



11. TransUnion collected personal data from credit providers (who subscribed to its consumer credit reference service), publicly available records and individuals. TransUnion provided credit reports to credit providers⁸ and individuals for a fee. It also worked with partners which facilitated individuals' access to credit reports. As of 30 November 2018, 145 credit providers subscribed to TransUnion's consumer credit reference service, 182,790 individuals maintained an active account for accessing credit report online, and five partners cooperated with TransUnion for allowing their customers / members to access credit reports online.
12. TransUnion's Privacy Policy⁹ was available online. It explained how TransUnion would collect, use and disclose the information about individuals that appeared in its database. Extracts from the relevant provisions in relation to the use of data, identification requirements, and security of data are at **Appendix A**.

Personal Data Affected

13. TransUnion's own investigation of the Incident revealed that Ming Pao had compromised the identities of three public figures, and made six attempts to access these three individuals' credit reports online directly from TransUnion and indirectly through the websites of MoneyHero, i-Choice and MoneySQ during the period from 30 October 2018 to 18 November 2018. TransUnion found no evidence of attempting to access credit reports through the website of Standard Chartered and mobile application of Mtel by Ming Pao.
14. A typical credit report on an individual obtained online directly from TransUnion contained the following information:-
 - (1) personal information (i.e. name, Hong Kong Identity Card number, address and contact number);
 - (2) credit score (i.e. grade, numeric score and score factors);

⁸ Credit reports had been provided to (a) banks and background check agencies for the purpose of background or employment check since September 2008; and (b) mortgage insurance companies for mortgage application since February 2009.

⁹ <https://www.transunion.hk/legal/privacy-policy>

- (3) credit account information (i.e. credit providers, credit account numbers, repayment history records, credit limits, outstanding balances, past due history records and hire-purchase information on vehicles, vessels and equipment);
 - (4) credit applications and other enquiry information (i.e. credit providers, dates of enquiry, account types and credit amount); and
 - (5) public records of potential relevance (i.e. case number, date, court and address shown in the court writ, petition and individual voluntary arrangement records).
15. Credit reports obtained through the other five websites / mobile application were simplified version which contained only some of the information listed above. A table listing the information displayed in credit reports obtained through TransUnion and the five websites / mobile application is at **Appendix B**.

Online Authentication Procedures

16. At the time of the Incident, online application for and access to credit reports by individuals was available through TransUnion's website and its Five Partners' websites / mobile application. The Five Partners were (1) MoneyHero; (2) Mtel; (3) Standard Chartered; (4) i-Choice; and (5) MoneySQ. The application procedures at TransUnion's website are at **Appendix C**, and a summary of TransUnion's joint operation with each of the Five Partners as well as the related application procedures are at **Appendix D**.
17. TransUnion set and verified the online authentication procedures for application for and access to credit reports, and applied the same procedures and standards across its own website and its partners' websites / mobile application. It was TransUnion that made the authentication decision.
18. The online authentication procedures covered:
- (1) the matching of the full name, date of birth and Hong Kong Identity Card number inputted by the individual against TransUnion's database, which contained credit information that TransUnion had collected from credit providers, publicly available records and individuals. Generally speaking,

individuals who had applied for credit with credit providers before would have their personal data kept in TransUnion's database;

- (2) the assessment of the risk associated with the device used to access the system. The assessment was first based on the risk rating of the device itself, for example, whether it had been jail-broken (restrictions placed by the device manufacturer had been removed) or whether it was coming from a high risk country. The second sets of rules checked the device against bad databases of IPs and device ID (a proprietary digital fingerprint TransUnion created on smart device). The third sets of rules check for behaviour anomalies such as high velocity of transactions from the same device;
 - (3) KBA which asked the individual three or five multiple choice questions. The degree of difficulty of the questions were based on the assessment results of procedures (1) and (2) above; and
 - (4) the sending of a OTP to the individual's mobile number for high risk cases.
19. TransUnion confirmed that short message service (SMS) forwarding of OTPs had been blocked¹⁰.
20. TransUnion was asked to elaborate on the security assessment and privacy impact assessment carried out before implementing its authentication procedures. TransUnion claimed that they had conducted a "*Service and Technology Assessment Review*", which was intended to identify and manage legal, regulatory, financial, business and other kinds of risks, and the process included a review of compliance with all applicable laws and regulations, including all consumer-reporting and consumer-privacy laws, consent decrees, contract law, and other application restrictions, as well as all applicable TransUnion obligations specified in agreements with customers, vendors and other third parties. A copy of the result of the "*Services and Technology*

¹⁰ The media reported in February 2019 that three Stored Value Facility Licensees did not block SMS forwarding of OTPs. When SMS forwarding service was activated, the telephone operators would deliver SMS OTP messages originating from these three Stored Value Facility Licensees to both the individual's registered mobile phone number and another mobile phone number under the SMS forwarding service. Hong Kong Monetary Authority subsequently required all Stored Value Facility Licensees to block SMS forwarding of OTPs. Given that TransUnion would send OTPs to the individual's mobile number for high risk cases, the Commissioner therefore enquired TransUnion whether it had blocked SMS forwarding of OTPs.

Assessment Review” on its authentication solution was provided as supporting evidence.

21. In the present case of credit reports being accessed by Ming Pao, TransUnion found that Ming Pao had made six attempts to access the credit reports of the three public figures. In each of the six attempts, Ming Pao submitted the three public figures’ correct names, dates of birth and Hong Kong Identity Card numbers and was given three KBA questions to answer. Ming Pao answered two questions correctly in the first five attempts and all of the three questions correctly in the sixth attempt, namely:
 - (1) What type of credit card (in Hong Kong dollar) do you have with the following financial institutions?
 - (2) Please select the following financial institutions (please choose all correct answers) you are engaged with in terms of credit card services (in Hong Kong dollar):
 - (3) What is your age today?
 - (4) What type of credit card (in Hong Kong dollar) did you close with the following financial institutions over the past six months?
 - (5) What are the last four digits of your credit card (in Hong Kong dollar)?
22. Ming Pao attempted to compromise six identities but was only able to access data of three individuals, access to the remaining three having been denied. Subsequently, TransUnion sent written notifications about the unauthorised access to credit report to each of the three affected individuals on 28 November 2018 and 1 December 2018.
23. The Commissioner went through the online application procedures on TransUnion’s website and the Five Partners’ websites / mobile application for 20 times from 26 to 28 November 2018 with the aim to understand the information required for online application for and access to credit report and obtaining the KBA questions and possible answers generated in the process. The tests revealed that as long as the correct name and Hong Kong Identity Card number were inputted, a set of three or five KBA questions would be generated regardless of whether the inputted date of birth or mobile number was

correct or not. Out of the 20 trials, three were blocked from proceeding to the KBA stage after the input of incorrect Hong Kong Identity Card number and / or name. Credit report was obtained despite the fact that one question was answered incorrectly.

24. Based on the Commissioner's test results and the responses from TransUnion, the online authentication procedures had the following features at the material time:
- (1) A mismatch of name and data of birth inputted by an individual against TransUnion's database did not prohibit him from proceeding with the application for a credit report, although the number and difficulty of the subsequent KBA questions would be increased;
 - (2) The generated KBA questions¹¹ included those relating to the general particulars of an individual instead of unique dealings with TransUnion, for example, the age range, the Chinese zodiac sign, the last four digits of mobile phone number of the individual. TransUnion explained that *"we might be asking phone number and address associated with the applicant in the past (and not the current phone number) which made it harder for someone other than the applicant to know"*;
 - (3) TransUnion admitted that the decoy answers were generated from an outdated subscriber list. The list was last updated in July 2014. For example, in the Commissioner's test in November 2018, Bell-Net Finance Co., Limited, which was no longer a card issuing institution at the material time, was included as a possible answer to a question on institutions issuing credit cards with the highest credit limit;
 - (4) TransUnion confirmed that in order to pass the KBA examination, two out of three questions would need to be answered correctly for low risk individuals, and three out of five questions would need to be answered correctly for medium or high risk individuals;

¹¹ TransUnion submitted to the Commissioner a full list of KBA questions, which were not disclosed in this report for security reasons.

- (5) Accessing credit reports through other websites / mobile application was possible even after an individual failed the authentication procedures on one website / mobile application;
- (6) OTP did not apply in cases where TransUnion classified as medium or low risk. Based on the figures from October to December 2018 provided by TransUnion, OTP was not required for over 70% of transactions;
- (7) OTP, if applied, would be sent to the number supplied by the individual as long as it matched with the one in TransUnion's database, be it a current or a past contact number;
- (8) Following initial authentication, the individual would be able to login to his account with a username and password he decided each time he visited TransUnion's website (or a partner's website / mobile application). The username and password would be set by the individual and the password must comprise eight to 40 characters, containing at least one number and one letter.

25. After the Incident, TransUnion proposed the following security enhancements:

- (1) require an exact match of the inputted name, Hong Kong Identity Card number and date of birth with the records in TransUnion's database;
- (2) use a global network of five billion devices and more than 100 device attributes¹² including OS¹³ version, Kernel¹⁴, MAC address¹⁵, etc. in the device verification solution;
- (3) verify the last eight digits of an active credit card (the last four digits are masked in all credit reports previously delivered by TransUnion to individual applicants);

¹² An attribute represents specific information about the state of a device.

¹³ OS, or operating system, is a software that communicates with the hardware and allows other programs to run. Examples include Windows, macOS.

¹⁴ Kernel is an essential centre of a computer's operating system, communicating with hardware and managing resources.

¹⁵ MAC address, or media access control address, is a hardware identification number that uniquely identifies each device on a network.

- (4) increase the number of correct answers required to pass the KBA¹⁶;
 - (5) remove KBA questions that asked about the Chinese zodiac sign and age as these questions could be inferred from the date of birth;
 - (6) update the subscriber lists from which the decoy answers are generated every three months;
 - (7) limit the number of failed attempts to no more than once in 90 days across its own website and partners' websites / mobile application;
 - (8) adopt two-factor authentication for returning users¹⁷ by looking at the device fingerprint each time an individual logs in and determines if it is the same device that is returning or a new device. If it is a new device, TransUnion would carry out OTP verification;
 - (9) apply OTP verification for new user authentications and existing user re-authentications. If the mobile number provided by the individual does not match with the records of TransUnion's database, the individual must input the last eight digits of credit card number correctly if the device risk is deemed to be low. If the device risk is medium or high, he would need to apply for credit report in person; and
 - (10) send OTP only to the latest mobile number contributed by credit providers who subscribe to TransUnion's credit reference service.
26. TransUnion stated that it had (since the Incident) engaged a third party to perform a security assessment of its online authentication mechanism, which covered architectural design review and penetration testing exercise, and remediated all observations identified by the third party. A copy of the security assessment report was submitted to the Commissioner (Details are not disclosed in this report for sensitivity reasons).
27. Incidentally, the public raised after the Incident whether TransUnion would shift from multiple choice questions to "fill in the blanks" questions, and would

¹⁶ The exact number of correct answers required is not disclosed in this report to protect the security of the system.

¹⁷ Returning users refer to users who had successfully passed the online authentication procedures and then login again.

deploy more unique questions, such as the customer's favourite colour. TransUnion responded that *"The use of multiple choice questions for KBA is a recognized standard and best practice; and consumers are used to it..."* and they *"can only derive questions and answers based on data available in our database as furnished by members. The answers of those suggested questions are not available to TransUnion and could not be used to confirm the consumer's identity."*

28. In response to the public's suggestion of the adoption of multiple ways of identity verification made after the Incident, such as the use of biometric authentication, TransUnion stated that *"We already have multiple layers of verification that the user needs to go through (velocity checks, device verification, IDV¹⁸ checks, KBA questions). We will continue to monitor the service after re-launch and consider other authentication mechanisms including biometric authentication as part of our on-going commitment to information security."*

Joint Operation between TransUnion and the Partners

29. The five commercial agreements concerning online access to credit reports by individuals at partners' websites / mobile application at the relevant time could be classified into two types:
- (1) Strategic Services and Licensing Agreement - the agreements with MoneyHero and Mtel fell within this category. These two companies were not authorised institutions¹⁹ or a moneylender, and therefore did not fall within the definition of "credit providers" as defined in Schedule 1 to the Code ; and
 - (2) CreditView Dashboard Agreement - the agreements with Standard Chartered, i-Choice and MoneySQ fell within this category. These three companies were "credit providers" as defined in Schedule 1 to the Code.
30. Common features between the two types of agreements included:

¹⁸ IDV stands for identity verification.

¹⁹ According to section 2(1) of the Banking Ordinance (Cap 155), *"an authorized institution means (a) a bank, (b) a restricted licence bank; or (c) a deposit-taking company"*
(<https://www.elegislation.gov.hk/hk/cap155?pmc=0&m=0&pm=1>)

- (1) TransUnion could receive fees from all the Five Partners based on the numbers of individuals who subscribed to the online credit report service and authentication requests to verify the identity of individuals who applied for such service for the first time;
- (2) the partners could not charge the individuals in providing the products / services of TransUnion²⁰. The practical effect was that the individuals could gain “free” access to their own credit reports derived from TransUnion. In exchange, the individuals’ data would be shared with three partners, namely MoneyHero, Mtel and Standard Chartered. No individuals’ data would be shared with the other two partners, namely i-Choice and MoneySQ; and
- (3) TransUnion and the Five Partners were independent contractors and no principal-agent relationship arose from the agreements. They were responsible for their own respective acts.

Strategic Services and Licensing Agreement

31. Under the operation of this type of licensing agreement, TransUnion did not host the user interface, website or mobile application. Its role was limited to providing consumer credit information to the partners only upon requests of the partners accompanied with individuals’ written consents in prescribed form as set out in the agreements²¹. The partners solely hosted the websites / mobile application for individuals to request and receive their credit information²² and were licensed by TransUnion to use the consumer credit data. As a result, an individual would authorise the two partners (i.e. MoneyHero or Mtel) to be his representative to obtain the relevant credit report from TransUnion. The partners approached TransUnion directly acting on behalf of the relevant individuals.

²⁰ Such restriction was stated in TransUnion’s agreements with i-Choice, MoneySQ, Standard Chartered and MoneyHero, but not in the agreement between TransUnion and Mtel, though Mtel did not charge its customers for the credit report either.

²¹ Clause I provides “*Company may request from TU on behalf of, and with the written consent of, consumers certain product features (the “offering”), consisting of the features set forth in Exhibit B in accordance with the Workflow set forth in Exhibit D hereto (the “services”) to display to the subject Consumer certain Consumer Credit Information as defined below while the Consumer is using Company’s [Service/website] and in accordance with the Consumer Written Consent and for no other purposes.*”

²² Clause II(G) provides “*The Offering shall be hosted by Company only*”.

CreditView Dashboard Agreement

32. Under this types of agreement, TransUnion was responsible for hosting, developing and managing a white-labeled²³ online credit monitoring platform for consumers known as “CreditView Dashboard” (**Dashboard**) including user enrollment, authentication process, content, etc.
33. Although the three partners concerned (i.e. Standard Chartered, i-Choice and MoneySQ) did not have a role in managing or hosting the Dashboard, they might choose their own logos and colours to be shown on the Dashboard and email to individuals to integrate this service with their brands and other services²⁴. The partners concerned provided a link in their websites to allow individuals to go to the welcome page of the Dashboard at no charge²⁵ and procured individuals to agree to all terms and conditions of the Dashboard²⁶. Before going to the welcome page of the Dashboard, individuals should have accepted the Dashboard’s terms of use and privacy policy. The individuals would then log into the Dashboard (managed by TransUnion) in their own capacities and access their own credit-related information.
34. The Dashboard’s terms of use expressly stated that the Dashboard was provided by TransUnion and the collection, use and disclosure of personal information will be in accordance with TransUnion’s privacy policy.
35. On the welcome page of the Dashboard (managed by TransUnion from here onwards), new users provided their personal data to TransUnion for enrollment and authentication while existing users submitted their usernames and passwords for login.
36. The agreements provided that the Dashboard “*shall only be used by or on behalf of the Consumer for whom it was requested*”. In other words, the

²³ White-labeled means non-branded.

²⁴ The agreement recital provides “*Company desires to offer certain financial services including CreditView to consumers (“Consumers”) using services offered by TU including without limitation all amendments thereto in order for TU to make available to Company, for the benefit of Company’s Consumers, a website that presents Consumers with credit information labeled with Company’s brand, integrated with Company’s website, and to be used by Consumers*”.

²⁵ The agreement provides “*Company shall provide to its Consumers (i) a free offer to the CreditView Dashboard, (ii) applicable terms and conditions for acceptance and enrollment in the CreditView Dashboard as specified by TU, and (iii) all necessary information for enrollment in the CreditView Dashboard. Company shall make the CreditView Dashboard available to Consumers at no charge.*”

²⁶ The agreement provides “*Company shall procure Consumer to agree to all terms and conditions under the schedules hereunder...*”.

individuals directly accessed their own credit-related information from TransUnion through the Dashboard. The partners had no role in this process.

37. Upon successful registration and verification, the Dashboard would display product features to the individuals as set out in **Appendix B**.
38. According to this type of Dashboard agreements, TransUnion should provide monthly reporting on, inter alia, enrollment subscriber details including the individuals' names, emails, addresses / phone numbers, etc. to the three partners. TransUnion clarified that the *“Monthly reports on dashboard utilization and subscriber counts do not include any personal information”*.

Types of Personal Data collected by the Partners

39. Individuals would need to first register as members on four out of the Five Partners' websites / mobile application in order to access their credit data. The table below summarises the types of personal data collected by the partners through membership registration and through TransUnion:

	MoneyHero	Mtel	Standard Chartered	i-Choice	MoneySQ
Types of personal data required for membership registration	Name, Hong Kong Identity Card number, date of birth, email address and mobile number	Email address	N/A	Mobile number and email address	Name, mobile number, email address and contact address
Types of personal data obtained from TransUnion	Name, address, mobile number, Hong Kong Identity Card number, credit data (including grade and numeric score, score factors, hire-purchase / leasing account, instalment account, charge card, credit card, revolving account, mortgage,	Credit data (including grade and numeric score, hire-purchase / leasing account, instalment account, charge card, credit card, revolving account)	Name, mobile number and first letter of Hong Kong Identity card number	N/A	N/A

	enquiries, public record and credit overview)				
Number of individuals whose personal data was transferred from TransUnion to the partner	15,868	30,889 ²⁷	2,582	N/A	N/A

Consent to the Use of Personal Data

40. In the joint operation with the Five Partners, TransUnion used the personal data it held to authenticate the individual’s identity and display his credit data at the website(s) / mobile application chosen by the individuals. TransUnion also transferred the individuals’ personal data to MoneyHero, Mtel and Standard Chartered. TransUnion explained that *“From the perspective of indirect means of providing consumer reports via other platforms or providing reports for other uses, all our business operations are in strict compliance with [Data Protection Principle 3 of] the Ordinance and [Clauses 3.8 and 3.10 of] the Code. Consumer consent is obtained in every case prior to transfer to or access from another platform or use not originally anticipated.”* The relevant consent languages presented in each of the Five Partners’ platforms are explained below:

(1) MoneyHero

41. An individual who would like to access his credit report through the MoneyHero’s CreditGo²⁸ website would need to first register as a member, and then click a checkbox stating *“By joining you confirm that you agree to sharing your information with TransUnion, and that you have read, understand and agree to CreditGo Terms & Conditions [HYPERLINK], Privacy Policy [HYPERLINK] and this Consent Agreement [HYPERLINK]”* before accessing a free credit report.

²⁷ The applicable agreement between TransUnion and Mtel at the relevant time of the Incident was entered in February 2018, and a total of 30,889 individuals’ personal data was transferred to Mtel under that agreement. Before this agreement, TransUnion and Mtel had entered into another agreement in May 2016, and a total of 86,028 individuals’ credit data was transferred to Mtel under that previous agreement.

²⁸ CreditGo is the brand of MoneyHero.

42. To view the full texts of “*Terms & Conditions*”, “*Privacy Policy*” and “*Consent Agreement*”, the individual would need to click the hyperlinks.

43. The “*Consent Agreement*” stated that “*By submitting this registration form/clicking on the “I Accept” button below, I understand that I am providing written consent to:*

(I) *CreditGo, which is owned and operated by CompareAsia Group Limited (the “Company”) requesting and receiving on my behalf from TransUnion Limited (“TransUnion”) all or part of my consumer credit data which may be held in the database of TransUnion from time to time (“My Credit Data”);*

(II) *TransUnion transferring all or part of My Credit Data, including but not limited to my consumer credit report and credit score, to the Company’s server located in the Republic of Singapore for the purpose of displaying My Credit Data to me on the Company’s website, or as otherwise described in the Company’s Privacy Policy and Terms & Conditions; and*

(III) *the Company transferring/sharing all or part of My Credit Data as well as ancillary data derived from or relating to My Credit Data to/with the Company’s affiliated companies and third parties that provide services to the Company in connection with My Credit Data.”*

44. The individual could proceed with the application for credit report without clicking the hyperlink to view the Consent Agreement.

(2) Mtel

45. An individual who would like to access his credit report through Mtel’s CreditCheck mobile application would need to first create an account and then click the checkboxes stating:

“ *By clicking on the “I Accept and Continue” button below, I understand that I am providing written consent for Mtel Limited to transmit the above information to TransUnion Limited and to request and receive all or part of my consumer credit data which may be held in the database of TransUnion Limited from time to time (“My Credit Data”), including but*

not limited to information in my consumer credit report and credit score. I hereby authorize TransUnion Limited to transfer My Credit Data including the score to Mtel Limited for the purpose of displaying My Credit Data and the credit score to me while I am using this website or application.

Further, I authorize Mtel Limited to retain My Credit Data and the credit score for so long as I have an active Credit Check account for the purpose of displaying the history of My Credit Data and the credit score for my own reference.

I hereby give my consent to and authorize TransUnion Limited to access all or part of My Credit Data and to:

(i) match all or part of My Credit Data against the information I have provided to Mtel Limited on this page; and

(ii) generate questions directly or indirectly from any or all of the information contained in My Credit Data whether on its own or in conjunction with other source of information, collect responses to such questions from me and match such responses against any information contained in My Credit Data, for the purposes of verifying my identity. I agree that TransUnion Limited may receive and then process, use and transfer the result of the verification or any data arising therefrom to Mtel Limited via this app.

I further acknowledge and agree that the access, transfer, process and use of My Credit Data by TransUnion Limited in the manner described above shall not be made the basis upon which any complaint, claim, suit, demand or cause of action or other proceedings will be made against TransUnion by me. ”

46. Mtel terminated the mobile application on 29 November 2018 and confirmed that it had deleted all personal data (including credit data) obtained through the cooperation with TransUnion.

(3) Standard Chartered

47. An individual who would like to access his credit report through Standard Chartered's website would need to agree to the consent clauses below:

"I understand that by clicking on the "I Accept & Consent" button below, I am providing "written consent" to TransUnion Limited ("TU") authorizing TU to obtain information from my personal credit profile from the database of TU solely for the purposes of confirming my identity, retaining and displaying my credit data to me.

I acknowledge that I have read the Service Agreement [Hyperlink], Terms of Use [Hyperlink] and Privacy Policy [Hyperlink], and agree to their terms.

I acknowledge that I have read the Terms and Conditions [Hyperlink] of CreditView and agree to their terms.

- I understand that this service is paid by Standard Chartered Bank (Hong Kong) Limited (the "Bank").*

I am interested in the personal loan products of the Bank and agree to have TransUnion transferring my personal details (including name, mobile phone number and the first letter of the Hong Kong Identity Card) to the Bank and consent to have the Bank contacting me for the purpose of introducing its Personal Loan product(s) to me.

I understand that this service is solely provided by TransUnion and by using this service, TransUnion will not share my credit data with the Bank. For the avoidance of doubt, this consent is given once and will not override my existing direct marketing preference with the Bank.

*TransUnion and the Bank are independent of each other with no alliance formed. If, however, I do not wish for TransUnion to transfer my personal details to the Bank, I can choose **not** to press "I Accept & Continue" and I understand that I have the option of accessing my credit data for a fee which will be **payable by me**. I understand I can visit TransUnion's website for subscription details. I acknowledge that I have read and agree to the Bank's Privacy Policy".*

(4) i-Choice

48. An individual who would like to access his credit report through i-Choice's website would need to first register as a member and click the "I Accept & Continue" button to declare that:

"I understand that by clicking on the "I Accept & Consent" button below, I am providing "written consent" to TransUnion Limited ("TU") authorizing TU to obtain information from my personal credit profile from the database of TU solely for the purposes of confirming my identity, retaining and displaying my credit data to me.

I acknowledge that I have read the Service Agreement [Hyperlink], Terms of Use [Hyperlink] and Privacy Policy [Hyperlink], and agree to their terms."

(5) MoneySQ

49. An individual who would like to access his credit report through MoneySQ website would need to first register as a member and then click the "I Accept & Continue" button to make the same declaration as described above under the i-Choice website.

Security Requirements Imposed on Partners

50. TransUnion stated that it "performs due diligence" on partners. Based on the security assessment reports submitted, TransUnion accepted MoneyHero, Mtel, Standard Chartered and i-Choice as partners after considering the results of security assessment questionnaire²⁹ and security risk rating report³⁰.
51. No security assessment report on MoneySQ was submitted to the Commissioner. When asked to explain why no security assessment was carried out for MoneySQ, TransUnion referred the Commissioner to an internal document

²⁹ The security assessment questionnaire acted as "a framework and focused on information security safeguards related to TransUnion data and the services provided to TransUnion. TransUnion's Information Security policies and industry best practices were used as assessment criteria and included the following areas: policy, information systems, organization, incident response, asset management, human resources security, physical security, network architecture, operations management, access control, compliance, business continuity, sub-contractors and off shore services".

³⁰ The security risk rating report included "An overview of the company's Security Rating history and overall performance, Comparisons to industry averages and an in-depth analysis of the company's observe events, and current security standards on its servers".

about the engagement of MoneySQ, which stated that “*CreditView HK – is hosted and operated by TransUnion Hong Kong...This integrated solution allows consumers to see their credit information – in one web site...The credit information viewed is not stored and relevant data e.g. cookies, internet temp files, cached memory are all deleted once the session concludes.*” That document also marked “*Security Assessment Not Required*”.

52. TransUnion imposed additional Internet security requirements (e.g. specific standards of encryption on data in transit over the Internet; specific security measures for servers; firewalls and network connections) on MoneyHero and Mtel, which would receive credit data from TransUnion.
53. TransUnion claimed that the partners “*are continuously monitored between audits. Any risks identified are tracked for remediation, with governance processes to monitor progress at all levels of management*”. No record of audit carried out after the acceptance of partners was provided despite the fact that the joint operation commenced back in 2016.

III. Legal Issues and Regulatory Framework

The Ordinance

54. The Ordinance³¹, which came into force in December 1996, seeks to protect the privacy of individuals in relation to personal data. Its core provisions are encapsulated in the six DPPs³² set out in Schedule 1 to the Ordinance, although individual acts may be specifically regulated under the Ordinance. The object of the DPP is to create a framework regulating the handling of personal data during the entire life cycle of personal data beginning from collection to destruction.
55. There is no dedicated legislation or licensing requirement on CRA in Hong Kong.

Personal Data

56. “*Personal data*”, as defined in section 2(1) of the Ordinance, means “*any data* –
(a) relating directly or indirectly to a living individual;
(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(c) in a form in which access to or processing of the data is practicable.”

Data Subject

57. “*Data subject*” in relation to personal data, means the individual who is the subject of the data, as defined in section 2(1) of the Ordinance.

Data User

58. The Ordinance, including the DPP, aims to regulate the acts and practices of a data user being, as defined in section 2(1) of the Ordinance, “*a person who,*

³¹ <https://www.elegislation.gov.hk/hk/cap486>

³² The six DPPs are: 1) Data Collection Principle; 2) Accuracy and Retention Principle; 3) Data Use Principle; 4) Data Security Principle; 5) Openness Principle; and 6) Data Access and Correction Principle (https://www.elegislation.gov.hk/hk/cap486?xpid=ID_1438403263424_003)

either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data”.

The Code

59. In February 1998, the Commissioner issued the Code pursuant to section 12³³ of the Ordinance to regulate the handling of consumer credit data by CRAs and credit providers. The Code was subsequently revised four times after public consultations³⁴. A breach of the Code is not of itself a contravention of a requirement under the Ordinance, but will give rise to a presumption against the data user in any legal proceedings under section 13 of the Ordinance³⁵.
60. As a data user and a CRA, TransUnion is required to comply with the six DPPs of Schedule 1 to the Ordinance and the guidelines under the Code.
61. Under the Code, a CRA should engage an independent compliance auditor to conduct compliance audit. The purpose is to ensure that the CRA complies with the Ordinance and the Code in providing the consumer credit reference service,

³³ Section 12(1) of the Ordinance provides that “*Subject to subsections (8) and (9), for the purpose of providing practical guidance in respect of any requirements under this Ordinance imposed on data users, the Commissioner may (a) approve and issue such codes of practice (whether prepared by him or not) as in his opinion are suitable for that purpose; and (b) approve such codes of practice issued or proposed to be issued otherwise than by him as in his opinion are suitable for that purpose.*”

(<https://www.elegislation.gov.hk/hk/cap486/en@2013-04-25T00:00:00/s12?elpid=153325>)

³⁴ The public consultations received views from members of the public, political parties, members of the legal profession, public organizations, private organizations, professional bodies and associations representing various trades and industries.

³⁵ Section 13 of the Ordinance provides that “(1) *A failure on the part of any data user to observe any provision of an approved code of practice shall not of itself render the data user liable to any civil or criminal proceedings but where in any proceedings under this Ordinance a data user is alleged to have contravened a requirement under this Ordinance, being a requirement for which there was an approved code of practice at the time of the alleged contravention, subsection (2) shall have effect with respect to such code in relation to those proceedings. (2) Any provision of a code of practice which appears to a specified body to be relevant to a requirement under this Ordinance alleged to have been contravened shall be admissible in evidence in the proceedings under this Ordinance concerned and if it is proved that there was at any material time a failure to observe any provision of the code which appears to that body to be relevant to any matter which it is necessary to prove in order to establish a contravention of such requirement, that matter shall be taken as proved in the absence of evidence that such requirement was in respect of that matter complied with otherwise than by way of observance of that provision. (3) In any proceedings under this Ordinance, a code of practice which appears to a specified body to be the subject of a notice under section 12 shall be taken to be the subject of such notice in the absence of evidence to the contrary. (4) In this section – proceedings under this Ordinance includes any criminal proceedings where a data user is alleged to have committed an offence by reason of a contravention of a requirement under this Ordinance; specified body means (a) a magistrate; (b) a court; (c) the Administrative Appeals Board; or (d) the chairman of the Administrative Appeals Board.*”

(https://www.elegislation.gov.hk/hk/cap486?xid=ID_1438403261349_001)

including the security of data. The Commissioner has to approve and may elect to nominate the auditor³⁶.

62. The CRA has to submit the first compliance audit report to the Commissioner for consideration and approval. The Commissioner has to either (i) approve the report or (ii) direct the CRA to take the necessary steps to ensure better compliance, arrange for a further audit and resubmit the audit report³⁷.
63. After the first audit report is approved, the CRA has to subsequently conduct annual compliance audits on a continuous basis. The Commissioner has to consider the report submitted and make comments (if any)³⁸.
64. Apart from the above, the Code does not specify what action or measure the Commissioner must take in relation to compliance audit by CRA. The requirement to compile an audit report is recommended as a “best practice”.

³⁶ Clauses 3.14 of the Code provides that “As a recommended practice, a CRA shall engage, at its expense, an independent compliance auditor as may be approved (or, at the election of the Commissioner, to be nominated) by the Commissioner, to conduct regular compliance audits on the way in which the CRA provides the consumer credit reference service, including the security of consumer credit data held by the CRA in its database, and the adequacy and efficiency of the measures taken by it to comply with the requirements under the Ordinance and the Code.”

³⁷ Clause 3.15 of the Code provides that “The first of such compliance audit on the sharing of consumer credit data relating to mortgage loans shall commence after 6 months (in any event no later than 7 months) from 1 April 2011, which a view to having the compliance auditor submit its audit report to the Commissioner for his consideration within 3 months from the commencement of the compliance audit. Such compliance audit shall address, in particular, the compliance with the provisions of the Code and the adequacy of the data handling system of the CRA as far as the sharing of consumer credit data relating to mortgage loans is concerned.” Clause 3.16 of the Code provides that “If the Commissioner does not approve the first compliance audit report on the sharing of consumer credit data relating to mortgage loans provided to him, he may, by written notice to the CRA, direct the CRA to take such steps as may be considered necessary for ensuring better compliance with the requirement under the Code and/or the Ordinance, thereafter to arrange for a further compliance audit on the sharing of consumer credit data relating to mortgage loans to be carried out, and for such further audit report to be submitted to the Commissioner for his reconsideration within such period as the Commissioner may specify.”

³⁸ Clause 3.14B of the Code provides that “The CRA shall continue to arrange for compliance audits as referred to in clause 3.14 to be conducted at intervals not exceeding 12 months and, in each instance, for audit reports to be provided to the Commissioner for his consideration and/or comments within 3 months from the commencement of the compliance audit.” Clause 3.17 of the Code provides that “Upon the receipt of a notice from the Commissioner under clause 3.16, the CRA shall duly comply with the Commissioner’s directions, and clause 3.16 shall continue to apply to the CRA until the Commissioner gives his approval to a compliance audit report submitted. From the date of such approval onwards, the compliance audits on the sharing of consumer credit data relating to mortgage loans shall be conducted together with the regular audits referred to in clause 3.14B above.”

Consumer Credit Data

65. “Consumer credit data”, as defined in Part I of the Code, “means any personal data concerning an individual collected by a credit provider in the course of or in connection with the provision of consumer credit, or any personal data collected by or generated in the data base of a CRA (including mortgage count) in the course of or in connection with the providing of consumer credit reference service”.

CRA

66. “CRA”, as defined in Part I of the Code, “means any data user who carries on a business of providing a consumer credit reference service, whether or not that business is the sole or principal activity of that data user”.
67. “Consumer credit reference service” referred to above “means the service of compiling and/or processing personal data (including consumer credit scoring) for disseminating such data and any data derived therefrom to a credit provider for consumer credit purposes and, for performing any other functions directly related to consumer credit transactions” as defined in Part I of the Code.

Credit provider

68. “Credit provider” as defined in Part I of the Code, “means any person described in Schedule 1” which includes the following:
- “(1) an authorized institution within the meaning of section 2 of the Banking Ordinance (Cap 155)³⁹
 - (2) a subsidiary of an authorized institution within the meaning of section 2 of the Banking Ordinance (Cap. 155) (the term “subsidiary” shall have the same meaning as in section 2 of the Companies Ordinance, (Cap. 32)
 - (3) a money lender licensed under the Money Lenders Ordinance (Cap. 163)⁴⁰
 - (4) a person whose business (whether or not the person carries on any other business) is that of providing finance for the acquisition of goods by way of leasing or hire-purchase”

³⁹ See footnote 19.

⁴⁰ <https://www.elegislation.gov.hk/hk/cap163>

69. Credit providers may access consumer credit data held by CRA in accordance with clauses 2.8 to 2.12 of the Code⁴¹ (at **Appendix E**).

Data Use

70. DPP 3 of Schedule 1 to the Ordinance (Data Use) provides as follows:

“(1) Personal data shall not, without the prescribed consent of the data subject, be used for a new purpose.

...

*(4) In this section—
new purpose (新目的), in relation to the use of personal data, means any purpose other than—*

- (a) the purpose for which the data was to be used at the time of the collection of the data; or*
- (b) a purpose directly related to the purpose referred to in paragraph (a).”*

71. “use”, in relation to personal data, includes disclose or transfer the data, as defined in section 2(1) of the Ordinance.

72. According to section 2(3) of the Ordinance, “prescribed consent” referred to the above:

*“(a) means the express consent of the person given voluntarily;
(b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served).”*

73. Guidance to the use of consumer credit data by a CRA is set out in clauses 3.8 and 3.10 of the Code as follows:

⁴¹ Clauses 2.8, 2.9, 2.9A and 2.10A of the Code provide circumstances under which access to consumer credit data may be made by credit providers, clause 2.11 of the Code requires credit providers to confirm to CRA upon access, and clause 2.12 of the Code prohibits credit providers from accessing consumer credit data for direct marketing purpose.

(https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/CCDCode_2013_e.pdf)

“Providing of credit report

3.8 In response to the seeking of access by a credit provider to consumer credit data relating to an individual pursuant to clause 2.9, 2.9A or 2.10A⁴², a CRA may provide to the credit provider a credit report on the individual. The credit report may contain any of the consumer credit data relating to the individual permitted to be collected and retained by the CRA, subject to the following constraints which apply to particular categories of consumer credit data..... [Note 35: If a CRA uses any consumer credit data otherwise than in a way permitted under clause 3.8 or 3.10, this will give rise to a presumption of contravention of DPP3(1) under section 13(2)⁴³ of the Ordinance.]”

“Other uses of consumer credit data

3.10 In addition to disclosure in a credit report pursuant to clause 3.8, a CRA may, in providing a consumer credit reference service, use any consumer credit data relating to an individual held in its database [Note 37: For the consequence of a CRA using any consumer credit data in its database otherwise than in a way permitted under clause 3.10, see Note 35 to clause 3.8 above.]:

3.10.1 to provide notice and information to a credit provider on a watch list, when new data of the individual in default has appeared in the system, to assist in debt collection action;

3.10.2 to provide notice to a relevant credit provider and to the Transport Department where an individual who has received credit in relation to a motor vehicle has been the subject of advice from the Department that it has received an application from the individual for a duplicate vehicle registration document;

3.10.3 to provide a report to insurers in relation to insurance cover

⁴² Clauses 2.9, 2.9A and 2.10A of the Code provide the circumstances under which a credit provider may access consumer credit data held by the CRA. (see **Appendix E**) (https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/CCDCode_2013_e.pdf)

⁴³ See footnote 35.

for property related to a consumer credit transaction;

3.10.4 *for reasonable internal management purposes, such as the defence of claims and the monitoring of the quality and efficiency of its service; or*

3.10.5 *to carry out consumer credit scoring, provided that the CRA shall not, in carrying out such scoring, take into account:*

...

3.10.5.1A *in relation to an account other than a terminated account, any account data created more than 5 years before the carrying out of the scoring; or*

3.10.5.2 *in relation to a terminated account, any account data created more than 5 years before account termination.”*

Data Security

74. DPP 4(1) of Schedule 1 to the Ordinance (Data Security) provides that:

“All practicable steps shall be taken to ensure that any personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user is protected against unauthorized or accidental access, processing, erasure, loss or use having particular regard to

—

- (a) the kind of data and the harm that could result if any of those things should occur;*
- (b) the physical location where the data is stored;*
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;*
- (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and*
- (e) any measures taken for ensuring the secure transmission of the data.”*

75. “Practicable” is defined in section 2(1) of the Ordinance to mean “reasonably practicable”.

76. The “harm” test in DPP 4(1)(a) above calls for the consideration of whether the security measures undertaken by the data user with respect to the personal data

held were proportionate to the degree of sensitivity of the data and the harm that might result from unauthorised or accidental access to such data.

77. In respect of data security and system integrity safeguards, clause 3.12 of the Code provides guidance on the measures to take in daily operations as follows:

“3.12 A CRA shall take appropriate measures in its daily operations, including the following, to safeguard against any improper access to or mishandling of consumer credit data held by it [Note 39: If a CRA, in its daily operations, fails to take any of the measures required under clause 3.12 or 3.13⁴⁴ to safeguard against any improper access to or mishandling of the consumer credit data held by it, this will give rise to a presumption of contravention of DPP4(1) under section 13(2) of the Ordinance.]:

- 3.12.1 review on a regular and frequent basis its password controls which help to ensure that only authorized staff are allowed access to its database;*
- 3.12.2 monitor and review on a regular and frequent basis usage of the database, with a view to detecting and investigating any unusual or irregular patterns of access or use;*
- 3.12.3 ensure that practices in relation to the deletion and disposal of data are secure, especially where records or discs are to be disposed of off-site or by external contractors; and*

⁴⁴ Clause 3.13 of the Code provides:

“3.13 Without prejudice to the generality of clause 3.12 above, a CRA shall:

- 3.13.1 in the case of there being any suspected abnormal access by a credit provider, report such suspected abnormal access as soon as reasonably practicable to the senior management of the credit provider and to the Commissioner;*
- 3.13.2 maintain a log of all instances of access to its database by credit providers, which log shall include:
 - 3.13.2.1 the identity of the credit provider seeking access;*
 - 3.13.2.2 the date and time of access;*
 - 3.13.2.3 the identity of the individual whose data was so accessed;*
 - 3.13.2.4 the circumstances provided for in clause 2.8, 2.9, 2.9A or 2.10A under which the access has been made (as confirmed by the credit provider pursuant to clause 2.11.1);*
 - 3.13.2.5 in the case where the access has been made in the course of the review of existing consumer credit facilities under clause 2.9.1.2, 2.9A.2, 2.9A.4, 2.9A.5, 2.10A.2, 2.10A.3 or 2.10A.4, the specific matter or matters provided for in clause 2.9.3, 2.9.4 or 2.9.5 (as confirmed by the credit provider pursuant to clause 2.11.2); and*
 - 3.13.2.6 instances of reporting by the CRA of suspected abnormal access to the senior management of a credit provider and to the Commissioner,*
*and shall keep such a log for not less than 2 years for examination by its compliance auditor and/or by the Commissioner, as the case may be.”**

3.12.4 *Maintain a log of all incidents involving a proven or suspected breach of security, which includes an indication of the records affected, an explanation of the circumstances and action taken.”*

IV. Views, Findings and Contraventions

(I) Data Use

78. In TransUnion's joint operation with the Five Partners, it used individuals' personal data for identity authentication and display to the individuals. TransUnion also transferred personal data to three partners, namely MoneyHero, Mtel and Standard Chartered in the process.

(1) Identity Authentication and Data Display

79. TransUnion's joint operation with partners at the relevant time provided a channel for individuals to access their credit data via the partners' websites / mobile application. For this purpose, TransUnion used the individual's personal data for identity authentication and display at the website(s) / mobile application that the individual chose.

80. According to TransUnion's privacy policy, personal data in its credit database would be used "*to provide consumer credit information directly to consumers who have requested a copy of their Credit Reports, or to provide related services to consumers*". The Commissioner considers the use of personal data for identity authentication and display of credit data to the individual was a purpose consistent with the purpose for which the data was collected, and finds **no contravention of DPP 3 of Schedule 1 to the Ordinance (Data Use) in such use of personal data.**

(2) Transfer of Personal Data by TransUnion

81. As part of TransUnion's joint operation with partners at the relevant time, TransUnion transferred credit data of 15,868 individuals and 30,889 individuals to MoneyHero and Mtel respectively, the names, mobile numbers and the first letter of the Hong Kong Identity Card numbers of 2,582 individuals to Standard Chartered, but did not transfer any personal data to i-Choice and MoneySQ.

(2.1) *The transfer was not covered by the Code*

82. Clause 3.8 of the Code allows a CRA to provide a credit provider with a credit report on the individual under limited circumstances but does not cover the transfer of an individual's personal data to a credit provider (Standard Chartered

in this case) under commercial arrangements other than the provision of consumer credit reference service by a CRA.

83. Clause 3.10 of the Code lists other permissible uses of consumer credit data, which include the use of such data to provide notice and information to credit providers on a watch list, notice to the Transport Department and report to insurers.
84. According to note 35 of the Code, if, in the absence of any applicable exemption, a CRA uses any consumer credit data in its database otherwise than in a way permitted under clauses 3.8 and 3.10 of the Code, this will give rise to a presumption of contravention of DPP 3(1) of Schedule 1 to the Ordinance (Data Use).
85. The collection of consumer credit data by MoneyHero and Mtel from TransUnion for provision of credit monitoring service to individuals is currently not prohibited or regulated by the Code since they are not credit providers.

(2.2) *The transfer was not mentioned in TransUnion's privacy policy*

86. The transfer of personal data to partners is not expressly stated in TransUnion's privacy policy either, which states:

“2.1 We limit our use of consumers' personal information to those purposes which have been disclosed to consumers by our members, or for purposes which are otherwise permitted by the laws. We disclose personal information in compliance with the law primarily by means of Credit Reports to both consumer and members...”

2.6 We may disclose your personal information to third parties in the good faith belief that such action is necessary in order to comply with, or be responsive to, legal process served on us...

2.7 We may disclose your personal information to consultants, agents and advisors, such as attorneys and accountants, in the good faith belief that such disclosure is within the scope of their professional duties to TransUnion...”

87. In particular, the Commissioner considers that, by merely referring individuals to “*those purposes which have been disclosed to consumers by our members*”, the uses of personal data by TransUnion are too vague and broad, if not without limits at all.

(2.3) *The transfer was not necessary for accessing credit report at other channels*

88. No transfer of personal data took place in TransUnion’s joint operation with MoneySQ and i-Choice which also provided free access to credit reports at their websites. It was therefore technically feasible for TransUnion to allow individuals to have free access to credit reports at partners’ websites without transferring personal data.

89. The Commissioner considers that the purpose of transferring the personal data to MoneyHero, Mtel and Standard Chartered did not fall within the original purpose or a directly related purpose for which TransUnion collected the concerned data and such transfer for a new purpose would therefore call for the individual’s prescribed consent as required under DPP 3(1) of Schedule 1 to the Ordinance (Data Use).

90. To determine whether TransUnion contravened DPP 3(1) of Schedule 1 to the Ordinance (Data Use) in respect of the transfer of personal data to MoneyHero, Mtel and Standard Chartered, the Commissioner went through the application procedures step by step. **No contravention of DPP 3(1) of Schedule 1 to the Ordinance (Data Use) is found** on such transfers for the reasons below:

(1) TransUnion sought the prescribed consent for transfer of personal data to MoneyHero, Mtel and Standard Chartered through each of these websites / mobile application;

(2) the consent clauses adopted on the three websites / mobile application expressly stated the transfer and they required the online applicants to click the relevant boxes to indicate his consent to:

- “...*TransUnion transferring all or part of My Credit Data, including but not limited to my consumer credit report and credit score...*” (MoneyHero’s website);
- “...*transfer My Credit Data including the score to Mtel Limited...*” (Mtel’s mobile application);

- “...have TransUnion transferring my personal details (including name, mobile phone number and the first letter of the Hong Kong Identity Card) to the Bank” (Standard Chartered’s website); and

(3) prescribed consent, as defined in section 2(3) of the Ordinance, is express and voluntary consent. The prescribed consent should be sufficiently clear and specific to cover the particular transfer in question. The Commissioner finds that the consent clauses adopted on each of these websites / mobile application were sufficiently clear.

(3) Data Use by MoneyHero, Mtel and Standard Chartered

91. The Commissioner finds that there is **no contravention of DPP 3(1) of Schedule 1 to the Ordinance (Data Use) on the part of MoneyHero, Mtel and Standard Chartered in respect of their use of personal data obtained from TransUnion** because their use was consistent with their collection purposes as stated in the respective websites and mobile application:

(1) MoneyHero used the personal data obtained from TransUnion for the display of credit data to individuals. *It “also plans, in future and subject to ensuring compliance with the Ordinance, to offer more detailed information from the credit report and to offer the full report for download by the user. Additionally, it plans, in future, to make product recommendations based on the credit report insights”;*

(2) similar to the case of MoneyHero, Mtel used the personal data obtained from TransUnion for the display of credit data to individuals and did not use this for marketing purposes; and

(3) Standard Chartered used the data for the purpose of introducing their personal loan products, and individual’s prescribed consent had been sought.

(II) Data Security

92. The key question raised from this Incident is whether TransUnion took all reasonably practicable steps to authenticate the identity of online applicants of credit report as required under DPP 4(1) of Schedule 1 to the Ordinance (Data Security). Besides, whilst TransUnion claimed that it “*performs due diligence*

on business partners including the imposition of security requirements and the right to audit. Business partners are audited for their ability to meet TransUnion's standards and are continuously monitored between audits", this investigation also examined whether TransUnion had evaluated the security standards of its partners as claimed.

(1) Online Authentication Procedures

93. The Ordinance is by design principle-based and technology-neutral. There is no checklist setting out the specific requirements of an acceptable online authentication procedures. The Commissioner considers that the stringency of authentication procedures should be commensurate with the risks to the organization as well as the harm to the individual. Given the volume and sensitivity of the personal data that TransUnion handled, TransUnion should have adopted stringent checks to verify the individual's identity before releasing the credit reports applied for.
94. The Commissioner notes that Hong Kong Monetary Authority (**HKMA**) and the Securities and Future Commission (**SFC**) require the banking and the securities industries to adopt two-factor authentication for Internet trading with effect from 27 April 2018⁴⁵. Two-factor authentication is a security technique that uses a combination of the following for verification purposes:
- (1) something that the individual knows, such as username and password;
 - (2) something that the user has, such as OTP sent to the user's phone or using apps that generate single-use codes or passwords, hardware tokens or cards; and
 - (3) something that the user is, such as facial recognition, a fingerprint or an iris scan.
95. Notwithstanding that TransUnion is not statutorily regulated by HKMA or SFC, the Commissioner expects TransUnion, which receives and processes a considerable amount of information obtainable from banks, implements controls equivalent to, if not higher than, what the banks are implementing themselves.
96. In light of the relevant facts admitted by TransUnion and revealed after investigation, and in all the circumstances of the case, **the Commissioner finds**

⁴⁵ <https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=17PR133>

TransUnion contravened DPP 4(1) of Schedule 1 to the Ordinance (Data Security) in respect of its online authentication procedures in that it failed to take all practicable steps to ensure that the personal data held was protected against unauthorised or accidental access or use.

(1.1) Exact match of the full name and date of birth was not required

97. Based on the Commissioner's tests of the online authentication procedures, inputting a wrong date of birth would not stop the application for online credit report. TransUnion clarified that, at the first stage of the online authentication procedures, TransUnion used the Hong Kong Identity Card number to locate the credit profile in its database, and match the inputted name and date of birth against its database to determine the number and difficulty of the KBA questions to be generated. If the name inputted by the individual did not match, the individual would be categorized as 'high risk' but would still be able to pass the authentication if he was able to answer the KBA questions. If the date of birth inputted by the individual did not match (but the name matched with the record of the database), TransUnion would categorise the individual based on the risk classification of the device he used. He would be classified as 'low risk' if his device was assessed as 'low risk'.
98. The Commissioner considers that an individual should have knowledge of his own name, date of birth and Hong Kong Identity Card number and should therefore have no difficulty in inputting such basic information correctly. Failure to do so should not be allowed to proceed with the online authentication procedures.

(1.2) KBA was not prudently designed

99. TransUnion used KBA as part of the authentication procedures. Questions asking about the age range or Chinese zodiac sign of the individual were found in 10 out of 17 KBA examinations in the Commissioner's test. Unlike those about the individual's credit card type or issuing institution, these questions did not relate to the individual's credit data. If a fraudster knew the date of birth of the individual, he could easily deduce answers to these questions, and increase his chance of passing the KBA.
100. Besides, the Commissioner found in the tests that a non-card issuing institution was included as a possible answer to a question on institutions issuing credit

cards with the highest credit limit. TransUnion explained that, *“For those questions that need to generate decoy answers, we will define the product type relevant to the question, e.g. CARD, MORTGAGE, PERSONAL LOAN, HIRE PURCHASE, UNIONPAY. For each product type, the list of subscribers offering such product in the market is identified. When the system generates answers to the question, the true answer will always be generated from credit report data of the subject while the remaining decoy answers will be generated from the identified subscriber list. After further investigation, we found that the subscriber list for each product type is outdated...”* Based on the Commissioner’s tests, five answers were provided for each question. If one answer (which was outdated and therefore obviously wrong) could be easily screened out, the probability of choosing the correct answer would increase.

(1.3) Access through other websites / mobile application was not blocked after an individual failed the authentication procedures on one website / mobile application

101. The Commissioner’s tests also revealed that credit reports could still be obtained on another websites / mobile application after failing the authentication procedures on one website / mobile application. TransUnion confirmed that *“the two-attempt blocking approach implemented since July 2015 was restricted to an individual site and at device level only, but not on an applicant level.”* This means that an individual would be able to attempt the authentication procedures at a website / mobile application other than the one he has failed, thereby increasing the chance for a third party to access others’ credit reports.

(1.4) Two-factor authentication was not applied to all applications

102. An authentication process that makes use of KBA questions and OTP authentication would be considered a two-factor authentication as it makes use of something that the individual knows and something that the user has. However, the Commissioner notes that TransUnion changed its practice of sending OTP to all applications in 2015. TransUnion explained that it *“moved to a multi-layer risk-based and more sophisticated rules-based authentication in 2015 that allows us to tailor our authentication approach based on risk and increase the level of difficulty for higher-risk consumers without making the overall system too burdensome for low-risk consumers. An OTP was sent only to applicants who we determined to be high risk based on the multi-layer*

authentication. In order to make the service available to a wider audience (those without a verified phone number on the credit file) and in alignment with industry standards for authentication, we move to a multi-layer risk based authentication.” The Commissioner cannot accept such a move as it failed to protect consumer credit data from unauthorised access.

103. According to the enhancements proposed by TransUnion after the Incident, the two-factor authentication still does not apply to the scenario where OTP is not feasible as TransUnion would use an exact match of the last eight digits of credit card numbers as an alternative to OTP (as detailed in paragraph 25(9)). Such enhancement would only provide an additional layer of verification but does not secure the effect of a two-factor authentication as both KBA questions and credit card number verification fall into the category of something that the individual knows. The Commissioner considers that the enhancements are not sufficient to tackle potential identity fraud and safeguard the security of personal data considering the volume and significance of personal data it possesses.
104. Clause 3.12 of the Code sets out the general measures to be taken by a CRA to safeguard against improper access or mishandling of consumer credit data in its daily operation whereas clause 3.13 focuses on maintaining a log of access by credit providers. The loopholes revealed in TransUnion’s authentication procedures concern the access to a CRA’s database by individuals (not TransUnion’s staff), which are not specifically addressed by the Code.
105. Given that it was TransUnion and not its partners that set and verified the authentication procedures and made the authentication decision for online application of credit report through partners’ websites / mobile application, the Commissioner finds **no prima facie evidence to support a contravention of the Ordinance on the parts of the Five Partners in respect of the authentication procedures for accessing credit reports.**

(2) Due Diligence on Partners

106. The Ordinance does not require a data user to ensure the security of another data user’s personal data system even if it transfers personal data to the latter, unless the latter is its data processor which is defined as a person who processes

personal data on behalf of another person; and does not process the data for any of the person's own purposes⁴⁶.

107. Under the joint operation arrangements between TransUnion and the Five Partners at the relevant time, TransUnion would transfer personal data to three partners. Despite the transfer, these three partners did not fall under the definition (see paragraph 105 above) of data processor under the Ordinance because they processed personal data collected from TransUnion for their own purposes. TransUnion was therefore not required under the Ordinance to adopt any means to monitor the security requirements of the personal data systems of the partners.
108. The Commissioner notes that TransUnion carried out security assessments on i-Choice, Standard Chartered, MoneyHero and Mtel before accepting them as partners. TransUnion included additional Internet security requirements (e.g. specific standards of encryption on data in transit over the Internet, specific security measures for servers, firewalls and network connections) on MoneyHero and Mtel which received credit data from TransUnion. There was however no security assessment conducted for MoneySQ though TransUnion's joint operation arrangement with MoneySQ was the same as i-Choice.
109. TransUnion stated that it would carry out scheduled audits on its partners to ensure continuous compliance with TransUnion's security requirements but no evidence was provided to support that such audits had been carried out as all the security assessment reports provided were dated before the commencement of joint operation.
110. The Commissioner understands that TransUnion is not specifically obliged by the Ordinance or the Code to carry out regular audit to monitor its partners' security requirement. However, the Commissioner finds that performing such an audit on its partners which receive credit data from TransUnion is part and parcel of "all practicable steps" to ensure that personal data is protected against unauthorised access, having particular to "*the kind of data and harm that could result therefrom*", and "*any measures taken in ensuring the secure transmission of the data*" as required under DPP4(1)(a) and (e) of Schedule 1 to the Ordinance.

⁴⁶ DPP 2(4), DPP 4(2) and (3) of Schedule 1 to the Ordinance.
(https://www.elegislation.gov.hk/hk/cap486?xpid=ID_1438403263424_003).

V. Enforcement Action

111. Section 50(1) of the Ordinance provides that in consequence of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, he may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent recurrence of the contraventions.
112. Finding that TransUnion contravened DPP 4(1) of Schedule 1 to the Ordinance (Data Security) as aforesaid, the Commissioner exercises his power pursuant to section 50(1) of the Ordinance to serve an **EN** on TransUnion directing TransUnion to:
- (1) cease to release any credit reports online through any website / mobile application without OTP verification;
 - (2) conduct in-person authentication for all online applications of credit reports where OTP verification is not applicable;
 - (3) comply with the direction in items (1) and (2) above and confirm to the Commissioner in writing of the compliance of items (1) and (2) above within 14 days from the date of the EN;
 - (4) devise clear procedures to specify the steps, time limits and monitoring measures to ensure the answers generated for KBA questions are relevant, functional and up-to-date; and
 - (5) provide documentary proof within three months from the date of the EN, or forthwith where the remedial actions have been taken earlier, showing the completion of item (4) above.

VI. Comments

Review of the Code

113. Consumer credit data is very private to the individuals concerned. The rationale behind the issuing of the Code by the Commissioner is to ensure that there is a proper balance between the privacy rights of individuals in their consumer credit data, and the interest of credit providers and society at large, to maintain both commercial viability and stability in the consumer lending industry.
114. As indicated in the response of HKMA at the Panel Meeting, from the risk management perspective, the sharing of consumer credit information enabled banks to make informed and risk-based decisions when assessing credit applications from customers for loans and other credit facilities and conducting credit reviews, and hence it was not advisable for consumer credit information not to be made available to banks.
115. Whilst the Commissioner remains the regulator for the protection of all personal data including credit data, the Commissioner takes the view that the role of a CRA is an integral feature of our financial market. How it should be effectively regulated may demand further study, as pointed out in the motion proposed in the Panel Meeting which *“urges the Government to study the regulation of credit reference agencies, strengthen the monitoring of the collection, holding, handling or use of customers' personal credit data, increase the transparency and security of using innovative technologies to provide personal credit data in the future, and refine the legislation to enhance the community's confidence in credit rating reference services.”*
116. Both scenarios under the Strategic Services and Licensing Agreement and CreditView Dashboard Agreement involve the obtaining of credit information by a data subject which is an area that the Code has limited coverage. The Code does not aim to regulate the obtaining of credit report by data subjects from TransUnion in other circumstances.
117. In the arrangement of the Strategic Services and Licensing Agreement, the relevant partners acted as agents for the data subjects and obtained the credit reports directly from TransUnion. These partners were not credit providers and thus were not regulated by the Code (though they were still required to comply with the Ordinance). The grant of licenses to these two partners allowed them

to use consumer credit information either in accordance with the agreement or their internal business operations. This broad-brushed use of personal data might allow them to use the data for consumer analysis or even direct marketing as long as they complied with the data privacy laws or other applicable laws, e.g. by seeking prescribed consent for direct marketing, despite the fact that at the material time, the two partners (namely MoneyHero and Mtel) under this type of agreement did not use the personal data obtained for direct marketing purposes.

118. In the arrangement of the CreditView Dashboard Agreement, the data subject obtained the credit information directly from TransUnion and with the data subject's prescribed consent, TransUnion provided personal data to one of the three partners under this type of agreement for the purposes of direct marketing of goods or services. Clause 2.12 of the Code provides that a credit provider cannot access a data subject's credit data with a view to providing or promoting goods, facilities or services to that data subject. TransUnion's release of the data subject's credit information to a credit provider for promoting sales or services constitutes a violation of the Code as no exception for consent is set out in the Code (though no contravention of DPP3(1) of Schedule 1 to the Ordinance (Data Use) was found in the investigation).
119. Currently, under the Code, credit information kept by TransUnion can be provided to a limited pool of persons such as credit providers, Transport Department, insurers and debt collection agencies. The types of information that can be shared are also regulated. However, the Commissioner notes that access to credit report is not limited to credit providers. Besides, the disclosure of data by TransUnion to credit provider falls outside the remit of the Code. Data subjects who are attracted to the idea of obtaining credit information for free may not have fully appraised of the risks involved in giving consent to pass his credit information to these other entities.
120. Against this background, the Commissioner suggests the following policy questions, inter alia, be canvassed in the future review of the Code which requires public consultation with all stakeholders, including other relevant regulatory authorities:
 - (1) whether a person (despite being authorised by a data subject) should be allowed to obtain consumer credit data for his own use, being relatively sensitive personal data, from a CRA;

- (2) whether the definition of “credit provider” in the Code should be expanded to include providers of consumer credit monitoring services like Mtel and MoneyHero; and
- (3) whether there should be more than one CRA in Hong Kong, given the high demand for such a service and the short of competition in this regard.

121. The compliance audit carried out by an independent compliance auditor engaged by any CRA in future would then be expected, if not required, to cover the related security measures, as well as the requirements on notification and use of credit data by a person authorised by the data subject.

Supervision of CRA and credit report charges in other jurisdictions

122. Public concern has been raised about the centralized credit database being managed by a commercial entity but not regulated by a financial regulator. The fact that TransUnion’s businesses are not regulated by other authorities cannot be simply and merely addressed by the Code, or a revised Code.

123. The Commissioner researched⁴⁷ on how CRAs were regulated and the fees for credit reports in Australia, the mainland of China, Singapore, the United Kingdom and the United States, and noted that:

- (1) three jurisdictions (the mainland of China, Singapore and the United Kingdom) had specific regulations governing credit data and had organisations similar to HKMA to assume licensing and regulatory matters of CRA. The remaining two jurisdictions (Australia and the United States) lacked a licensing system but CRA were required to follow privacy-related legislation;
- (2) credit report was obtainable free of charge in three jurisdictions (once a year in Australia and the United States, and twice a year in the mainland of China), while the fee for a credit report in the remaining two jurisdictions (Singapore and the United Kingdom) was lower than HK\$30.

⁴⁷ See **Appendix F** for the summary of the research finding on how CRAs are regulated and the fees of credit reports in five jurisdictions.

- (3) Fee charging may be attributable to the short or availability of competitors providing the same services in the market.

Recommendations to TransUnion

124. Having considered all the circumstances of the case and the available information, the Commissioner makes the following five recommendations:

(1) *Devise privacy-friendly default setting*

- As demonstrated in TransUnion's joint operation arrangements with MoneySQ and i-Choice, it was technically feasible not to transfer any personal data to partners which allowed individuals' access to credit report. However, credit data was transferred to MoneyHero and Mtel under the joint operation arrangements. Transfer of credit data to partners should not be a default setting and less privacy-intrusive alternatives should be chosen.

(2) *Offer individuals a choice of the types of data to be transferred*

- An individual may not know the exact extent of data that would be transferred when he is asked to consent to the transfer of credit data from TransUnion to the partners concerned. TransUnion is therefore recommended to list the data and give the individual a choice on the data to be transferred to the partners.

(3) *Exercise control over partners which receive personal data from TransUnion*

- The investigation revealed that audit was not conducted on partners who received credit data from TransUnion throughout the contractual period. TransUnion is recommended to conduct audit no less than once a year to ensure the level of data protection afforded by the partners is adequate.

(4) *Conduct periodic review of online authentication procedures*

- Online access to credit reports offers convenience to individuals but at the same time demands reliable online authentication procedures.

It is legitimately expected that TransUnion will continue to review and improve its online authentication procedures in order to block fraudsters from accessing credit data. Periodic reviews with the aim to identifying and fixing loopholes as well as improving the authentication procedures (including assessing the appropriateness of using biometric authentication) in view of technology advancements should be conducted by in-house and / or third party experts.

(5) *Allow individuals to access credit reports at a lower cost*

- The Commissioner received a question on whether it is reasonable for TransUnion to charge a service fee of HK\$280 for a credit report. TransUnion explained that significant investment was required to convert the raw data contributed to TransUnion into comprehensive, meaningful information that was presented in a straightforward way for ease of understanding by the data subjects and credit providers. TransUnion added that it customised a unique credit score for each data subject, summarized key credit data to create the Dashboard and Score Trending for viewing individual credit information at a glance, provided Credit Monitoring tools such as SMS / Email credit alert, and different innovative educational tools, such as Score Factor, Debt Analysis and Credit Score Calculator etc. TransUnion also needed to invest heavily in security. The fee charged by TransUnion appeared however on the high side compared with that of other jurisdictions, considering the magnitude of the demand, and the comparable fees charged or not charged in other jurisdictions. TransUnion is recommended to review its fee structure and offer individuals an option to obtain a copy of the credit report with no provision of other auxiliary services at a lower fee.

— End —

Appendix A: Extracts from TransUnion’s Privacy Policy⁴⁸

Below are extracts from the relevant provisions of TransUnion’s Privacy Policy in respect of the data use, data disclosure, identification requirements and security safeguards.

“2 Use and Disclosure of Your Personal Information

2.1 *We limit our use of consumers’ personal information to those purposes which have been disclosed to consumers by our members⁴⁹, or for purposes which are otherwise permitted by the laws. We disclose personal information in compliance with the law primarily by means of Credit Reports to both consumer and members. Specifically, we use and disclose personal data in the following circumstances:*

(a) *to provide our consumer credit reporting services and other related services to our members; or*

(b) *to provide consumer credit information directly to consumers who have requested a copy of their Credit Reports, or to provide related services to consumers.*

2.2 *We may use information about your subscription of our service / products, such as your usage patterns, to customize your web site and / or customer service experience.*

2.3 *As a service to you, we will use your email address to provide you a receipt of your purchase...*

2.4 *We may provide anonymous information...to our members, customers or service providers.*

2.5 *We may share information without personal identifiers with third parties engaged to assist us in providing services and information to our members...*

⁴⁸ Downloaded on 26 November 2018.

⁴⁹ Members refer to credit providers who are TransUnion’s members who provide credit information about the individuals.

- 2.6 *We may disclose your personal information to third parties in the good faith belief that such action is necessary in order to comply with, or be responsive to, legal process served on us (such as subpoena or court warrant), or if we believe such disclosure is necessary to protect and defend the rights, property or safety of TransUnion, our users or others.*
- 2.7 *We may disclose your personal information to consultants, agents and advisers, such as attorneys and accountants, in the good faith belief that such disclosure is within the scope of their professional duties to TransUnion and with the understanding that such professionals will abide by our security and confidentiality policies.*
- ...

4 Identification Requirements

- 4.1 *In order to process your transactions and provide you with quality customer service, we need your full name and current and/or billing address, your email address (so we can contact you) and, if you purchase one of our products or services, a valid credit card number, your identity card number and certain other personal information, such as your date of birth, address information, employment information, and certain credit card and loan account information. We use such information to verify and authenticate the credit card number and to confirm that the person requesting your personal information or credit report really is you and not an impostor or other person improperly seeking to access your information.*
- 4.2 *You hereby give your consent to and authorize TransUnion to access all or part of your consumer credit data which may be held in our database from time to time (“**Your Credit Data**”) and to:-*
- (a) *match all or part of Your Credit Data against the information you provided or match against any information you provided with each other; and*
 - (b) *generate questions directly or indirectly from any or all of the information contained in Your Credit Data whether on its own or in conjunction with other source of information, collect responses to such questions from me and match such responses against any information contained in Your Credit Data,*

in order to verify your identity, to use such data or any data arising therefrom for purpose of Identity Manager Solutions which is a solution provided by TransUnion for identity management and related solution.

4.3 *You may not be able to register, subscribe or purchase the products on our Site or TransUnion Mobile, if you do not agree to give us your consent to verify your identity.*

...

6 *Our Safeguarding Practices*

6.1 *We take the protection of personal information seriously. We have adopted procedures to secure storage of personal information and are committed to working with our members to protect the security of personal information during any transfer to or from us. We have also instituted a number of safeguards to identify and help prevent the fraudulent use of personal credit information.*

6.2 *In our Site or TransUnion Mobile, we take precautions to secure your personal information...”*

Appendix B: Information Displayed in Credit Reports Obtained from Online Platforms⁵⁰

Data Displayed	TransUnion	MoneyHero	Mtel	Standard Chartered	i-Choice	Money SQ
Credit Score (grade & numeric)	Yes	Yes	Yes	Yes	Yes	Yes
Score Factors	Yes	Yes	No	No	No	No
Score Trending	Yes	No	No	Yes	Yes	Yes
Name	Yes	Yes	No	No	No	No
Address	Yes	Yes	No	No	No	No
Phone number	Yes	Yes	No	No	No	No
ID number	Yes	Yes	No	No	No	No
Hire Purchase / Leasing Account	Yes	Yes	Yes	No	No	No
Instalment Account	Yes	Yes	Yes	No	No	No
Charge Card	Yes	Yes	Yes	No	No	No
Credit Card	Yes	Yes	Yes	No	No	No
Revolving Account	Yes	Yes	Yes	No	No	No
Mortgage	Yes	Yes	No	No	No	No
Enquiries	Yes	Yes	No	No	No	No

⁵⁰ TransUnion's own investigation of the Incident revealed that Ming Pao accessed three public figures' credit reports online directly from TransUnion and indirectly through the websites of MoneyHero, i-Choice and MoneySQ during the period from 30 October 2018 to 18 November 2018. TransUnion found no evidence of attempting to access credit reports through the website of Standard Chartered and mobile application of Mtel by Ming Pao.

Public Record	Yes	Yes	No	No	No	No
Credit Overview (Delinquent, Utilization, Open Accounts, Enquiries, Year of History, Available Credit, Outstanding Balance)	Yes	Yes	No	Yes	Yes	Yes
Credit Alert	Yes	No	No	No	No	No
Score Simulator	Yes	No	No	No	No	No
Debt Analysis	Yes	No	No	Yes	Yes	Yes

Appendix C: Online Application for a Credit Report at TransUnion's Website

Step 1: Enter the following personal data:

1. Title
2. Surname
3. Given name and other name
4. HKID number
5. Date of birth
6. Mobile number

Be In Control - Get access to Credit Report, Score & Alerts Print

Step 1. Enter your personal information | Step 2. Verify Your Identity | Step 3. Review and submit your order

Your account is almost done. Please complete this page to create your account.

Title *

Surname *

Given Name *

Other Name

HKID Number *
 ()

Date of Birth *

Mobile Number *

Please disable call forwarding. A verification SMS may be sent.

I understand that by clicking on the "I Accept & Continue" button below, I am providing "written consent" to TransUnion Limited ("TU") authorizing TU to obtain information from my personal credit profile from the database of TU solely for the purposes of confirming my identity, retaining, displaying my credit data and calculating my credit score for my own reference.

I acknowledge that I have read the [Service Agreement](#), [Conditions for Online Report Ordering through Secure Access & Identity Manager](#), [Terms of Use](#) and [Privacy Policy](#), and agree to their terms.

I ACCEPT & CONTINUE ⊕

Step 2: Answer a set of three or five multiple choice KBA questions

Step 2 of 3: Verify Your Identity Print

Step 1: Enter your personal information | **Step 2: Verify Your Identity** | Step 3: Review and submit your order

To protect your identity, please answer the verification questions below to continue your order.
Please select the following financial institutions (please choose all correct answers) you are engaged with in terms of credit card services (in HKD):

- A) The Hongkong and Shanghai Banking Corporation Ltd.
- B) Bell-net Finance Co. Ltd.
- C) Ever Credit Consumer Corporation Ltd.
- D) A + B
- None of the above

Please select one of the following credit cards (in HKD) that you have

- XXXX XXXX XXXX XXXX
- None of the above

What is your zodiac sign?

- Dog
- Dragon
- Goat
- Rooster
- None of the above

How many credit card(s) (in HKD) do you have with The Hongkong and Shanghai Banking Corporation Ltd. (excluding supplementary/suspended/closed cards)?

- 1
- 2
- 3
- 4
- None of the above

How many financial institution(s) do you have its/their credit card(s) (in HKD)? (excluding supplementary/suspended/closed cards)

- 1
- 2
- 3
- 4
- None of the above

CONTINUE ↻

Step 3: Enter OTP (for high risk applications only)

Step 2 of 3: Verify Your Identity Print

Step 1: Tell Us About Yourself | **Step 2: Verify Your Identity** | Step 3: Review and submit your order

- An SMS message with a single use passcode will be sent to the mobile number you provided
- Please ensure your mobile phone is switched on and that call forwarding is disabled

One-time Passcode

TU- 176496

Please [click here](#) to resend your one-time passcode if it is not received within a few minutes.

SUBMIT ↻

Step 4: Submit credit card information for payment

Step 3 of 3: Review and submit your order Print

Step 1: Enter your personal information Step 2: Verify Your identity **Step 3: Review and submit your order**

Please enter your payment details below:

Credit Card Number

Expiration Date /

Security Code



Promotional Code

I hereby authorize TransUnion Limited to effectively transfer from my above credit card account the monthly fee on every month until further notice.

 By clicking the button below, you give your consent to TransUnion to use, collect, retain and transfer your credit card information to process payment and authenticate your identity.

Order Summary

Product	Amount
Credit Report, Score & Alerts	HKD 280
Total:	HKD 280

Account Details

Email Address

Mobile Number

Appendix D: Joint Operation between TransUnion and the Five Partners

1. MoneyHero

- TransUnion entered into an agreement with MoneyHero, which is a CAG’s subsidiary, in February 2018.
- MoneyHero *“is in the business of providing certain services including comparison of financial and insurance products and services, direct marketing including email and other advertising activities for the promotion of financial and insurance products, and the facilitation of applications for financial and insurance products and services to consumers in Hong Kong.”*⁵¹ Throughout 2018, TransUnion and CAG worked together to enable CAG to build the CreditGo platform, and the website⁵² was launched in September 2018 to provide registered members with free access to credit reports.
- According to the agreement between TransUnion and MoneyHero,

“Company may request from TU on behalf of, and with the written consent of, consumers certain product features... to display to the subject Consumer certain Consumer Credit Information...while the Consumer is using Company’s Service and in accordance with the Consumer Written Consent and for no other purposes.”

“TransUnion will deliver a credit report, credit score, and key credit report factors impacting the credit score when requested to do so by Company.”

“Company will pay the amount due for the TransUnion products in accordance with the per-member-per-month rate schedule...Per-member, per-month pricing, includes access to credit reports data, TransUnion credit scores, and credit education contents, at US\$XXX flat rate (“Credit Data Fee”)...Company shall pay an additional fee of US\$XXX per authentication request to verify the identity of new enrollees (“Authentication Fee”)...”

⁵¹ As stated in the agreement between TransUnion and MoneyHero.

⁵² <https://www.creditgo.com.hk/en>

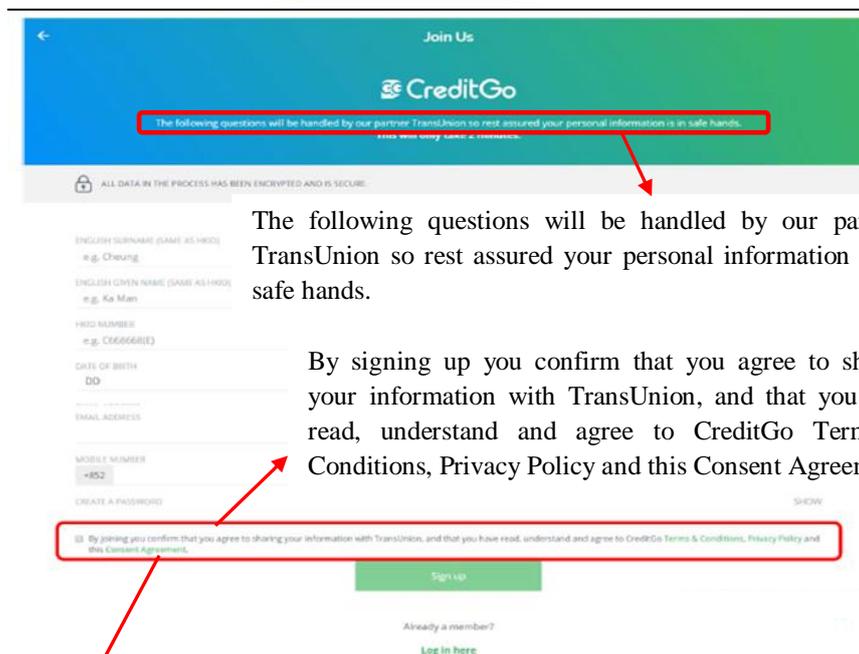
- The application procedures before the suspension of online application are set out below:

Step 1: Click the “Free Checking Now” button



Step 2: Enter personal data and provide consent to the Terms & Conditions, Privacy Policy and Consent Agreement

1. Surname
2. Given name
3. HKID number
4. Date of birth
5. Email address
6. Mobile number



The following questions will be handled by our partner TransUnion so rest assured your personal information is in safe hands.

By signing up you confirm that you agree to sharing your information with TransUnion, and that you have read, understand and agree to CreditGo Terms & Conditions, Privacy Policy and this Consent Agreement.

Consent Agreement

By accepting this Agreement, I understand that I am providing written consent to:

- (i) *CreditGo, which is owned and operated by CompareAsia Group Limited (the “Company”) requesting and receiving on my behalf from TransUnion Limited (“TransUnion”) all or part of my consumer credit data which may be held in the database of TransUnion from time to time (“My Credit*

- Data”)
- (ii) *TransUnion transferring all or part of My Credit Data, including but not limited to my consumer credit report and credit score, to the Company’s server located in the Republic of Singapore for the purpose of displaying My Credit Data to me on the Company’s website, or as otherwise described in the Company’s Privacy Policy and Terms & Conditions and*
 - (iii) *the Company transferring/sharing all or part of My Credit Data as well as ancillary data derived from or relating to My Credit Data to/with the Company’s affiliated companies and third parties that provide services to the Company in connection with My Credit Data.*

Step 3: Validate email address by clicking a verification link



Check Your Email

A verification link has been sent to your registered email address. Please click on the link to validate your email and continue your registration process.

EMAIL NOT RECEIVED? [RESEND](#)

Success

Your email has been validated. Before you proceed, please have your banking information at hand as you will need to answer some TransUnion security questions that are specific to your personal banking details.

EMAIL ADDRESS

PASSWORD

Forgot your password? [Click here](#)

Log in

English 中文

Step 4: Answer multiple choice KBA questions

Welcome to CreditGo!

To verify and protect your privacy, we need to ask 2 verification questions.

What is your age today?

None of the above

How many credit card(s) (in HKD) do you have with ABC DEF Bank Co.Ltd. (excluding supplementary/suspended/closed cards)?

None of the above

XXXX XXXX XXXX XXXX (only display last 4 digits) belongs to which card type?

Classic, Master Card

Classic, Union Pay

Platinum / Infinite / Ultima / Centurion / Titanium, Master Card

Platinum / Infinite / Ultima / Centurion / Titanium, Visa

None of the above

[Next](#)

2. Mtel

- TransUnion first entered into an agreement with Mtel in May 2016, and renewed it in February 2018.
- Mtel is “*in the business of providing digital solution services*”⁵³. It developed an app called “Credit Check”, which allowed users to “*get free credit data, get an overview of all credit card and loan accounts, sync payment due dates to the in-app calendar and set up reminders*”.
- According to the agreement between TransUnion and Mtel,

“Company may request from TU on behalf of, and with the written consent of, Consumers certain product features... to display to the subject Consumer certain Consumer Credit Information...and for Company to directly market to the Consumer financial products and services...while the Consumer is using Company’s website and in accordance with the Consumer Written Consent and for no other purposes.”

“Upon execution of the Agreement, Company shall pay TU the monthly minimum fee of HKDXXX to avail itself to unlimited number of transaction for Consumer Connect Services; AND the service of authentication to verify identity shall be charged at a special price of HKD XXX per request.”

⁵³ Extract from the Agreement between TransUnion and Mtel.

- The application procedures before the suspension of online application are set out below:

Step 1: Enter email address and provide consent for sign up

HKBN 12:07 74%

← CreditCheck

Sign up for a free Credit Check account.

Email Address

Please enter your email

Confirm Email Address

Please enter your email

By clicking NEXT to obtain your free credit report sponsored by Mtel Limited, you confirm that you accept the [Terms and Conditions](#) and privacy Policy relating to the Personal Data (Privacy) Ordinance, and you consent to your Personal Data (Privacy) Ordinance, and you consent to your personal data being provided to Credit Check and to Credit Check using your personal data for direct marketing as detailed in the [Privacy Policy](#). You can opt out of direct marketing any time.

NEXT

Step 2: Receive a temporary password at the registered email address and login with this temporary password

HKBN 13:08 71%

← CreditCheck

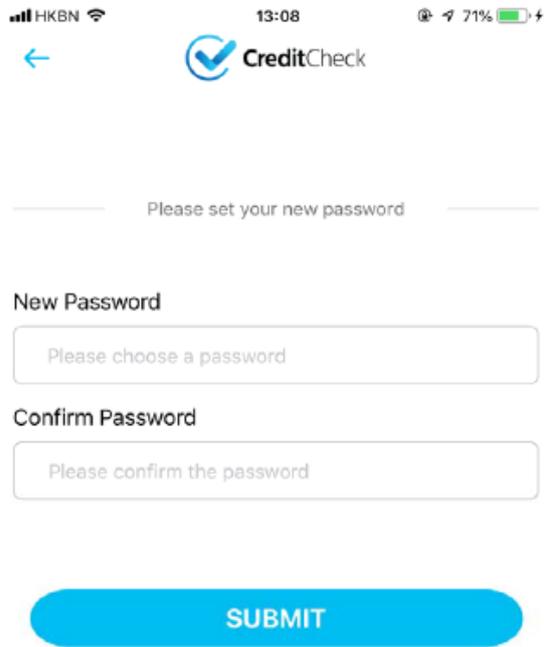
TEMPORARY PASSWORD has been sent to your registered email address, please check your mailbox spam folder if you cannot receive it.

Please Login with your temporary password.

LOGIN NOW

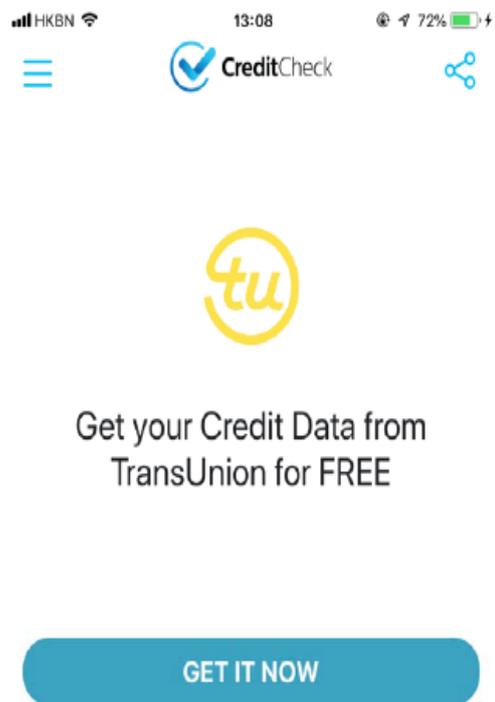
[Resend Password](#)

Step 3: Create a new password



The screenshot shows the 'CreditCheck' app interface for creating a new password. At the top, the status bar displays 'HKBN', '13:08', and '71%' battery. The app header includes a back arrow and the 'CreditCheck' logo. The main heading is 'Please set your new password'. Below this, there are two input fields: 'New Password' with the placeholder 'Please choose a password' and 'Confirm Password' with the placeholder 'Please confirm the password'. A large blue 'SUBMIT' button is positioned at the bottom.

Step 4: Apply for credit data



The screenshot shows the 'CreditCheck' app interface with a TransUnion offer. The status bar shows 'HKBN', '13:08', and '72%' battery. The app header includes a menu icon, the 'CreditCheck' logo, and a share icon. The central focus is the TransUnion logo (a yellow circle with 'tu' inside). Below the logo, the text reads 'Get your Credit Data from TransUnion for FREE'. A large blue 'GET IT NOW' button is at the bottom.

Step 5: Enter personal data and provide consent

1. Title
2. Surname
3. Given name and other name
4. HKID number
5. Date of birth

The screenshot shows a mobile app interface for 'CreditCheck'. At the top, there is a status bar with 'HKBN', signal strength, Wi-Fi, time '13:08', and battery '72%'. Below the status bar is a blue checkmark icon and the text 'CreditCheck'. A message reads: 'Get your Credit Data from TransUnion. You will have two attempts to answer the verification questions and you may need to have your statements and cards at your hand for reference.' The form contains the following fields:

- Title:** A dropdown menu with 'Please select' and a downward arrow.
- Surname (same as it is shown on your HKID, please input in English):** A text input field with the placeholder 'e.g. Chan'.
- Given Name (same as it is shown on your HKID, please input in English):** A text input field with the placeholder 'e.g. Tai Man'.
- Other Name (if applicable; same as it is shown on your HKID, please input in English):** A text input field with the placeholder 'e.g. Peter'.
- HKID Number:** A text input field with the placeholder 'e.g. A123456' and a separate box containing the number '7'.
- Date of Birth:** Three separate input boxes labeled 'DD', 'MM', and 'YYYY'.

HKBN 21:30 81%



Mobile Number (one time password may be sent via SMS)

Please enter your Hong Kong mobile number

Promotion Code: (Optional)

Please input promotion code

By clicking on the "I Accept and Continue" button below, I understand that I am providing written consent for Mtel Limited to transmit the above information to TransUnion Limited and to request and receive all or part of my consumer credit data which may be held in the database of TransUnion Limited from time to time ("My Credit Data"), including but not limited to information in my consumer credit report and credit score. I hereby authorize TransUnion Limited to transfer My Credit Data including the score to Mtel Limited for the purpose of displaying My Credit Data and the credit score to me while I am using this website or application.

Further, I authorize Mtel Limited to retain My Credit Data and the credit score for so long as I have an active Credit Check account for the purpose of displaying the history of My Credit Data and the cr...

I hereby give my consent to and authorize TransUnion Limited to access all or part of My Credit Data and to:

Limited to access all or part of My Credit Data and to:

- (i) match all or part of My Credit Data against the information I have provided to Mtel Limited on this page; and
- (ii) generate questions directly or indirectly from any or all of the information contained in My Credit Data whether on its own or in conjunction with other source of information, collect responses to such questions from me and match such responses against any information contained in My Credit Data, for the purposes of verifying my identity. I agree that TransUnion Limited may receive and then process, use and transfer the result of the verification or any data arising therefrom to Mtel Limited via this app.

I further acknowledge and agree that the access, transfer, process and use of My Credit Data by TransUnion Limited in the manner described above shall not be made the basis upon which any complaint, claim, suit, demand or cause of action or other proceedings will be made against TransUnion Limited by me.

I ACCEPT & CONTINUE

Step 6: Answer multiple choice KBA questions

••••• CMHK 17:52 39%

2. What is your age today?

37 - 38 - (true)

39 - 40 - (false)

43 - 44 - (false)

45 - 46 - (false)

None of the above - (false)

3. Please select the contact phone number(s) you have ever used:

A) 69146974 - (false)

B) 10062079 - (true)

C) 65541072 - (false)

D) A + B - (false)

None of the above - (false)

3. Standard Chartered

- TransUnion entered into an agreement with Standard Chartered in April 2017.
- Standard Chartered is a licensed bank. A dedicated website was established for users to “see credit overview for FREE”⁵⁴.
- According to the agreement between TransUnion and Standard Chartered,

“...TU has developed a white-labeled credit management dashboard (“CreditView”) to be used by financial institutions and financial services companies to provide free credit information to their customers; and

Company desires to offer certain financial services including CreditView to consumers (“Consumers”) using services offered by TU...for the benefit of Company’s Consumers, a website that presents Consumers with credit information labeled with Company’s brand, integrated with Company’s website, and to be used by Consumers.”

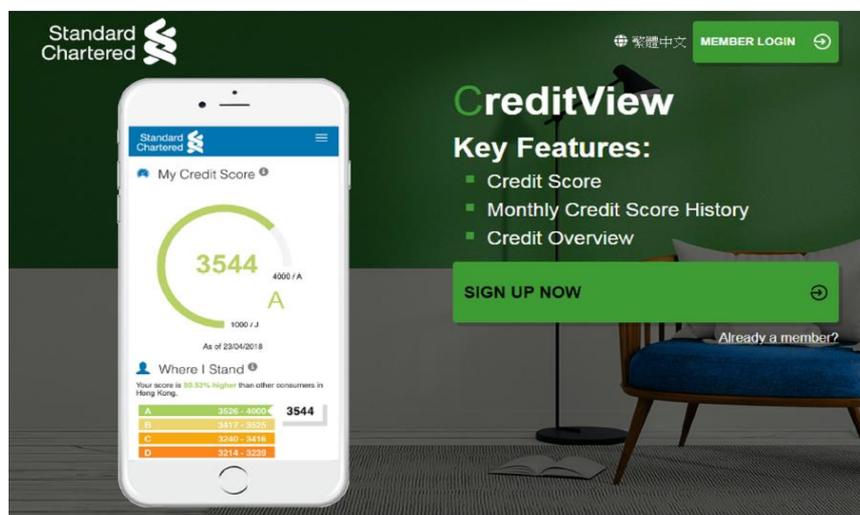
“Company shall pay a credit information processing fee based on the number of Consumers having access to the CreditView Dashboard at any time each month...”

“TU shall provide monthly reporting on (a) dashboard utilization, and weekly report on (b) enrollment subscriber details...Enrollment subscriber details shall include the customer ID, the partner customer code, name (first and last), email and phone...”

⁵⁴ According to www.sc.com/hk/zh/loans/creditview/ on 28 November 2018.

- The application procedures before the suspension of online application are set out below:

Step 1: Click the “Sign Up Now” button



Step 2: Enter personal data and provide consent

1. Title
2. Surname
3. Given name and other name
4. HKID number
5. Date of birth
6. Email address
7. Mobile number

Standard Chartered

繁體中文

CreditView

Get started to see your credit overview for FREE

1 Enter your personal information 2 Authenticate your ID

- Enter your personal information as shown on your HKID card to authenticate your identity.
- Ensure your email address is correct for username/password retrieval purpose. Your email is important for us to securely communicate with you.
- Store your username and password in a safe place for future logins.

Invalid HKID

Fields marked * are mandatory (Please fill in with English)

Personal Information

Title * Surname * Given Name *

Other Name Date of Birth * HKID Number *

Mobile Number * Email Address *

Please disable call forwarding. A verification SMS may be sent.

Account Information

Create a Username * Create a Password * Confirm a Password *

Already a member?
Welcome back! Please [login here](#)

Need Help?

Contact Us
Email: verifyid@transunion.hk
Phone: (852) 2979-3087
Office hours
Monday – Friday 9:00 – 17:30
Saturdays, Sundays and Public Holidays Closed

FAQ

Will checking my credit through CreditView lower my score?
No. Checking your own credit counts as a “soft inquiry” and isn’t factored into a credit score

Is this site secure?
Yes. Our top priority is to keep your information safe using the latest encryption technology.

I understand that by clicking on the "I Accept & Continue" button below, I am providing "written consent" to TransUnion Limited ("TU") authorizing TU to obtain information from my personal credit profile from the database of TU solely for the purposes of confirming my identity, retaining and displaying my credit data to me.

I acknowledge that I have read the [Service Agreement](#), [Terms of Use](#) and [Privacy Policy](#), and agree to their terms.

I acknowledge that I have read the [Terms and Conditions](#) of CreditView and agree to their terms.

I understand that this service is paid for by Standard Chartered Bank (Hong Kong) Limited (the "Bank").

I am interested in the personal loan products of the Bank and agree to have TransUnion transferring my personal details (including name, mobile phone number and the first letter of the Hong Kong Identity Card) to the Bank and consent to have the Bank contacting me for the purpose of introducing its Personal Loan product(s) to me.

I understand that this service is solely provided by TransUnion and by using this service, TransUnion will not share my credit data with the Bank. For the avoidance of doubt, this consent is given once and will not override my existing direct marketing preference with the Bank.

TransUnion and the Bank are independent of each other with no alliance formed. If, however, I do not wish for TransUnion to transfer my personal details to the Bank, I can choose **not** to press "I Accept & Continue" and I understand that I have the option of accessing my credit data for a fee which will be **payable by me**. I understand I can visit TransUnion's website for subscription details.

I acknowledge that I have read and agree to the Bank's Privacy Policy.

I Accept & Continue 

Step 3 Answer multiple choice KBA questions

 ▶ ❌ +

CreditView

All security reasons we cannot set up your account if you cannot be authenticated. Please answer the questions below accurately. Please note that the page will be locked after 15 minutes. Please submit the answers before that.

How many credit card(s) (in HKD) do you have (including supplementary/suspended/closed cards)?

- 0
- 1
- 2
- 3
- 4
- None of the above

How many credit card(s) (in HKD) have you closed over the past six months?

- 1
- 2
- 3
- 4
- None of the above

Please select the following financial institutions (please choose all correct answers) you are engaged with in terms of credit card services (in HKD):

- A. Citibank, N.A.
- B. The Hongkong and Shanghai Banking Corporation, Ltd.
- C. BOC Credit Card (HK) Ltd.
- D. A + B
- None of the above

How many credit card(s) (in HKD) do you have with The Hongkong and Shanghai Banking Corporation Ltd. (excluding supplementary/suspended/closed cards)?

- 1
- 2
- 3
- 4
- None of the above

What is the last 4 digits of your Citibank, N.A. Classic credit card (in HKD)?

- XXXX XXXX XXXX 0000
- XXXX XXXX XXXX 1000
- XXXX XXXX XXXX 3600
- XXXX XXXX XXXX 8000
- None of the above

CONTINUE 

4. i-Choice

- TransUnion entered into an agreement with i-Choice in November 2017.
- i-Choice is a money lender licensee and provides an online lending platform⁵⁵. It provided registered members with free access to credit data.
- According to the agreement between TransUnion and i-Choice,

“...TU has developed a white-labeled credit management dashboard (“CreditView”) to be used by financial institutions and financial services companies to provide free credit information to their customers; and

Company desires to offer certain financial services including CreditView to consumers (“Consumers”) using services offered by TU...for the benefit of Company’s Consumers, a website that presents Consumers with credit information labeled with Company’s brand, integrated with Company’s website, and to be used by Consumers.”

“Company shall pay a credit information processing fee based on the number of Consumers having access to the CreditView Dashboard at any time each month...”

“TU shall provide monthly reporting on (a) dashboard utilization, and (b) enrollment subscriber details...Enrollment subscriber details shall include the customer ID, the partner customer code, name (first and last), email, current address and enrolment date...”

⁵⁵ www.i-choice.hk

- The application procedures before the suspension of online application are set out below:

Step 1:

Register as a member by entering the following personal data:

1. Mobile number
2. Email address
3. Captcha code



Step 2: Input OTP to verify mobile number



Step 3: Confirm email address



Step 4: Click to apply for a free credit report



Step 5: Enter personal data

1. Title
2. Surname
3. Given name
4. Other name
5. HKID number
6. Date of birth
7. Mobile number
8. Email address

免費信貸報告表格

請將以下填報的個人資料包括香港身份證號碼、姓名、出生日期和身份證上的資料一致。此等資料將會提交與聯匯有限公司，用作申請個人免費信貸報告。

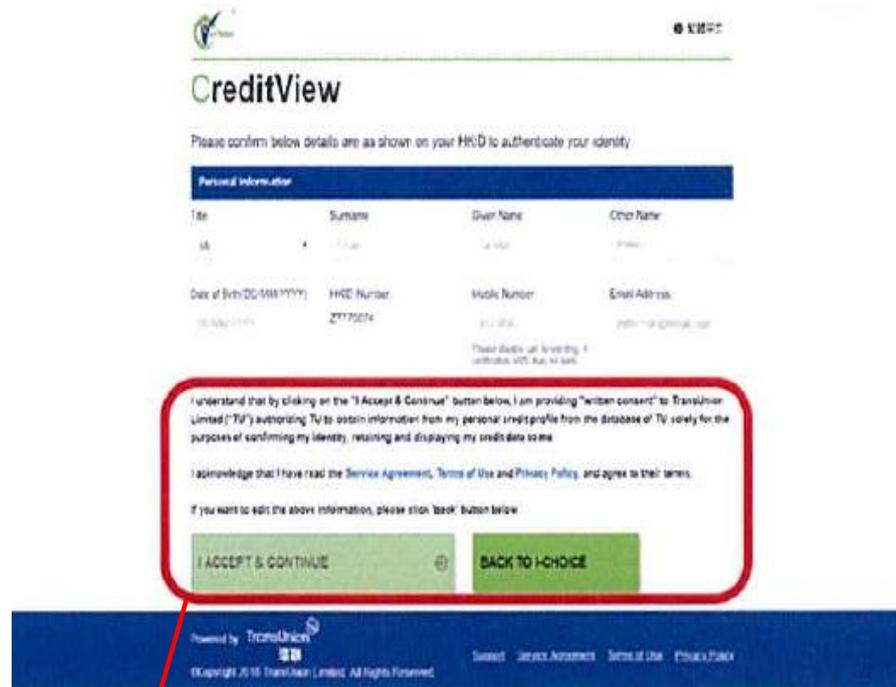
稱謂*	先生	出生日期*	
姓氏(英文)*		名字(英文)*	
別名		香港身份證號碼*	()
手提電話號碼*		電郵地址*	

如此申請導致信貸報告錯誤，需要更改個人資料或資料有誤，請於辦公時間內，聯絡本公司客戶服務部 2727 5500。
Should there need any amendment on the personal information provided, please contact our customer hotline 2727 5500 during office hours.

提交

聯絡熱線 查詢詳情 免費信貸報告

Step 6: Provide consent to the Terms & Condition, Privacy Policy and Service Agreement

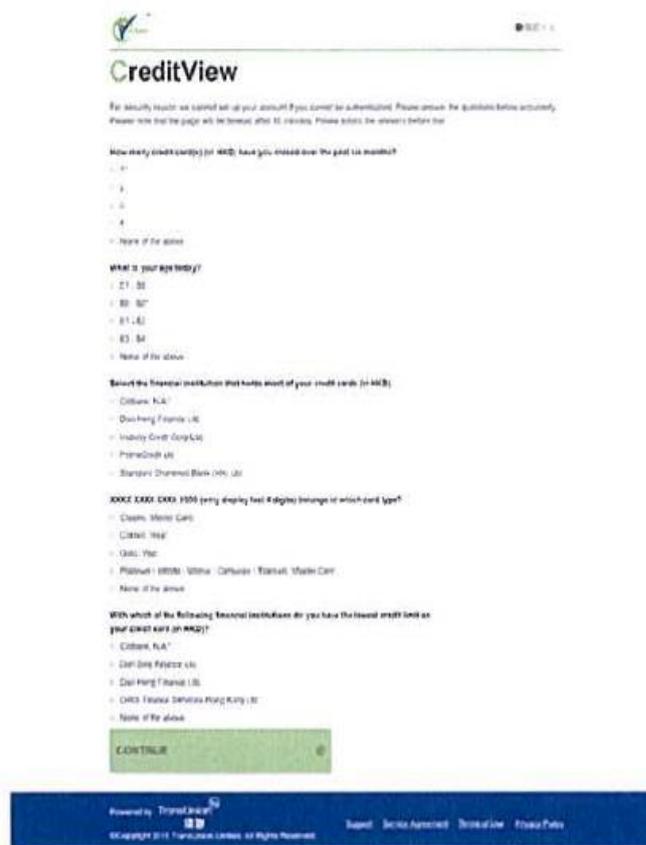


I understand that by clicking on the “I Accept & Continue” button below, I am providing “written consent” to TransUnion Limited (“TU”) authorizing TU to obtain information from my personal credit profile from the database of TU solely for the purpose of confirming my identity, retaining and displaying my credit data to me.

I acknowledge that I have read the Service Agreement, Terms of Use and Privacy Policy and agree to their terms.

If you want to edit the above information, please click “back” button below.

Step 7: Answer multiple choice KBA questions



The screenshot shows a web interface for CreditView. At the top left is the CreditView logo, and at the top right is a user profile icon. Below the logo is a warning message: "For security reasons we cannot set up your account if you cannot be authenticated. Please answer the questions below accurately. Please note that the page will be locked after 30 minutes. Please select an answer before that." There are four multiple-choice questions, each with radio button options. The first question asks about the number of credit cards used in the last 12 months, with options 1, 2, 3, 4, and "None of the above". The second question asks for the user's age, with options 21-30, 31-40, 41-50, 51-60, and "None of the above". The third question asks for the financial institution that holds most of the user's credit cards, with options Citibank, N.A., Citibank Finance Ltd, Industrial Credit Corp Ltd, PwncrCredit Ltd, and Standard Chartered Bank (HK) Ltd. The fourth question asks for the type of credit card, with options Classic, Metro Card, Classic, Visa, Gold, Visa, Platinum / BNP Paribas, Citibank, Citibank, Metro Card, and "None of the above". The fifth question asks for the financial institution with the lowest credit limit on the user's credit cards, with options Citibank, N.A., Citibank Finance Ltd, Citibank Finance Ltd, Citibank Finance Ltd, Citibank Finance Ltd, and "None of the above". A green "CONTINUE" button is located below the questions. At the bottom of the page is a dark blue footer containing the text "Powered by TransUnion", a logo, and links for "Support", "Service Agreement", "Privacy Policy", and "Terms of Use".

CreditView

For security reasons we cannot set up your account if you cannot be authenticated. Please answer the questions below accurately. Please note that the page will be locked after 30 minutes. Please select an answer before that.

How many credit cards (or A/Cs) have you used over the past 12 months?

- 1
- 2
- 3
- 4
- None of the above

What is your age today?

- 21 - 30
- 31 - 40
- 41 - 50
- 51 - 60
- None of the above

Select the financial institution that holds most of your credit cards (if any)

- Citibank, N.A.
- Citibank Finance Ltd
- Industrial Credit Corp Ltd
- PwncrCredit Ltd
- Standard Chartered Bank (HK) Ltd

XXXX XXXX XXXX (only display first 4 digits) (change if which card type?)

- Classic, Metro Card
- Classic, Visa
- Gold, Visa
- Platinum / BNP Paribas, Citibank, Citibank, Metro Card
- None of the above

With which of the following financial institutions do you have the lowest credit limit on your credit cards (if any)?

- Citibank, N.A.
- Citibank Finance Ltd
- Citibank Finance Ltd
- Citibank Finance Ltd
- Citibank Finance Ltd
- None of the above

CONTINUE

Powered by **TransUnion**
Support Service Agreement Privacy Policy Terms of Use
Copyright © 2018 TransUnion Limited. All Rights Reserved.

5. MoneySQ

- TransUnion entered into an agreement with MoneySQ in April 2016.
- MoneySQ is a money lender licensee and provides an online lending platform. It provided registered members with free access to credit data.
- According to the agreement between TransUnion and MoneySQ,

“...TU has developed a white-labeled credit management dashboard (“CreditView”) to be used by financial institutions and financial services companies to provide free credit information to their customers; and

Company desires to offer certain financial services including CreditView to consumers (“Consumers”) using services offered by TU...for the benefit of Company’s Consumers, a website that presents Consumers with credit information labeled with Company’s brand, integrated with Company’s website, and to be used by Consumers.”

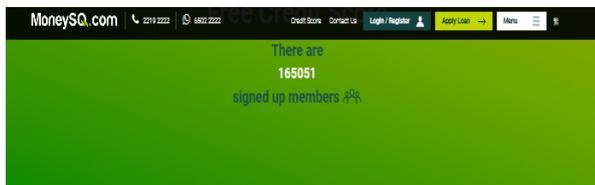
“Company shall pay a credit information processing fee based on the number of Consumers having access to the CreditView Dashboard at any time each month...”

“TU shall provide monthly reporting on (a) dashboard utilization, and (b) enrollment subscriber details...Enrollment subscriber details shall include the customer ID, the partner customer code, name (first and last), email, current address and enrolment date...⁵⁶”

⁵⁶ Both TransUnion and MoneySQ confirmed that the monthly reporting did not cover subscriber details. A copy of the monthly report was also provided to the Commissioner as supporting document.

- The application procedures before the suspension of online application are set out below:

Step1: Register as a member by entering the following personal data:



1. First name
2. Last name
3. Mobile number
4. Email address
5. Contact address

Member Registration

- Or Social Account Login -



First Name* Last Name*

Mobile Number

Email

Contact Address

Password (8-16 digits)

Confirm Password

I have read, understand and agree to the Website Terms of Use, Use of Cookies, Privacy Policy and any applicable disclosure statement(s).

[Sign Up](#)

[Forgot password?](#)

Step 2: Enter HKID number



CreditView™

TU CreditView™ service is solely provided by TransUnion. All personal data is directly transferred to TransUnion server. Please note that MoneySQ.com will NOT store any personal data from this transmission to protect user privacy.

[Check Now](#)

- After creating a new account with TransUnion, users will be able to check their personal credit score. After submitting personal details, users will have their identity verified.



Please enter HKID and you will be redirected to TransUnion CreditView™

HKID e.g. A1234567

[Submit](#)

Step 3: Enter personal data and provide consent

1. Title
2. Surname
3. Given name and other name
4. HKID number
5. Date of birth
6. Mobile number
7. Email address

MoneySQ.com
Spend Smart Loan Smart

繁體中文

CreditView

Please confirm your details below are as shown on your HKID to authenticate your identity

Personal Information

Title Mr.	Surname Chan	Given Name Tai Man	Other Name Peter
Date of Birth(DD/MM/YYYY) DDMM/YYYY	HKID Number [REDACTED]	Mobile Number 91234567	Email Address peterchan@email.com

Please disable call forwarding. A verification SMS may be sent.

I understand that by clicking on the "I Accept & Continue" button below, I am providing "written consent" to TransUnion Limited ("TU") authorizing TU to obtain information from my personal credit profile from the database of TU solely for the purposes of confirming my identity, retaining and displaying my credit data to me.

I acknowledge that I have read the [Service Agreement](#), [Terms of Use](#) and [Privacy Policy](#), and agree to their terms.

If you want to edit the above information, please click 'back' button below

I ACCEPT & CONTINUE
Return to MoneySQ

Powered by **TransUnion** 環聯
Support Data Security Privacy Policy Terms of Use
©Copyright 2018 TransUnion Limited. All Rights Reserved.

Step 4: Answer multiple choice KBA questions

MoneySQ.com
Spend Smart Loan Smart

CreditView

For security reasons, we cannot log you out of your account if you cannot be authenticated. Please be aware of your session timeout situation. Please close this page all old browser after 10 minutes. Please saved the answers before this.

What is the credit limit on your Citibank, N.A. credit card that has an account number 3456 7890 1234 5678?

HKD 10,000
 HKD 20,000
 HKD 30,000
 HKD 40,000
 HKD 50,000
 HKD 60,000

Please select the correct phone number(s) you have ever used:

81234567
 91234567
 12345678
 23456789
 None of the above

What type of credit card(s) HKID do you share with Citibank, N.A. over past six months?

Classic Visa®
 Bank of America Card
 Gold Visa®
 Platinum Infinite Global Companion™ TransUnion Member Card
 Platinum Infinite Global Companion™ TransUnion Visa®

What is the principal amount of your customer associated user (p1111111111) last loan, pay loan fee, withdrawal fee etc. (excluding overdraft and revolving accounts) opened over the past six months with TransUnion (TU) Ltd.?

HKD 30,000
 HKD 40,000
 HKD 50,000
 HKD 60,000
 HKD 70,000
 HKD 80,000
 HKD 90,000

How many credit cards (or HKID) do you have (including suspended/closed cards)?

0
 1
 2
 3
 4
 None of the above

CONTINUE

Powered by **TransUnion** 環聯
Support Data Security Privacy Policy Terms of Use
©Copyright 2018 TransUnion Limited. All Rights Reserved.

Appendix E: Clauses 2.8 to 2.12 of the Code of Practice on Consumer Credit Data - Access by credit provider to consumer credit data held by CRA

Access for updating

- 2.8 A credit provider may at any time, for the purpose of providing or updating consumer credit data on an individual, access from a CRA such consumer credit data on the individual as was previously provided by it to the CRA.

Access through credit report

- 2.9 Without prejudice to the generality of clause 2.8 but subject to clauses 2.9A and 2.10A, a credit provider may, through a credit report provided by a CRA, access consumer credit data (except mortgage count) held by the CRA on an individual:

- 2.9.1 in the course of:

2.9.1.1 the consideration of any application for grant of consumer credit;

2.9.1.2 the review of existing consumer credit facilities granted; or

2.9.1.3 the renewal of existing consumer credit facilities granted,

to the individual as borrower or to another person for whom the individual proposes to act or acts as mortgagor or guarantor; or

- 2.9.2 for the purpose of the reasonable monitoring of the indebtedness of the individual while there is currently a default by the individual as borrower, mortgagor or guarantor,

and for the purpose of clauses 2.9.1.2, 2.9A.2, 2.9A.4, 2.9A.5, 2.10A.2, 2.10A.3, 2.10A.4 and other related clauses, the word “review” means consideration by the credit provider of any of the following matters (and those matters only) in relation to the existing credit facilities, namely:

- 2.9.3 an increase in the credit amount;

- 2.9.4 the curtailing of credit (including the cancellation of credit or a decrease in the credit amount); or

- 2.9.5 the putting in place or the implementation of a scheme of arrangement with the individual.

- 2.9A Without prejudice to the generality of clause 2.8 but subject to clause 2.10A, a credit provider may, with the written consent from the individual and through a credit report provided by a CRA, access the mortgage count held by the CRA on an individual in the course of:
- 2.9A.1 the consideration of any application for grant of a mortgage loan;
 - 2.9A.2 the review of existing mortgage loans granted;
 - 2.9A.3 the consideration of any application for grant of consumer credit facilities (other than mortgage loan);
 - 2.9A.4 the review of existing consumer credit facilities granted (other than mortgage loan);
 - 2.9A.5 the review under the circumstances in clauses 2.10A.2, 2.10A.3 and 2.10A.4 for any existing consumer credit facilities granted;
 - 2.9A.6 the renewal of existing mortgage loans granted; or
 - 2.9A.7 the renewal of existing consumer credit facilities granted (other than mortgage loan),

to the individual as borrower or to another person for whom the individual proposes to act or acts as mortgagor or guarantor and for the purposes of clauses 2.9A.3, 2.9A.4 and 2.9A.7, the consumer credit facilities granted or to be granted shall be of an amount not less than such level or be determined by a mechanism as prescribed or approved by the Commissioner from time to time.

Access to Mortgage Count during transitional period

- 2.10A Notwithstanding clause 2.9A, a credit provider shall not, during the transitional period, be entitled to access the mortgage count of an individual through a credit report, unless the access is made with the written consent of the individual and under any of the following circumstances:
- 2.10A.1 in the course of considering any application for grant of a mortgage loan to the individual, or to another person for whom the individual proposes to act as mortgagor or guarantor;
 - 2.10A.2 in the course of the review of existing credit facilities currently in material default, with a view to putting in place a loan restructuring arrangement by the credit provider;

- 2.10A.3 in the course of the review of existing credit facilities, where there is in place a loan restructuring arrangement between the individual and the credit provider (whether or not other parties are also involved), for the implementation of the said arrangement by the credit provider; or
- 2.10A.4 in the course of the review of existing credit facilities, with a view to putting in place a scheme of arrangement with the individual initiated by a request from the individual.

Confirmation to CRA upon access

- 2.11 On each occasion of accessing any consumer credit data held by a CRA, the credit provider shall confirm to the CRA for its record:
 - 2.11.1 the circumstances provided for in clause 2.8, 2.9, 2.9A or 2.10A under which the access has been made; and
 - 2.11.2 in the case where the access has been made in the course of the review of existing consumer credit facilities under clause 2.9.1.2, 2.9A.2, 2.9A.4, 2.9A.5, 2.10A.2, 2.10A.3 or 2.10A.4 above, the specific matter or matters provided for in clause 2.9.3, 2.9.4 or 2.9.5 above that has been considered upon such a review.

No access for direct marketing

- 2.12 A credit provider is prohibited from accessing the consumer credit data of an individual held by a CRA for the purpose of offering or advertising the availability of goods, facilities or services to such individual. For the avoidance of doubt, this clause does not prohibit a credit provider from accessing the consumer credit data of its existing customers in the course of the review or renewal of existing consumer credit facilities under the circumstances as provided under clauses 2.9.1.2, 2.9.1.3, 2.9A.2, 2.9A.4, 2.9A.5, 2.9A.6, 2.9A.7, 2.10A.2, 2.10A.3 and 2.10A.4.

Appendix F: Supervision of CRA and Credit Report Charges in Five Jurisdictions

	Australia	China	Singapore	UK	US
Relevant law or regulation	Privacy Act 1988 – Part IIIA: Credit Reporting	Regulation on the Administration of Credit Investigation Industry	Consumer Credit Bureau Act 2016	<ul style="list-style-type: none"> Consumer Credit Act Data Protection Act 2018 	Fair Credit Reporting Act
Regulatee	<ul style="list-style-type: none"> Credit reporting bodies Credit providers Other prescribed recipients of credit data 	Credit investigation institutions (Same as credit reference/reporting agencies)	<ul style="list-style-type: none"> Credit bureaus (Same as credit reference/reporting agencies) Members of credit bureaus (i.e. banks and finance companies) 	<ul style="list-style-type: none"> Consumer credit business (including credit reference agencies) Consumer hire business 	Consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records)
Regulatory body	Information Commissioner	People’s Bank of China	Monetary Authority of Singapore	Financial Conduct Authority	Federal Trade Commission
Fees Charged	Free access once a year and in certain conditions ⁵⁷	Free access twice a year ⁵⁸	Access with a fee of S\$6.42 plus GST ⁵⁹	<ul style="list-style-type: none"> Access with a fee of £2⁶⁰ Free access for victims 	<ul style="list-style-type: none"> Free access once a year and in certain conditions⁶¹

⁵⁷ If (a) a consumer has been refused credit, within the past 90 days or (b) the credit-related personal information has been corrected. See <https://www.oaic.gov.au/individuals/faqs-for-individuals/credit-reporting/accessing-your-credit-report>

⁵⁸ See <http://www.pbccrc.org.cn/crc/kffw/201412/1f3503d61cf64587bcd1edce707516b4.shtml>

⁵⁹ See <https://www.creditbureau.com.sg/how-to-get-my-credit-report.html>

⁶⁰ See <https://www.gov.uk/government/news/credit-reports-available-online-for-all-consumers>

⁶¹ Free disclosure (a) after adverse notice to consumer; (b) under certain other circumstances: if the consumer certifies in writing that he (i) is unemployed and intends to apply for employment in the 60-day period beginning on the date on which the certification is made; (ii) is a recipient of public welfare assistance; or (iii)

	Australia	China	Singapore	UK	US
				of ID fraud and the financially vulnerable	<ul style="list-style-type: none"> Access with charge, plus tax where applicable (Equifax US \$15.95⁶², Experian US \$14.95⁶³ and TransUnion US \$19.95/month⁶⁴)

has reason to believe that the file on the consumer at the agency contains inaccurate information due to fraud; (c) in connection with fraud alerts. https://www.ftc.gov/system/files/545a_fair-credit-reporting-act-0918.pdf

⁶² As of 6 May 2019, credit scores and reports can be obtained from <https://www.equifax.com/personal/products/credit/report-and-score/> for US\$15.95.

⁶³ As of 6 May 2019, personal credit reports (with credit score) can be purchased at <https://connect.experian.com/register/personal-use.html> for US\$14.95.

⁶⁴ As of 6 May 2019, credit score with credit monitoring service is available at https://membership.tui.transunion.com/tucm/orderStep1_form.page?offer=3BM10203&PLACE_CTA=home:center:tu for US\$19.95 per month.