Report Published under Section 48(1) of the Personal Data (Privacy) Ordinance (Cap. 486)

Report Number: R11-3803

Date issued: 15 March 2011

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

This page is intentionally left blank to facilitate double-side printing

Report on the Inspection of the Personal Data System of TransUnion Limited

This report of an inspection carried out by the Privacy Commissioner for Personal Data ("**the Commissioner**") pursuant to section 36 of the Personal Data (Privacy) Ordinance, Cap. 486 ("**the Ordinance**") in relation to the personal data system used by TransUnion Limited ("**TransUnion**") is published in the exercise of the power conferred on the Commissioner by Part VII of the Ordinance.

Section 36 of the Ordinance provides that:

"*Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-*

(a) any personal data system used by a data user; or

(b) any personal data system used by a data user belonging to a class of data users,

for the purposes of ascertaining information to assist the Commissioner in making recommendations-

(i) to-

(A) where paragraph (a) is applicable, the relevant data user;

(B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs; and

(ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be."

The term "**personal data system**" is defined in **section 2(1)** of the Ordinance to mean "*any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system*."

TransUnion belongs to the class of data users who carries on a business of providing consumer credit reference service.

Section 48 of the Ordinance provides that:-

"*(1) Subject to subsection (3), the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-*

(a) setting out any recommendations arising from the inspection 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

(b) in such manner as he thinks fit."

"*(3) Subject to subsection (4), a report published under subsection (1) or (2) shall be so framed as to the prevent the identity of any individual being ascertained from it.*"

"*(4) Subsection (3) shall not apply to any individual who is-*

(a) the Commissioner or a prescribed officer;

(b) the relevant data user."

Allan CHIANG
Privacy Commissioner for Personal Data
Hong Kong SAR

Table of Contents

Chapter One

Introduction

Historical Background

The need for credit reference services

1.1 Consumer credit is one of the major financing facilities contributing to the economic growth of Hong Kong. Individuals who wish to expand their businesses, purchase properties on mortgages, pay taxes on loans, purchase goods by hire purchase, or enjoy the convenience of credit cards can apply for consumer credits. Provision of consumer credit affects almost all walks of life.

1.2 In deciding whether or not to provide consumer credit to an individual and the terms of the consumer credit, credit providers like banks need to assess the creditworthiness of the individual. While a credit provider may make the assessment based on the information provided by the individual, information from other independent sources such as credit reference agencies ("**CRA**") can be more reliable and comprehensive.

1.3 CRA provides consumer credit reference services to credit providers by supplying information about an individual that is considered relevant to the individual's creditworthiness. CRA gathers the credit information from three major sources: (i) information provided by other credit providers, e.g. payment in default by an individual, (ii) information available from public records, e.g. Court records showing the possible involvement of an individual in bankruptcy proceedings or in a debt recovery action, and (iii) information provided by the consumers themselves.

Introduction and evolution of the Code of Practice on Consumer Credit Data ("the Code")

1.4 When the Office of the Privacy Commissioner for Personal Data ("**PCPD**") was established in 1996, the general practice in Hong Kong was that

credit providers participating in consumer credit reference services only provided information about a customer to a CRA if that customer was in significant default of his repayment obligations. The PCPD noted that Hong Kong's major CRA was upgrading its system and had plans to widen the scope of information by adding information such as an individual's current debt exposure and previous manner of repayment.

1.5 With a view to laying clear ground rules for CRA and to increasing transparency of how the personal data maintained by CRA may be used, the Commissioner issued the Code in February 1998 pursuant to section 12 of the Ordinance.[1] As regards the practice of CRA, the Code as it was first issued required CRA to, among others, collect only specific types of personal data and on request promptly provide a credit report to a consumer whose credit was refused.

1.6 The Code was revised in February 2002 and again in June 2003. The first revision included, among other things, extension of the period of retention of certain credit data and permission for CRA to carry out credit scoring, and the second revision included, among other things, restrictions on the meaning of "review" by credit providers and disclosure of notice of disputed data in the credit report.

Current version of the Code

1.7 The Code is designed to provide practical guidance to data users in Hong Kong in the handling of consumer credit data. It deals with collection, accuracy, use, security, access and correction of personal data of individuals who are, or have been, applicants for consumer credit.

[1] 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."

1.8 The current version of the Code took effect on 2 June 2003. It regulates the processing of the following personal data of individual consumers about their creditworthiness:-

(1) "**Account General Data**"[2]

- identity of the credit provider;
- account number;
- capacity of the individual (whether as borrower or as guarantor);
- account opened date;
- account closed date;
- type of the facility and currency denominated;
- approved credit limit or loan amount (as appropriate);
- repayment period or terms (if any);
- account status (active, closed, write-off, etc.);
- facility maturity date (if any);
- details of any scheme of arrangement, including:
  - the date of the arrangement, the number and frequency of installments, the installment amount, etc.; and
- in the case of a hire-purchase, leasing or charge account, including:
  - account expiry date, type of security, investigation date, installment amount, etc;
  - particulars for the identification of the motor vehicles, equipment, vessels or the asset secured by the charge, and notification of termination of the charge.

(2) "**Account Repayment Data**"[3]

- amount last due;
- amount of repayment made during the last reporting period;
- remaining available credit or outstanding balance;
- default data being:
  - amount past due (if any) and number of days past due;
  - date of settlement of amount past due (if any).

[2] See Clause 1.3 and Part (A) in Schedule 2 of the Code.
[3] See Clause 1.4 and Part (B) in Schedule 2 of the Code.

The Account General Data and the Account Repayment Data collectively are referred to as "**Account Data**" under the Code.[4]

(3) "**Consumer Credit Data**" 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 database of a CRA in the course of or in connection with the providing of consumer credit reference service*".[5]

(4) Public records, including Court records, judgments and data relating to an individual's bankruptcy.[6]

1.9 The Code consists of four parts. Part III contains provisions on the handling of Consumer Credit Data by CRA in the following aspects:-

(1) Scope of data to be collected by CRA: Clause 3.1
(2) Retention of Consumer Credit Data by CRA: Clauses 3.2 to 3.7
(3) Use of Consumer Credit Data by CRA: Clauses 3.8 to 3.10
(4) Data security and system integrity safeguards by CRA: Clauses 3.11 to 3.13
(5) Compliance audit of CRA: Clauses 3.14 to 3.17
(6) Data access and correction request to CRA: Clauses 3.18 to 3.20

1.10 Breach of the Code itself is not a contravention of a requirement under the Ordinance, but will give rise to a presumption against the data user in any legal proceedings under the Ordinance, including the presumption of contravention of the relevant Data Protection Principles ("**DPPs**").

[4] See Clause 1.2 and Schedule 2 of the Code.
[5] See Clause 1.8 of the Code.
[6] See Clause 3.1.3 of the Code.

Reasons for the Inspection

1.11 TransUnion is a major CRA in Hong Kong.[7] It maintains credit records of about 4.3 million individuals and is the major source of consumer credit information for credit providers. Consumer Credit Data relate to the financial standing of individuals, based on which assessment of their creditworthiness will be made. They are sensitive in nature and are being collected, accessed and used on a daily basis.

1.12 Given the vast amount of Consumer Credit Data being held by a single CRA and the serious adverse impact it may have on individual consumer in the event of mishandling of the data, the Commissioner considered that a comprehensive examination of the personal data system of TransUnion by way of an inspection under section 36 of the Ordinance is warranted. Given further that the Code has undergone a series of changes and the consumer credit database of TransUnion has expanded significantly since 1998, it was appropriate to carry out an inspection.

1.13 Between 2003 and 2009, TransUnion had completed a total of six privacy compliance audits through the engagement of external auditors and had supplied six audit reports to the Commissioner for his consideration and comments. Although the audit reports had provided valuable indicators that would assist in assessing the integrity, accuracy and security of the personal data system of TransUnion, the Commissioner believed that the community's confidence in the system would be further enhanced if a comprehensive review was conducted by PCPD itself further to TransUnion's self-arranged audits.

1.14 The efficiency and reliability of the consumer credit database are legitimate expectations of the community. It is also of paramount importance to ensure that credit providers have fair and reasonable access to accurate Consumer Credit Data for credit assessment under prudent lending policies consistent with their obligations as data users. Given the public interest in this matter, the Commissioner decided to invoke the power vested in him under

[7] The other CRA is Dun & Bradstreet (HK) Limited.

section 36 of the Ordinance to carry out an inspection of the personal data system used by TransUnion ("**the Inspection**").

Chapter Two

The Business Structure of TransUnion

The Establishment, Shareholders and Businesses of TransUnion

2.1 TransUnion provides credit information in 25 countries, including the Mainland China.[8] In Hong Kong, TransUnion was formerly known as "Credit Information Services Limited" (香港資信有限公司), which was incorporated in Hong Kong in May 1981 and subsequently changed its name to "TransUnion Information Services Limited" (環聯資訊有限公司) and then to "TransUnion Limited".

2.2 According to the annual return of TransUnion filed with the Companies Registry on 22 June 2010, the shareholders of TransUnion are Vail Systemen Groep B.V. (56.25%), The Hongkong and Shanghai Banking Corporation Limited (6.25%), DBS Bank (Hong Kong) Limited (6.25%), Standard Chartered Bank (Hong Kong) Limited (6.25%), American Express International Inc. (6.25%), The Bank of East Asia, Limited (6.25%), Hang Seng Finance Limited (6.25%) and Dun & Bradstreet (HK) Limited (6.25%).

2.3 The principal businesses of TransUnion as shown in its Memorandum of Association are "*to provide credit information service, including the collation and retention of credit information, and statistics and such other information and statistics as may be decided to be appropriate and to disseminate such information to all and any interested persons on such terms and conditions as may be thought fit and to carry on any other business incidental to or arising out of such business*".

2.4 TransUnion provides consumer credit reference services to credit providers who have subscribed to its services ("**Subscribers**").

[8] According to information available at www.transunion.com.

The Organization of TransUnion

2.5 There are about 60 staff in 10 different departments of TransUnion, namely Finance, HR & Administration, Compliance, Data Quality Assurance, Data Administration, MIS & System Project Management, Operations, IT, Consumer Relations, and Sales & Marketing departments. Table 1 below shows the organization structure of TransUnion:

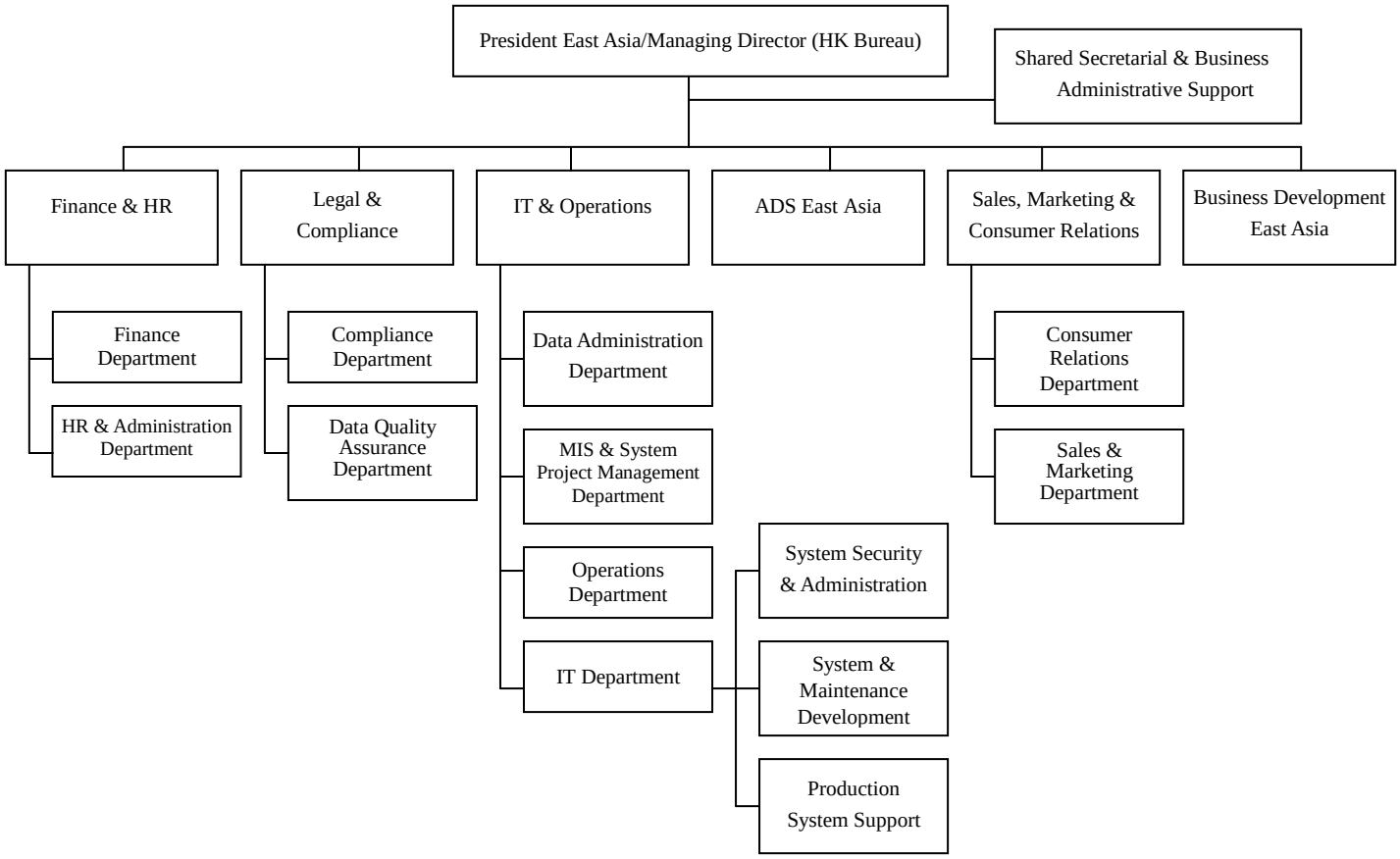


Table 1 : Organization Structure of TransUnion

2.6 According to TransUnion, only the following departments/teams and personnel have access to Consumer Credit Data:-

Departments	**Major Duties**
Operations Department ("**OD**") - 1 Operations Manager - 1 Operations Supervisor - 1 Assistant Operations	• Verifying Consumer Credit Data supplied by Subscribers in batches; • Verifying public records obtained by Data Administration Department;

Supervisor - 3 Operations Support staff	• Approving public records for inputting according to TransUnion's *Public Record Approval Procedure* and inputting public records such as Individual Voluntary Arrangement ("**IVA**") and bankruptcy discharge records; • Amending personal and company records according to Subscribers' requests; • Processing account contribution batch requests and credit check batch requests from Subscribers; and • Performing user account administration of TransUnion's consumer credit database system for Subscribers.
Data Administration Department ("**DAD**") - 1 Data Administration Manager - 1 Data Administration Supervisor - 4 Data Administration Support Staff	• Collecting personal data from public records and updating TransUnion's records; • Verifying and amending Consumer Credit Data supplied by Subscribers for updating; and • Updating and investigating inaccuracies account data, collateral data, etc.
Consumer Relations Department ("**CRD**") - 1 Consumer Relations Manager - 1 Consumer Relations Supervisor - 7 Consumer Relations Officers	• Handling consumers' requests for credit reports and requests for correction of Consumer Credit Data made by consumers; and • Preparing consumer credit report according to consumers' requests.
Shared Secretarial & Business Administrative Support ("**SSBAS**") - 1 Head, Shared Secretarial &	• Handling requests for credit reports submitted by consumers by mail.

Business Administrative Support - 2 Administrative Officers	
Information Technology Department ("**ITD**") - 1 IT Manager - 1 Database/System Administrative Officer - 1 Unix/Database Administrative Support Staff - 1 System Architect (Application Development) - 1 Senior System Analyst - 1 System Analyst - 1 Network/Security Administrative Officer	• Supervising retention period of Consumer Credit Data in the consumer credit database system of TransUnion; • Backup and purge of Consumer Credit Data; and • Access and update of account data, collateral data, etc. according to authorized requests.
Legal and Compliance (Compliance Department and Data Quality Assurance Department) ("**LC**") - 1 Compliance Officer - 1 Data Quality Assurance Officer	• Ensuring compliance with the requirements under the Ordinance and the Code by all departments of TransUnion; and • Ensuring Subscribers' data quality meets the requirements under the Code.

Chapter Three

The Inspection

The Inspection Team

3.1 Pursuant to section 41 of the Ordinance, by a letter from the Commissioner to TransUnion dated 31 March 2010, the Commissioner gave notice in writing of his intention to carry out the Inspection on the personal data system operated by TransUnion. At the same time, the Commissioner requested TransUnion to supply various documents (e.g. organization structure, all current policies, guidelines, procedures on the handling of Consumer Credit Data, and description of the flow of Consumer Credit Data) to enable the Commissioner to have a preliminary understanding of the personal data system of TransUnion.

3.2 An inspection team ("**the Team**") was formed for the purpose of the Inspection of the personal data system of TransUnion. The Team was led by the Commissioner who was assisted by the Deputy Commissioner, and was made up of the following officers from the Compliance & Policy Division, Operations Division and Information Technology Division of the PCPD:-

(1) Mr Wilson LEE, Chief Personal Data Officer
(2) Mr Henry CHANG, Information Technology Advisor
(3) Mr Ronald KWAN, Acting Senior Personal Data Officer
(4) Ms Maggie LO, Personal Data Officer
(5) Ms Joanna CHAN, Personal Data Officer
(6) Ms Kimmy CHENG, Assistant Personal Data Officer (IT)
(7) Mr Brad KWOK, Assistant Personal Data Officer
(8) Mr Sacha CHIU, Assistant Personal Data Officer

Scope of the Inspection

3.3 The Inspection was to ascertain information relating to the processing cycle of the Consumer Credit Data in the personal data system of TransUnion

in order to make recommendations to TransUnion relating to the promotion of compliance with the six DPPs and the Code.

3.4 The following requirements of CRA under the Code are not within the scope of the Inspection:

(1) Specific guidance on the conduct of compliance audit of TransUnion as a CRA under Clauses 3.14 to 3.17 of the Code; and

(2) Practice of TransUnion during the transitional period of the Code, i.e. from 2 June 2003 to 1 June 2005, e.g. provision of credit report during the transitional period under Clause 3.8.2.3 of the Code.

Methodology

3.5 The Ordinance does not prescribe a methodology for an inspection to be carried out under section 36 of the Ordinance. Unlike the inspection previously conducted by the PCPD, the present Inspection was not prompted by an incident of intrusion of personal data privacy, e.g. data leakage, on which the scope of the Inspection may be focused. The scope of the present Inspection is wide in that the entire data processing cycle of the personal data system of TransUnion was considered by the Team in the light of all six DPPs and the Code.

3.6 The Inspection consists of 7 major types of review work:-

(1) System walkthrough

TransUnion is a major CRA in Hong Kong and its personal data system is unique. In order to conduct the Inspection more efficiently, the Team needed a better understanding of the structure and daily operation of the personal data system. To this end, at the request of the Team, the relevant department heads of TransUnion provided comprehensive explanatory

materials and oral presentation to the Team before the Inspection.

(2) Policy review

The Team has examined documents relevant to the processing of Consumer Credit Data in the personal data system of TransUnion including documents relating to organisation structure, rules and responsibilities, polices, guidelines, operational procedures, training materials, service agreements, system journals/log, IT documents, internal forms and compliance related documents. The objective of the policy review was to determine whether appropriate and sufficient policies, guidelines and procedures on protection of Consumer Credit Data are in place.

(3) Interactive queries

The database of the Consumer Credit Data maintained by TransUnion is kept in a database system called 2000Plus ("**the Database System**"). While it is not practicable for the Team to inspect the entire database, the Team performed extensive interactive queries with the Database System in the presence of the representatives of TransUnion with a view to determining the integrity of the Consumer Credit Data, the security of the Database System, whether the retention periods of various Consumer Credit Data exceed the requirements under the Code. Furthermore, interactive queries were also conducted on the development and testing systems, where modification of the Database System would first be carried out and tested prior to implementation on the 'live' production system, to ascertain that these non-production environments did not hold any personal data.

(4) Interviews

In the Inspection, the Team interviewed 15 key staff from different departments of TransUnion to understand their daily handling of Consumer Credit Data, their familiarity with the policies, guidelines and procedures relating to their work, and the training they provided and received. In the process, the Team aimed at determining whether the policies, guidelines and procedures had been effectively communicated and observed. A list of the staff the Team interviewed in the Inspection can be found in *Annex A.*

(5) On-site inspection

On-site inspection enabled the Team to inspect the physical layout and appropriate security measures of the premises where Consumer Credit Data were processed and stored by TransUnion. Since part of the office premises of TransUnion is used to receive and process consumers' requests for credit reports made in person, on-site inspection also enabled the Team to inspect the data protection measures taken by TransUnion in processing such requests.

(6) Requests for credit reports

In order to ascertain how TransUnion processed consumers' requests for credit reports, in June 2010 the Team caused three requests to be made in person, by post and on-line. To ensure the accuracy of our observations, TransUnion was not notified of the three requests made for the purpose of this Inspection.

(7) Survey

In order to ascertain the consumers' reasons for accessing their credit reports and whether TransUnion had taken adequate steps to prevent the credit reports from being disclosed to

unauthorized parties, the Team conducted a survey from 10:30 am to 5:00 pm on 21 June 2010 and from 10:00 am to 5:00 pm on 22 June 2010 in the waiting area of TransUnion reserved for customer service. The Team successfully obtained responses from 37 consumers who requested for their credit reports at the material time. The questions and the analysis of the survey are in *Annex B*.

Pre-Inspection Works

3.7 On or about 21 April 2010, the Team received and started perusal of the documents requested by the Commissioner on 31 March 2010. On 17 May 2010, the Team requested for further documents from TransUnion for perusal.

3.8 On 26 May 2010, a pre-inspection meeting was held between the Team and the representatives of TransUnion including the Managing Director, Senior Director of IT & Operation East Asia, Director of Sales & Marketing, Director of Legal and Compliance, Manager of Consumer Relations, and Compliance Officer at its office premises at Suite 1001, Tower 6, The Gateway, 9 Canton Road, Tsim Sha Tsui, Kowloon, Hong Kong ("**the TST Office**"). At the meeting, key staff of TransUnion gave a powerpoint presentation to the Team in explaining the operation and data flow of the personal data system of TransUnion.

3.9 Subsequent to the pre-inspection meeting, the Team received further documents from TransUnion for perusal on 31 May 2010 and 14 June 2010.

Inspection on 21 and 22 June 2010

3.10 The Inspection was scheduled for two days to be held in the TST Office of TransUnion on 21 and 22 June 2010. The following were carried out on the respective dates of the Inspection:

21 June 2010

(1) Physical inspection of the TST Office of TransUnion;

(2) Demonstration of the handling of data contributed by Subscribers in batches and Transport Department's reports of duplicate vehicle registration;[9]

(3) Demonstration of the procedure for updating public records obtained from the gazette and handling of bankruptcy discharge data received;

(4) Interactive queries on development and testing systems and the data warehouse system to ascertain that they did not contain any personal data;

(5) Interactive queries on the Database System to check whether the Consumer Credit Data stored in it were retained according to the requirements under the Code;

(6) Survey of consumers; and

(7) Interview with selected staff of TransUnion.

22 June 2010

(1) Demonstration of the handling of credit check requests in batches and the on-line credit check enquiry;

(2) Interactive queries on the appropriate access rights of the TransUnion staff;

(3) Interactive queries to generate from the Database System consumer credit reports for Subscribers and for consumers, and to compare the contents of these two types of reports;

(4) Survey of consumers; and

[9] The reports should enable TransUnion to notify the Subscriber who has provided finance to a vehicle when duplicate license registration is detected.

(5) Interview with other staff of TransUnion.

Inspection on 18 August 2010

3.11 Since it was revealed in the first two days of the Inspection that the backup tapes storing the Consumer Credit Data are transported back and forth every weekday between the TST Office and a security company ("**the Security Company**") for safekeeping in the vault of the Security Company, the Team carried out further site inspection on the transportation and storage procedure for the backup tapes on 18 August 2010.

3.12 After the Inspection on 21 and 22 June 2010 and 18 August 2010, the Team made further queries on issues brought up during the Inspection so that TransUnion could make clarification and provide additional information for the Commissioner's consideration.

Chapter Four

Personal Data System of TransUnion and Data Flow

The Personal Data System of TransUnion

4.1 The subject matter of which the Commissioner may conduct an inspection under section 36 of the Ordinance is the personal data system used by a data user. The statutory meaning of "personal data system"[10] is wide enough to cover not only automated system used for processing of personal data, but also systematic operation of different departments and the relevant staff of TransUnion in the collection, holding, processing or use of the Consumer Credit Data.

4.2 Given the general meaning of the term "personal data system", it is not possible to demarcate which branch of TransUnion's operations should be considered as part of the personal data system and which is not. Instead, the Team defined the scope of the personal data system by first identifying the automated system used by TransUnion to maintain the consumer credit database i.e. the Database System, and then including the departments and staff interacting with the automated system as part of their daily operations.

4.3 While Consumer Credit Data are stored in the Database System, the Database System was not considered as a standalone system for which the Inspection was carried out. For example, the Database System is underpinned by a number of servers and a network infrastructure. It is accessible via various communication systems or interfaces by TransUnion's internal staff, external Subscribers and the general public, and administrated via a support system that consists of separate backup/standby systems, development and testing environments. Collectively all these systems and equipment are considered as part of the overall personal data system for which this Inspection was carried out.

[10] Section 2(1) of the Ordinance.

4.4 In the Inspection, the departments involved in the personal data system of TransUnion are OD, DAD, CRD LC, SSBAS and ITD.

4.5 To better understand the operation of the personal data system of TransUnion, it is helpful to set out details of the Consumer Credit Data flow into and from the Database System.

Data Flow

Data Collection

4.6 Under Clauses 3.1.1 to 3.1.8 of the Code, TransUnion may, for the purpose of providing consumer credit reference service, collect personal data of consumers. According to the information available to the Team, the consumers' personal data held by TransUnion come from three major sources: (1) contribution from Subscribers such as banks, finance companies and credit card companies, (2) public records and (3) consumers.

4.7 Subscribers who have collected Consumer Credit Data from an individual consumer may provide TransUnion with the consumer's general particulars (name, sex, address, contact information, date of birth, Hong Kong Identity Card number or travel document number) and credit application data (the fact that the individual has made an application for consumer credit, the type and the amount of credit sought) according to Clauses 2.4.1 and 2.4.2 of the Code. There are two ways for the Subscribers to supply the Consumer Credit Data to the Database System, namely on-line contribution for data pertaining to a single consumer and batch contribution for data pertaining to multiple consumers. TransUnion receives updated Consumer Credit Data from its Subscribers in batches on a monthly basis.

4.8 Another source of consumers' personal data is public information such as those relating to actions for the recovery of debts or judgments for monies owed by consumers and declaration or discharge of bankruptcy about consumers that are available in the Government Gazette, records of IVA in the Official Receiver's Office ("**ORO**") and civil actions in Court Registry.

4.9 Further, TransUnion receives personal data from consumers from time to time where the consumers submit applications for correction of their personal data to TransUnion.

Use of Data

4.10 TransUnion provides Consumer Credit Data in response to Subscribers' credit check enquiries made through the following ways:-

(1) Host to host enquiry – Enquiry for and provision of a single credit report via a dedicated lease line between the Subscribers and TransUnion.

(2) PC online enquiry – Enquiry for and provision of a single credit report via a web-based application.

(3) Batch enquiry – Enquiry for and provision of multiple credit reports via electronic file submission through a proprietary Email function of TransUnion's computer system.

4.11 A typical credit report supplied pursuant to a Subscriber's enquiry of a credit report of an individual contains the following information:

(1) Name, Hong Kong Identity Card number or travel document number, date of birth, gender, current and previous addresses and telephone numbers.

(2) Types of credit accounts, repayment history records, credit limits and outstanding balances.

(3) Delinquent account information such as type of credit, the amount involved, date of default and date of repayment.

(4) Hire-purchase information on vehicles, vessels and equipment.

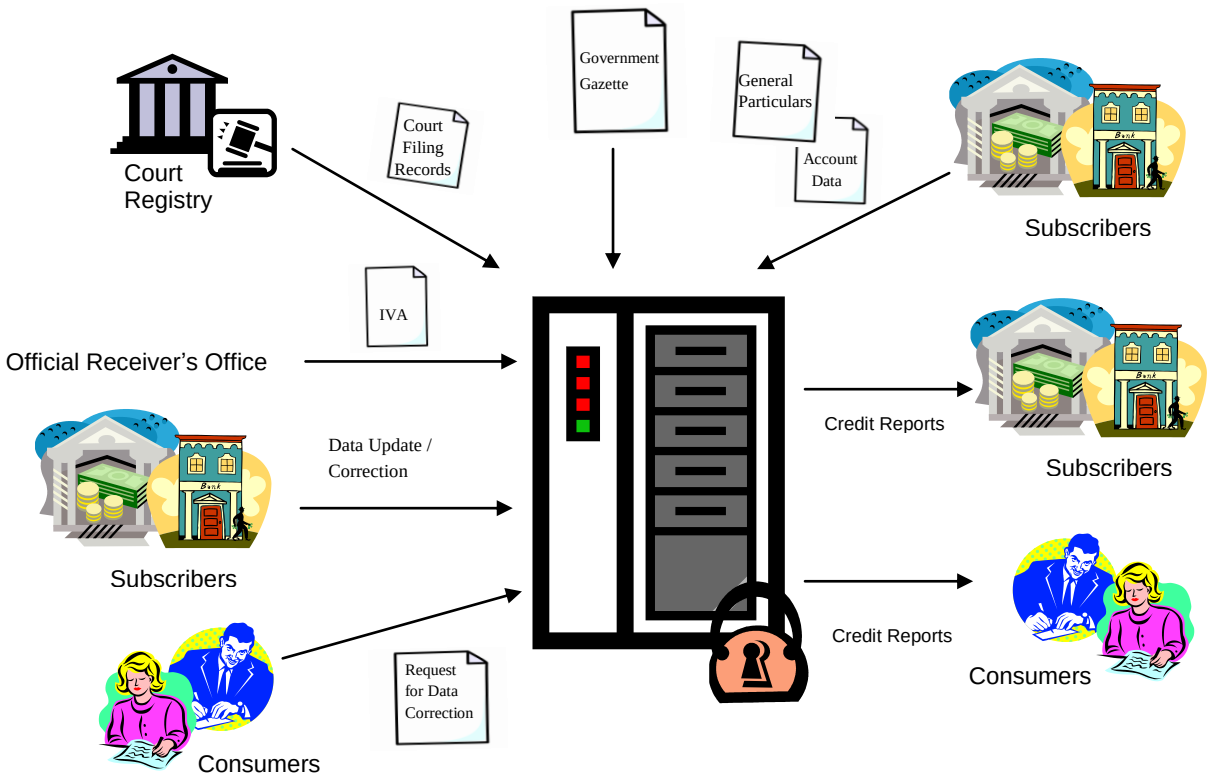
(5) Public records such as court actions, bankruptcy and winding-up petitions.

(6) Names of Subscribers that have accessed the credit report within the last two years.

(7) Credit score.

4.12 Consumer Credit Data are also provided to consumers in the form of credit reports upon requests. The form of a typical credit report downloaded from www.transunion.hk is in *Annex C*. The requests can be made and the credit reports provided in person, by mail or through its online system at a fee.

4.13 The flow of Consumer Credit Data into and from the personal data system of TransUnion is illustrated below:



Chapter Five

Findings and Recommendations

5.1 The findings of the Commissioner in the Inspection are divided into two categories. The first category is "specific findings", being findings on the level of compliance with the relevant DPP of the Ordinance and the Code by TransUnion in the processing cycle of the Consumer Credit Data in its personal data system. The second category is "other findings" in the Inspection in relation to the handling of consumer's personal data other than Consumer Credit Data by TransUnion.

5.2 The observations, findings and recommendations made in this Report are based on the documents and information provided by TransUnion and the Team's own observations at the material time. They shall not be treated as exhaustive to cover every aspect of the operation of the personal data system of TransUnion, and shall only be regarded as verification of the compliance level of the matters in question at the time when the Inspection was carried out.

Specific Findings

5.3 In maintaining the consumer credit database, TransUnion is the data user who is required to comply with the six DPPs and the relevant requirements, in particular Part III, of the Code. Details of the six DPPs and Part III of the Code are set out in *Annex D.* In this Report, specific findings are arranged in the order of the six DPPs.

DPP1 – Purpose and Manner of Collection of Personal Data

Requirements under the Ordinance and the Code

5.4 DPP1 regulates the collection of personal data in respect of (i) the purposes for which and how much personal data may be collected; (ii) the proper means to be used in collecting the personal data; and (iii) the data user's

duty to inform the data subject details of the collection of personal data from the data subject. More specifically, DPP1(1) stipulates that:

> "*(1) Personal data shall not be collected unless –*
>
> *(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;*
>
> *(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and*
>
> *(c) the data are adequate but not excessive in relation to that purpose.*"

5.5 Given that the circumstances under which data users may collect personal data vary, the Ordinance does not specify the personal data that may be collected by data users. The types of personal data that may be collected by CRA, including TransUnion, are specifically provided under the Code.

5.6 Under Clauses 3.1.1 to 3.1.8 of the Code, TransUnion as a CRA may collect eight types of personal data, namely:

(1) General particulars of a consumer, i.e. name, sex, address, contact information, date of birth, Hong Kong Identity Card Number or travel document number;

(2) Consumer Credit Data, including the identity of the credit provider and the date of the providing of such data;

(3) Public record relating to any action for the recovery of a debt, judgments for monies owed and bankruptcy;

(4) A list of credit providers who wish to be notified and provided information to assist in debt collection if an individual in default has reappeared in the system;

(5) Record of credit provider's access to an individual's personal data held by the CRA;

(6) Credit score of individuals;

(7) Notification by the Transport Department that it has received an application from an individual for a duplicate vehicle registration document; and

(8) Any other personal data as described in Schedule 3 of the Code. At the time of the Inspection, no personal data is prescribed in Schedule 3 of the Code.[11]

5.7 A CRA who collects Consumer Credit Data other than the above eight permitted types of personal data for the consumer credit reference service is presumed to have contravened DPP1(1).[12]

The Team's Findings

5.8 The Team inspected the schema of the Database System. Based on the descriptions of the fields of data in the schema, it appeared to the Team that the data that may be stored in the Database System should fall within the seven types of personal data listed in Clauses 3.1.1 to 3.1.7 of the Code.

5.9 In respect of the collection of public record and related data, the Team noted that TransUnion collects a wide range of data from various sources, namely:-

(1) Collection from the Court Registry every weekday records relating to proceedings such as bankruptcy, companies winding-

[11] Descriptions of the eight types of personal data above are summarized in this Report for ease of reference only. For details, please refer to Clauses 3.1.1 to 3.1.8 of the Code.

[12] Footnote 23 of the Code states that "*If a CRA, for the consumer credit reference service which it provides, collects personal data other than those permitted under clause 3.1, this will give rise to a presumption of contravention of DPP1(1) under section 13(2) of the Ordinance*."

up, personal injuries, construction and arbitration, etc., according to the *Public Record Input Guide* of TransUnion.

(2) Collection from ORO once a week records relating to IVA, including debtors' names, Hong Kong Identity Card numbers, addresses, etc.; and

(3) Information contained in various notices (e.g. Notice of Bankruptcy Order and Notice of Summary Procedure Order) published in the Government Gazette every Friday, including names of the parties and the partial Hong Kong Identity Card numbers of the debtors.

5.10 The Team inspected the records TransUnion collected from the Court Registry on 1 and 26 February 2010. Both dates were randomly selected by the Team. The Team noticed that the records included filing records of proceedings relating to debt recovery, personal injuries, companies winding-up, tax claims and bankruptcy filed on the previous working days. Some of the records were not approved as input to the Database System as they were "*non-debt related*" or the individuals' names were in Chinese. Most of them were approved to be inputted in the Database System.

Commissioner's Observations and Comments

5.11 In general, the Commissioner is satisfied that the Consumer Credit Data that TransUnion may and does collect are within the scope of data that may be collected by it under Clause 3.1 of the Code. However, the Commissioner has reservation on the collection of personal data from the Court records of proceedings relating to personal injuries and companies winding-up.

5.12 Under Clause 3.1.3 of the Code, the official records that are publicly available and may be collected by TransUnion are those relating to (i) any action of the recovery of a debt; (ii) judgments for monies owed entered against the individual; and (iii) declaration or discharge of bankruptcy.

5.13 Obviously, filing of a company winding-up proceedings does not relate to any of the three categories specified in Clause 3.1.3 of the Code. Further, it is arguable that filing of a personal injury claim, which by its nature is a claim for *damages*, should not amount to an action of the recovery of a *debt*.

Recommendation

(1) To ensure compliance with Clause 3.1 of the Code and DPP1(1), so that only adequate data are collected for the purpose of providing consumer credit reference services, TransUnion should:

(a) cease to keep and collect the Court records of proceedings relating to companies winding-up and personal injuries ("**the Court Records in Question**"); and

(b) completely erase and destroy the Court Records in Question that are already in the Database System, and amend the *Public Record Input Guide* and / or other relevant policies, guidelines and procedures of TransUnion to ensure that the Court Records in Question will not be collected in the future.

DPP2 – Accuracy and Duration of Retention of Personal Data

DPP2(1) – Accuracy of Personal Data

5.14 Accurate assessment of the creditworthiness of consumers is without doubt the whole purpose of the maintenance and utilization of the consumer credit database. This in turn depends upon the accuracy of the Consumer Credit Data. Inaccurate Consumer Credit Data of a consumer may not only prejudice the consumer, but may also increase the credit risk of credit providers.

Requirements under the Ordinance and the Code

5.15 DPP2(1) requires data users to, among other things, take all reasonably practicable steps to ensure that the personal data are accurate having regard to the purpose (including any directly related purpose) for which the

personal data are or are to be used. Given the importance of the accuracy of Consumer Credit Data, TransUnion is expected to take particular care in complying with DPP2(1).

5.16 The obligation to ensure accuracy of the Consumer Credit Data supplied by Subscribers to TransUnion is on the Subscribers themselves. Under Clause 2.5 of the Code, Subscribers of TransUnion are required to check the accuracy of the data before supplying them to TransUnion, and they are under a continuing obligation to update such data.[13]

5.17 The Code does not impose specific obligation on TransUnion to ensure the accuracy of the Consumer Credit Data. However, TransUnion is still required to comply with the requirements under the Ordinance on the accuracy of the data it compiled, e.g. accurate recording of the data collected from public records.

The Team's Findings

5.18 For Consumer Credit Data supplied by Subscribers, the Database System of TransUnion performs automatic data verification process in accordance with its *Name Editing Procedure*, *Account Contribution Batch Processing Procedure* and *Credit Check Batch Processing Procedure*. For instance, under the *Name Editing Procedure*, the Database System will automatically reject data not in valid format (e.g. name contains symbols like "%") and will identify potential mistakes (e.g. a name with "To" as the first name and "Sze" as the last name). The Database System would then generate a batch processing report showing details of the records rejected and send the report to the Subscribers for their verification and re-submission, where appropriate.

5.19 Court records are inputted in the Database System based on the photocopies made of the records. For IVA records, TransUnion assigns two employees of the DAD to copy the records by hand and based upon these

[13] Clause 2.5 of the Code provides that "*Before a credit provider provides any consumer credit data to a CRA, it shall have taken reasonably practicable steps to check such data for accuracy. If subsequently the credit provider discovers any inaccuracy in the data which have been provided to the CRA, it shall update such data held in the database of the CRA as soon as reasonably practicable*".

manually prepared records the relevant data are entered into the Database System.

5.20 According to the *Quarterly Public Record Audit Procedure* of TransUnion, the Data Quality Assurance Officer would randomly select 200 approved public records of various types in the Database System quarterly to check against the images of the copied public records.

5.21 The Team randomly selected the IVA records copied by TransUnion's staff by hand on 23 March 2010, compared them with the records kept by ORO and found the following discrepancies:-

Item	Court /Writ Type & Nos	Handwritten IVA Record in TransUnion	Record in the ORO's public register (i.e. correct data)	Data inputted in Database System
1.	IVAxxxx/2009	x 穎 x	x 頌 x	N/A (Chinese characters not inputted)
2.	IVAxxxx/2009	x 權 x	x 耀 x	N/A (Chinese characters not inputted)
3.	IVAxxxx/2009	Kam x x	Kan x x	Debtor's surname was wrongly inputted as "Kam"

Commissioner's Observations and Comments

5.22 It is good to note that TransUnion's Database System has incorporated features which detects possible inaccuracies in the Consumer Credit Data provided by the Subscribers and their *Public Record Input Guide* serves to guide its staff to input relevant Court records in the Database System correctly. The quarterly random check of public records inputted in the Database System also enables TransUnion to make necessary corrections in a timely manner. There is however room for improvement in ensuring accuracy in copying IVA records.

5.23 To ensure that the IVA records inputted in the Database System are accurate, reasonably practicable steps have to be taken to ensure that the

records copied manually by TransUnion's staff are accurate. From the discrepancies identified above, it is apparent that mistakes were made in the present arrangement for copying the names of the debtors.

5.24 TransUnion advised the Team that staff responsible for copying the IVA records had been instructed to copy the records in a "*clear and legible*" manner, but this is clearly not adequate in preventing mistakes in copying the IVA records. It is prudent and reasonable for TransUnion to incorporate procedures to cross-check the handwritten records compiled by their staff.

Recommendations

(2) To ensure the accuracy of the data copied from public records by hand, including the IVA records, TransUnion should:

(a) take practicable steps to cross-check that the records prepared are accurate, for example, by requiring its two staff members responsible for copying the public records to cross-check the copied records of each other against the public records on the spot;

(b) devise policy or procedural guidelines for copying public records by hand.

DPP2(2) – Retention of Personal Data

Requirements under the Ordinance and the Code

5.25 Under section 26(1) of the Ordinance, once the personal data collected are no longer required for the purpose (including any directly related purpose) for which they were used, they have to be erased. This ties in with DPP2(2), which stipulates that personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

5.26 The retention periods of the specific types of Consumer Credit Data are specified in Clauses 3.2 to 3.7 of the Code and are summarized as below:-

Data	Retention Period	The Code (Clause)
Account General Data	As long as there remain any account repayment data relating to the same account	3.2
Account repayment data revealing a default period in excess of 60 days	5 years from the date of final settlement of the amount in default; or 5 years from the date of the individual's discharge from bankruptcy	3.3.1 3.3.2
Account repayment data not revealing a default period in excess of 60 days	5 years from the date of creation of such data, provided that if the account is in the meantime terminated, then the CRA may continue to retain the account repayment data in its database until the expiry of 5 years after account termination	3.4
Account Data	TransUnion shall not retain if (i) a Subscriber requests TransUnion to delete the Account Data within 5 years after termination of account; and (ii) there was no material default (default period in excess of 60 days) in the relevant account within 5 years immediately before account termination	3.5
Public record and related data except data relating to a declaration or discharge of bankruptcy	7 years from the date of the event shown in the official record	3.6.1
Public record and related data relating to a declaration or discharge of	8 years from the relevant declaration of bankruptcy	3.6.2

bankruptcy		
Credit application data	5 years from the date of the reporting of the application	3.6.3
Credit card loss data	5 years from the date of report of the loss of the credit card	3.6.4
File activity data	5 years from the date of creation of such data	3.6.5
Credit score data	Until the end of the next business day following the date of creation of such data	3.6.6
General particulars of an individual	As long as there are other Consumer Credit Data related to the individual contained in the database of a CRA	3.6.7
Consumer Credit Data to which exemption from DPP3 and section 62 [14] of the Ordinance applies	TransUnion may continue to retain the consumer Credit Data for so long as such exemption applies	3.7

The Team's Findings

5.27 To ascertain that the Consumer Credit Data are not retained by TransUnion longer than is necessary under the Code, a number of interactive queries were conducted during the Inspection. Given that the number of records held in the Database System is huge, it was not practicable to examine each and every record in the Inspection. Instead, direct access to the backend database was arranged so that the data to be examined could be generated quickly, sorted, searched and compared easily.

5.28 In the interactive queries, the Team generated and sorted according to retention periods of the repayment records, Court records, credit application records and file activities data. None of these records seemed to have been

[14] Section 62 of the Ordinance provides that "*Personal data are exempt from the provisions of data protection principle 3 where-*
(a) the data are to be used for preparing statistics or carrying out research;
(b) the data are to be used for preparing statistics or carrying out research;
(c) *the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them.*"

retained for a period longer than that specified in Clauses 3.3.1, 3.3.2, 3.4, 3.6.1, 3.6.2, 3.6.3 and 3.6.5 of the Code.

5.29 On the other hand, the Team's findings in respect of Account General Data, credit card loss data, credit score data and general particulars of an individual are set out below:-

(1) Account General Data and general particulars of an individual should not have been kept if there is no more relevant account repayment data or Consumer Credit Data in the Database System. Samples of Account General Data and general particulars of an individual were examined and no irregularities against the data retention requirements under Clauses 3.2 and 3.6.7 of the Code were found;

(2) No test for credit card loss data (Clause 3.6.4 of the Code) was carried out because, as confirmed by the Team's examination of the schema and informed by TransUnion, they are not kept by the Database System at all; and

(3) Credit score data (Clause 3.6.6 of the Code) was generated every time a credit report is requested and not stored in the Database System. Therefore, the data do not appear to have been retained by TransUnion at all.

5.30 Regarding Clause 3.5 of the Code on the deletion of terminated account data on request by Subscribers, the Team notes that this deletion request by Subscribers rarely occurred and the Team examined the paper log of such request and verified that the recent few requests over the previous months had been executed and the associated data could not be found in the Database System.

5.31 The Team was given the understanding by TransUnion that TransUnion did not hold any exempted data described under Clause 3.7 of the Code. TransUnion confirmed that it did retain Consumer Credit Data for the purpose of the development of credit scoring model but all the retained data

had been anonymised. The data warehouse system was subsequently checked and found not to contain any personal data.

5.32 Based on the observations and results of the interactive queries conducted in the Inspection, no excessive retention of the Consumer Credit Data against the specifications in Clauses 3.2 to 3.7 of the Code was found.

5.33 Apart from the data stored in the Database System, TransUnion also collects personal data of consumers who had made requests for their credit reports and for correction of data. Such requests are made through "Application Form of Credit Information Record" (for in-person application), "Consumer Credit Report Access Form" (for mail-in application) and "Personal Data Correction Form".

5.34 According to the *DAR Application Handling Procedure* and the *DCR Processing Procedure*, hardcopies of the "Application Form of Credit Information Record", "Consumer Credit Report Access Form" collected should be kept for 3 months and the "Personal Data Correction Form" would be kept for 1 year. Both procedures are silent as to the retention period of the documents in support of the requests, e.g. a notice of discontinuance submitted by a consumer proving that he has been discharged from a legal action.

5.35 In processing consumers' requests for correction of their data, both the CRD and DAD would keep records of the "Personal Data Correction Form" and supporting documents. In the Inspection, the Team found that while CRD would keep the "Personal Data Correction Form" and supporting documents for 1 year according to the *DCR Processing Procedure*, DAD would keep the same documents for 2 years.

Commissioner's Observations and Comments

5.36 Consumer credit database contains huge amount of personal data and requires prudent management and reliable technical support to ensure that each of the relevant data are not kept longer than is required under the Code. The Commissioner is pleased to find in the Inspection that TransUnion seems to have met the requirements under the Code.

5.37 Obviously, the "Personal Data Correction Form" and the supporting documents are collected by TransUnion for the purpose of processing consumers' requests for correction of their data maintained in its Database System. It should be understandable that TransUnion may need to keep the relevant documents for a reasonable period of time after completion of the requests so that they may need to be referred to in case of a dispute. The retention period of the relevant documents should be strictly followed by all of TransUnion's staff, and DAD should not keep them for one more year than CRD.

Recommendation

(3) To ensure that the personal data submitted by consumers in the course of requesting for credit reports or correction of their personal data are not kept longer than is necessary, TransUnion should:-

(a) specify clearly in their relevant policies and procedures the retention period for the request forms and the supporting documents; and

(b) direct DAD in writing not to keep the "Personal Data Correction Form" and its supporting documents for more than 1 year and to completely destroy those that have been kept for more than 1 year.

DPP3 – Use of Personal Data

Requirements under the Ordinance and the Code

5.38 DPP3 provides that personal data may only be used (the term "use" includes disclosure or transfer under the Ordinance) (i) for the purpose that is the same as or directly related to the purpose for which the data were to be used at the time of collection; or (ii) otherwise with the data subject's express and voluntary consent.

5.39 The Code provides for more specific guidance on circumstances under which Consumer Credit Data may be used by a CRA. According to the Code, TransUnion may allow Subscribers to access the Consumer Credit Data:

(1) For provision or update of the data;[15]

(2) Through a credit report, in the course of (i) considering any grant of consumer credit; (ii) review of existing consumer credit facilities granted; or (iii) renewal of existing consumer credit facilities granted, to the consumer as borrower or an individual as a guarantor;[16] and

(3) For reasonable monitoring of the indebtedness of a defaulting borrower or guarantor.[17]

5.40 In the situations set out in paragraphs 5.39(2) and (3) above, TransUnion may provide certain specific data in the credit report.[18] In addition, TransUnion may use the Consumer Credit Data for the following purposes in providing consumer credit reference services:-

(1) To provide notice and information to a Subscriber on a watch list, when new data of the individual in default have appeared in the Database System, to assist in the Subscriber's debt collection action;

(2) To provide notice to a relevant Subscriber 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;

[15] See Clause 2.8 of the Code.
[16] See Clause 2.9.1 of the Code.
[17] See Clause 2.9.2 of the Code.
[18] Credit application data, credit card loss data and file activity data, created for not more than 2 years, and account data and their derivatives. See Clauses 3.8.1 and 3.8.2 of the Code.

(3) To provide a report to insurers in relation to insurance cover for property related to a consumer credit transaction;

(4) For reasonable internal management purposes, such as the defence of claims and the monitoring of the quality and efficiency of its service; or

(5) To carry out consumer credit scoring.[19]

5.41 Access to Consumer Credit Data by a Subscriber for direct marketing of goods, facilities or services to a consumer is expressly prohibited under Clause 2.12 of the Code.

The Team's Findings

5.42 There are three methods for Subscribers to make credit checking enquiries with TransUnion. The first two methods are made through emails within the Database System environment in the form of "host-to-host enquiry" about a single consumer and in the form of "batch enquiry" about multiple consumers.

5.43 The third method is "PC on-line enquiry". According to the written operation procedure *On-line Credit Check Enquiry Handling Procedure*, it would only be available if a Subscriber is unable to use the first two methods, e.g. breakdown of the Subscriber's workstation. TransUnion advised the Team that, if the Subscriber's workstation broke down, it would immediately send a system consultant to the Subscriber's office to attempt to repair the workstation, and the *On-line Credit Check Enquiry Handling Procedure* would be followed only if the repair also failed. According to TransUnion, "PC on-line enquiry" has not been used by Subscribers for over two years.

5.44 The three methods of making credit check enquiries are used within the automated environment of the Database System. The Team randomly inspected the credit reports of three consumers generated by the Database

[19] See Clause 3.10 of the Code.

System for provision to Subscribers. The Team found that provision of the information contained in the reports to the Subscribers were permitted under the Code.

5.45 The Team also noticed from a demonstration conducted in the Inspection that the Database System would process the credit check enquiries from Subscribers if a purpose permitted under the Code was stated, and that the Database System would reject a request not supported by any reason.

5.46 In addition to credit reference services, TransUnion also provides consultancy services to credit providers subscribed to the services. According to TransUnion, the credit data kept by it are anonymised data and stored in a data warehouse. Based on the anonymised credit data, TransUnion will perform analysis and provide credit providers subscribing to the consultancy services with information such as credit management score and bankruptcy score (i.e. the risk of bankruptcy for a given repayment pattern), with a view to giving a holistic view (as opposed to account specific) on credit risk and assisting the credit providers to formulate their lending policy. TransUnion stressed that the anonymised data used for provision of the consultancy services do not contain consumers' identities nor could they be reverted to credit data identifiable with individuals.

5.47 The Team conducted a check on the data warehouse and confirmed that the schema contained no identifiable Consumer Credit Data. Moreover, TransUnion confirmed that it had never transferred any Consumer Credit Data to any other parties for direct marketing and/or other purposes.

5.48 TransUnion further confirmed to the Team that none of its Subscribers are from the insurance industry, and that it had never provided any report to insurers in relation to insurance cover for property related to a consumer credit transaction.

Commissioner's Observations and Comments

5.49 Consumer Credit Data are made available to credit providers so that they can make more accurate assessment of the creditworthiness of potential or

existing consumers. The Code permits access by credit providers for certain purposes only, e.g. consideration of a grant of consumer credit and review of existing credit facilities.

5.50 The Commissioner is generally satisfied by the information obtained from the Inspection that TransUnion has been using the Consumer Credit Data in accordance with the requirements under the Code.

5.51 Since the consultancy services currently provided by TransUnion may not be directly related to the purposes for which the Consumer Credit Data were provided to it, TransUnion should continue to take extra care in ensuring that no personal data are used in the provision of the consultancy services.

DPP4 – Security of Personal Data

Requirements under the Ordinance and the Code

5.52 Under DPP4, data users are required to take all reasonably practicable steps to ensure that personal data they hold are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to, among other things, the kind of data and the harm that could result if such irregularities should arise and the security measures incorporated into any equipment in which the data are stored. The requirement is not to impose an obligation on data users to provide absolute security of personal data, but the steps taken to safeguard security should be proportionate to the sensitivity of the personal data involved.

5.53 The Code requires TransUnion as a CRA to take a number of security measures to safeguard against any improper access, including:-

(1) Entering into a formal written agreement with the Subscriber specifying the duty of both parties to comply with the Code, conditions under which the Subscriber may access Consumer Credit Data and the controls and procedures to be applied when the Subscriber seek access to TransUnion's Database System. (Clause 3.11.1);

(2) Training staff in relation to the requirements under the Ordinance and the Code and, in particular, good security practice (Clause 3.11.3);

(3) Developing written guidelines, and disciplinary or contractual procedures in relation to the proper use of access authorities by staff, external contractors or subscribers (Clause 3.11.4);

(4) Ensuring that adequate protection exists to minimize, as far as possible, the risk of unauthorized entry into the database or interception of communications made to and from the database (Clause 3.11.5);

(5) Regularly and frequently monitoring and reviewing usage of the database in order to detect and investigate any unusual or irregular patterns of access or use (Clause 3.12.2);

(6) Ensuring secure practices in relation to the deletion and disposal of data, especially where records or discs are to be disposed of off-site or by external contractors (Clause 3.12.3);

(7) Maintaining a log of all incidents involving a proven or suspected breach of security (Clause 3.12.4).

(8) Reporting any suspected abnormal access by a Subscriber (i.e. access on 5 or more occasions within a period of 31 days made by the same Subscriber seeking access to Consumer Credit Data of a particular individual) as soon as reasonably practicable to the senior management of the Subscriber and to the Commissioner (Clause 3.13.1); and

(9) Maintaining a log of all instances of access to its database by Subscribers including information such as the identity of the Subscriber seeking access, date and time of access, identity of the relevant consumer, reasons for access and reported instances

of suspected abnormal access to the senior management of a Subscriber and to the Commissioner (Clause 3.13.2).

The Team's Findings on Security Measures Generally

5.54 The Team inspected a standard subscriber agreement between TransUnion and its Subscribers and noted that there are specific provisions requiring:-

(1) TransUnion and the Subscribers to comply with all applicable laws or regulations, including, but not limited to, the Ordinance and the Code;

(2) Subscribers may access the Consumer Credit Data held by TransUnion only in the circumstances permitted under Clauses 2.9.1 and 2.9.2 of the Code;

(3) TransUnion maintains a list of persons authorized by the relevant Subscribers to access the Consumer Credit Data kept by TransUnion. These authorized persons were each assigned a security password for accessing the Consumer Credit Data. Only the persons authorized by the Subscribers may gain access to the Consumer Credit Data.

5.55 As regards training on the requirements under the Ordinance and the Code:-

(1) According to TransUnion, all its new staff are required to attend a staff orientation program in which the basic requirements under the Ordinance and the Code will be introduced. For departmental heads, one-on-one briefing is provided by the LC. The Team was provided with the attendance records of the staff orientation programs held in June 2008, October & November 2009 and March 2010.

(2) The Team was advised that TransUnion had held periodic Compliance Forums for Subscribers and managers of TransUnion on the provisions of the Ordinance and the Code. According to the filed presentation materials of TransUnion, such forums were held in October 2007 and November 2008. Besides, a centralized refresher workshops for the staff of TransUnion were held on 5 and 6 May 2010.

(3) According to the training materials of the staff orientation program and the refresher training, the Team found that the programs generally covered all the requirements under the Ordinance and the Code, and the attendance records showed that all the concerned staff had attended the trainings. Training materials of Compliance Forums also contained a general introduction of the Ordinance and the Code.

5.56 *The Security Policy (August 2005)* of TransUnion ("**the Security Policy**") requires that only authorized users have access to the Consumer Credit Data. For example, the Security Policy states that a user of the Database System should be allowed access only to those menu items he is authorized to access. It also requires the controlling of staff's and Subscribers' access rights to the Database System and that output containing Consumer Credit Data must only be sent to authorized terminals and locations including Subscribers' premises. As regards minimizing the risk of unauthorized access to the consumer credit database, the Team noticed that TransUnion has written guidelines, e.g. *Production Access Monitoring Procedure*, in place for its staff to review and monitor whether access to the Database System is authorized.

5.57 The Team noticed that every credit checking enquiry is logged by the *Enquiry Journal* (log for enquiry checks on individual consumer), *Maintenance Audit Journal* (log for accessing Consumer Credit Data and change transaction for each staff and Subscribers), *Daily Usage Journal*(log for enquiry checks, data access and change of staff and Subscribers with transaction descriptions) and *User Administration Audit Journal* (all transactions in relation to the change of user account and access rights of the Database System for staff and Subscribers). The Team was advised that these Journals were reviewed by the

Manager of the OD on a daily basis according to the procedure *Monitoring of Abnormal Access*.

5.58 TransUnion has set up a Security Committee overseeing and reviewing existing policies concerning data security issues. The responsibilities of the Security Committee include the review of the operational procedures for granting applications' user access rights to staff of TransUnion and Subscribers. On 21 April 2010, TransUnion informed the Commissioner that the Security Committee had recently devised a policy prohibiting new staff from handling personal data during probation period.

5.59 Among the signed "2000Plus System Transaction Authority Application Forms" the Team inspected, the Team found that a new user account was created on 31 May 2010 with access rights to Consumer Credit Data. However, this new user was not found from the "User List" of the staff who have access right to the Database System.

5.60 TransUnion confirmed that the new user joined TransUnion in early June and explained that the head of each department may decide when to grant new staff access to the Database System of TransUnion based on his/her business needs.

5.61 The Team conducted documentation review in respect of the Database System to examine the adequacy of control measures adopted to protect Consumer Credit Data by TransUnion. The review covered general security and IT security policies, network diagrams, system architecture documentations, numerous operating procedures from access control, backup tape arrangements to logs reviewing.

5.62 In general, the Team noted that TransUnion had in place a list of comprehensive IT related policies and procedures required to be followed by its staff. This general observation was based on the following checks and examinations carried out by the Team:-

(1) Evaluation of job functions against the paper printout of the Database System access rights to check if users (staff) were given the appropriate access rights;

(2) Paper evaluation of Database System account creation records to check if appropriate authorities were obtained before accounts were created, and that they were created with the correct access rights;

(3) Spot-check of Database System access right online against users' job functions;

(4) Spot-check the development and testing database to ascertain if they contain any real personal data;

(5) Discussion with individual staff to ascertain if they are familiar with the relevant operating procedures, security requirements and compliance requirements;

(6) Examination of backend database contents and their corresponding credit reports destined for consumers and Subscribers to check if they are the same;

(7) Paper evaluation of the effectiveness and comprehensiveness of previous audit/compliance checks, and of working documents to ascertain the accuracy of audit/compliance checks on log examinations; and

(8) Observation of the entire process of handling the backup tapes (including the identification of the correct tapes, their sealing and transportation to the secured off-site storage location) in order to ascertain if the processes were sound and followed the written procedures.

5.63 During the Inspection, no notable abnormality or discrepancy was found relating to compliance with security procedures. TransUnion was found to have followed the procedures on the basis of the checks performed.

5.64 TransUnion was found to have a multi-layer approach to IT security compliance and assessment, with a number of specific operational reviews carried out each year covering the compliance of user (staff) access rights, journal/log reviews, data retention rules reviews etc. On top of the regular internal review, TransUnion also commissioned an external party to carry out an annual compliance audit pursuant to Clause 3.14 of the Code. The scope of the compliance audit was restricted to the compliance with the Ordinance and the relevant clauses of the Code regarding CRA.

5.65 The internal audit department of TransUnion LLC conducted an IT Security Audit on TransUnion in 2008 with a focused scope. No further IT Security Audit seems to have been conducted after 2008.

Commissioner's Observations and Comments

5.66 Training on protection of credit data enhances the awareness of staff and Subscribers and plays no less important part in ensuring security of the Consumer Credit Data. This may be achieved by the periodic Compliance Forums organized by TransUnion. However, no such forum has been held since late 2008.

5.67 Given the sensitivity of Consumer Credit Data, the Commissioner considers it appropriate for TransUnion not to grant data access right to new staff who are still on probation. However, the fact as revealed in paragraph 5.59 above shows that its policy of prohibiting new staff from handling personal data during probation period was not strictly followed. Although heads of departments may exercise discretion to grant access to new staff based on their operational needs, relevant considerations in exercising the discretion and the reasons should be documented in the relevant policy and the "2000Plus System Transaction Authority Application Forms".

5.68 Given that TransUnion holds over 4 million people's sensitive credit data, TransUnion is expected to achieve a high standard of IT security for its entire operation, including but not limited to those systems and practice directly related to the Consumer Credit Data. Risk assessment and reviews at fixed intervals should be carried out in line the industry's best practice.

Recommendations

(4) TransUnion should resume the periodic Compliance Forums or organizing similar training as soon as practicable and on regular basis.

(5) TransUnion should set out in its relevant policy the relevant matters to be considered by department heads should they wish to deviate from TransUnion's policy of prohibiting new staff from accessing personal data during probation period. The reason for departure from the policy should be documented for individual cases.

(6) TransUnion should take a holistic approach to IT security audit and assessment by instigating a regular and independent IT security audit regime adopting the industry's best-practice such as the ISO/IEC 27002 Code of practice for information security management. The frequency of the IT security audit should also be increased.

The Team's Findings on Disposal of Electronic Storage Media and Storage of Backup Tapes

5.69 Erasure of data from electronic storage media such as optical disk, backup tape and hard disk is not a straightforward procedure. Nowadays, there are forensic detection tools in the market that enables one to retrieve data previously stored on the hard drive or other electronic storage devices even though they were thought to have been re-formatted and were blank. Therefore, it is important to ensure that confidential or sensitive data intended to be erased from the storage media are indeed erased and cannot be retrieved any more. For example, hard disk drives can be re-formatted according to industry standard so that residual data cannot be retrieved even with forensic tools;

magnetic backup tapes can be erased with a degaussing device by randomizing the magnetic patterns on the storage media, rendering data previously stored unreadable. For some storage media that cannot be sanitized, e.g. a CD-R discs, physical destruction is the best solution.

5.70 TransUnion has been engaging a vendor ("**the Data Disposal Company**") to dispose of TransUnion's electronic storage devices such as hard drives and magnetic backup tapes. Safe and complete disposal of electronic storage devices containing Consumer Credit Data is one of the most important aspects of the obligations of TransUnion in handling the Consumer Credit Data. Additional security measures should be taken where a third party is entrusted to dispose of the devices. According to TransUnion, the Data Disposal Company is the market leader in providing data degaussing and destruction services in Hong Kong. In the Inspection, the Team found some quotations and certificates of data erasure issued by the Data Disposal Company to TransUnion and photographs showing how TransUnion's electronic storage media were destroyed by the Data Disposal Company. According to these documents, the equipment passed by TransUnion to the Data Disposal Company for degaussing and destruction included hard disks and tape cartridges. Besides, TransUnion had assessed the Data Disposal Company's security level in data protection in 2007 by conducting a vendor security audit questionnaire with the Data Disposal Company before engaging their services.

5.71 Despite the importance of the work the Data Disposal Company is entrusted to perform, there is no comprehensive written service contract governing the security standard of the Data Disposal Company in relation to the degaussing and destruction services, and all disposals were done on an as-needed basis. TransUnion explained that it was not the Data Disposal Company's usual business practice to enter into any written agreement with their customers. TransUnion re-assured the Team that it had conducted security due diligence on the Data Disposal Company to ensure their compliance with TransUnion's *Corporate Security Policy* as its disposal vendor, and it also assigned its internal IT employee to monitor the entire destruction process carried out by the Data Disposal Company.

5.72 TransUnion performs automatic backup of its consumer credit database daily in magnetic tapes via a hardware device that will automatically encrypt the data to the AES 256-bit industry-standard before they are stored in the backup tapes. This renders the tape contents meaningless to anyone without the appropriate encrypting hardware and encryption key (the password) held by TransUnion.

5.73 TransUnion employed the Security Company to store the backup tapes in an off-site data vault managed by the Security Company. On 18 August 2010, the Team inspected the backup tapes storage process with representatives from TransUnion and the Security Company, including the collection and transportation of backup tapes from the TST Office to the secure storage location of the Security Company.

5.74 Backup tapes are recycled once every two weeks. The Security Company retrieves from its data vault the old backup tapes of TransUnion and returns them to TransUnion for reuse on each working day according to the collection schedule provided by TransUnion in advance. At the time the old tapes are returned to TransUnion, the Security Company collects from TransUnion the new backup tapes and stores them in its data vault.

5.75 TransUnion advised the Team that administrators of each of its computer system would check the backup result in the morning of each working day and notify the Network/Security Administrative Officer if any problem occurs. If the backup job was performed smoothly, the responsible IT staff would collect the corresponding backup tapes from the backup device of the Database System. Afterwards, the Network/Security Administrative Officer would put the backup tapes in a tamper-proof and serially-numbered plastic bag. The serial number and other details would then be entered in a log sheet named "Log of Backup Tapes to [Name of the Security Company]" except the consignment number which would be provided by the Security Company later.

5.76 The sealed plastic bag would ultimately be put in a security box ("**Outgoing Security Box**") with a label "TransUnion" on it (*Annex E*), locked with a plastic seal and a combination lock (the combination numbers were

known by TransUnion staff only), ready for collection by the security guards of the Security Company.

5.77 A security guard of the Security Company would arrive at the TST Office at a designated time to collect the Outgoing Security Box and return the backup tapes collected two weeks ago to TransUnion. The responsible staff of TransUnion would check if the security box received from the Security Company ("**Returned Security Box**") remains securely locked. If so, the security guard of the Security Company would cause a receipt to be signed by TransUnion. For the Returned Security Box, staff of TransUnion would record the consignment number as well as other information such as the serial number of the seal and the bag number, etc. on the "Log of Backup Tapes from the Security Company". Such information was checked against the record from the "Log of Backup Tapes to the Security Company" to ensure that the Returned Security Box was the same as the one sent out two weeks previously. Afterwards, he would take out all the backup tapes returned by the Security Company from the Returned Security Box and lock them in a cabinet inside the computer room.

5.78 The Team was given to understand that the Security Company uses its own transportation for delivery of the items entrusted to it. Before entering the Security Company's office, the Team was required to pass through a turnstile manned by a security guard. Besides, the whole premises was under CCTV monitoring at all times and all visitors are required to be escorted by the Security Company's staff. The Team observed that TransUnion's backup tapes were stored in a strong room equipped with access card system and CCTV cameras. Only authorized persons could enter the strong room to handle the security boxes storing the backup tapes.

5.79 The Team inspected the current service contract between TransUnion and the Security Company ("**the Service Contract**") and found no evidence showing that the Security Company had failed to handle the backup tapes of TransUnion in accordance with the terms and conditions prescribed by the Service Contract. The Team noted that the Service Contract does not specify the kind of transportation used by the Security Company to deliver the backup tapes of TransUnion.

5.80 In the morning of the Inspection on 18 August 2010, a member of the Team took a minibus from Kowloon Station to the TST Office and noticed that a male in the Security Company's uniform was on the same minibus carrying a security box. The member of the Team was not able to see any label marked "TransUnion" on the security box. As he was aware that the Security Company was the courier for TransUnion's backup tapes, he made a special mental note of the Security Company staff. It was revealed later on the same day in the Inspection that the male was the security guard of the Security Company responsible for carrying the backup tapes for TransUnion on that day and the security box under escort indeed contained old backup tapes to be returned to TransUnion on that day ("**the Incident**").

5.81 The Team was concerned that the use of public transport in conveying the tapes threw doubt on whether security safeguards were adequate. The Team passed its observations and concerns to TransUnion. TransUnion in turn directed the Security Company to investigate into the Incident.

5.82 The Team also found that under the Service Contract, the Security Company may open the locked security boxes and inspect the backup tapes TransUnion entrusted to it for delivery. It is understood that the Security Company may have a need to check the content of what it was entrusted to courier due to security reason. Also, the Service Contract does not require the Security Company to comply with the requirements under the Ordinance in handling the backup tapes nor does it set out any condition and circumstance under which the Security Company may inspect the locked security boxes. In addition, the Service Contract does not impose a duty of confidentiality upon the Security Company relating to the personal data contained in the backup tapes. Therefore, it is important to include specific terms in the Service Contract requiring the handling staff of the Security Company to protect the personal data in accordance with the requirement under the Ordinance.

5.83 TransUnion advised that the padlocks used for the security boxes were provided by TransUnion and the lock combination numbers were known to the authorized officer of TransUnion only. Therefore, the Security Company

should not be able to open the security boxes without TransUnion's authorization.

5.84 In relation to the Team's findings, TU has the following explanation and additional information:

(1) "*Both the disposal agent and [the Security Company] were chosen by us with care due to their good reputation in the market and being leaders in their respective businesses. As far as the disposal agent is concerned, while it would obviously have been ideal, we have not been able in the past to get them to enter into a 'comprehensive agreement' as disposals are done on an ad hoc basis and request for terms and conditions have been refused. However, that is not to say we do not have control procedures in place. As we have demonstrated during the Inspection, prior to selection of the agent, a thorough due diligence process was conducted in accordance with our corporate standards to make sure that the agent is competent, professional and reliable. Upon each disposal, one of our staff always accompanies and monitors the entire disposal process until it is done to our satisfaction and photos of the end result are taken for documentation. While contractual provisions can help us seek remedy in case of leakage of information, it is equally, if not more important, for us to accompany and monitor the whole process for compliance which is preventive and not remedial. We have also recently approached the agent again informing them of your recommendations and they are now willing to sign an agreement with us setting out the recommendations you made. In view of the importance of their service to our company and to the community in Hong Kong, we are hopeful that they will agree to our terms.*"

(2) "*As far as [the Security Company] arrangement for transfer of backup tapes is concerned, the incident of transporting the tape via public transport came as a big surprise to us and is to be regretted. Members from your office will also recall that when we first spoke to the supervisor of [the Security Company] about*

the incidence, even the supervisor did not know that the tapes on that day were transported other than by a dedicated car and was equally surprised as us. On subsequent investigation, we were informed by [the Security Company] that according to their usual business procedures, [the Security Company] vehicle should be used to transport the tapes unless there were unforeseeable circumstances. We were given to understand that the tapes had to be transported by public transport on that day due to exceptional circumstances, but we were assured that this was an exceptional incident and would not happen again in the future. In the meantime, we are already negotiating a new contract with them taking into account all your recommendations with additional undertaking that all tapes will only be transported by [the Security Company] vehicle. While we regret the incident, it was something out of the ordinary course of business and very exceptional even to the surprise of the supervisor in charge. We did not expect this to happen, but will do our best to ensure that this will not happen again. We are also considering practicable means of monitoring the transport of tapes in the future although a good practicable method is challenging."

Commissioner's Observations and Comments

5.85 Section 65(2) of the Ordinance stipulates that any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of the Ordinance as done or engaged in by that other person as well as by him.

5.86 Although safe keeping of the backup tapes and destruction of Consumer Credit Data are not carried out by TransUnion itself, it is potentially liable for the act done or practice of the Security Company and the Data Disposal Company under section 65(2) of the Ordinance, including a contravention of DPP4. As such, TransUnion should impose appropriate contractual obligations, including the duty of confidentiality, in its agreements

with third parties with a view to protecting personal data entrusted to them for storage or purging.

5.87 Given that the Data Disposal Company is entrusted with a huge amount of Consumer Credit Data for purging, the fact that no comprehensive written agreement was entered into between TransUnion and the Data Disposal Company at all, and that no duty of confidentiality is imposed on the Security Company and the Data Disposal Company is unsatisfactory.

5.88 Moreover, being a security specialist dedicated to protect customers' assets, the Security Company should use its own transportation for safe transportation of secured items entrusted to it. The Incident should call for serious and immediate attention of TransUnion. Additionally, the current practice of using the "TransUnion" label to identify the security boxes containing the backup tapes may unnecessarily indicate that their contents should relate to Consumer Credit Data, hence pose data security risk.

Recommendations

(7) TransUnion should enter into a comprehensive agreement with its data disposal agent with specific requirements on the security and safe disposal of the Consumer Credit Data entrusted to it. TransUnion should consider imposing a duty of confidentiality in the agreement on the Consumer Credit Data.

(8) TransUnion should work out with the Security Company detailed and appropriate measures to address the Commissioner's concerns arising from the Incident.

(9) TransUnion should impose a duty of confidentiality on the Security Company in their existing Service Contract with the Security Company. In any case, TransUnion should impose the duty of confidentiality in any future service agreement with its security agent for safekeeping of backup tapes.

(10) TransUnion should consider ceasing to use the "TransUnion" label to identify the security boxes.

The Team's Findings on Checking of Abnormal Access

5.89 According to the written procedure *Monitoring of Abnormal Access*, the Manager of the OD is responsible for verifying transactions of access by Subscribers to Consumer Credit Data logged in computer reports generated by the Database System every working day to check for "*Specific subscriber attempted to perform particular transaction without the respective authority consistently*" and "*Specific subscriber attempted to perform transaction during non-office hours consistently*". However, the written procedure does not define "non-office hours". If any such abnormal access to the Database System is found, the Manager of the OD is required by the *Monitoring of Abnormal Access* to report it to the Director of Legal & Compliance for immediate attention.

5.90 The Team interviewed the Manager of the OD who confirmed that there is no written guidelines or documentations specifying the "non-office hours". The Manager of the OD added that since Subscribers are allowed remote access to the Database System from 9 am to 9 pm, "non-office hours" for detecting abnormal access should be 10 pm to 8 am (next day). This, however, seems to be the personal judgment of the Manager of the OD only. While TransUnion subsequently advised the Team that "non-office hours" indeed means what the Manager of OD told the Team, this definition is not stated in any written policy or guidelines of TransUnion.

Commissioner's Observations and Comments

5.91 Monitoring access to consumer credit database at abnormal hours is a reasonable and effective measure to identify and deter unauthorized Subscribers' access. While the practice of TransUnion to monitor such access is welcome, the Commissioner found that the lack of a definition of "non-office hours" would likely lead to confusion and arbitrary practices, thus affecting the effectiveness of detecting suspicious access.

Recommendation

(11) TransUnion should define clearly "non-office hours" in its operation procedure *Monitoring of Abnormal Access* so that a uniform practice can be adopted by the staff in identifying and detecting suspicious access to the Database System.

DPP5 – Information to be Generally Available

Requirements under the Ordinance

5.92 DPP5 requires a data user to take all reasonably practicable steps to ensure that a person can (i) ascertain a data user's policies and practices in relation to personal data, (ii) be informed of the kind of personal data held by a data user, and (iii) be informed of the main purposes for which personal data held by a data user are or are to be used.

The Team's Findings

5.93 *TransUnion Privacy Policy* ("**the Policy**") is available on the official website of TransUnion (http://www.transunion.hk/privacypolicy_en.html). The Team noted that reasonably detailed information about the kind of personal data to be collected and the purposes for which they are or are to be used are stated in the Policy. The Policy further covers matters relating to retention, safe storage and transfer of personal data, access to and correction of personal data contained in credit reports.

5.94 TransUnion also makes its "*Notice to Individuals relating to the Personal Data (Privacy) Ordinance*" available to consumers visiting the TST Office. The notice summarizes the Policy by stating the kinds of data to be collected by TransUnion, the purpose of use of the data and the consumers' rights of access to and correction of their personal data.

Commissioner's Observations and Comments

5.95 The obligations of keeping one's personal data policies and practices transparent under DPP5 is particularly important for TransUnion as it engages in regular acts or practices that involve the collection of substantial amount of personal data in the course of its business or performance of its activities or functions. The Commissioner has not found any major issue that requires remedial action in relation to TransUnion's compliance with DPP5.

DPP6 – Access to Personal Data

5.96 An individual's right of access to his personal data held by a data user provides an important data protection means to him. Once the individual has ascertained what personal data the data user is holding, he should be able to see whether excessive data had been collected by the data user, and whether the data are inaccurate and need correction.

Requirements under the Ordinance and the Code

5.97 Under DPP6, a data subject is entitled to ascertain whether a data user holds his personal data, request for a copy of the data, and request for correction of the data if there is any inaccuracy. Requests for access ("**DAR**") and correction ("**DCR**") of personal data may be made pursuant to sections 18 and 22 of the Ordinance respectively. As for the time for data user's compliance with or otherwise respond to the DAR or DCR, it is prescribed under the Ordinance that the data user must do so within 40 days after receipt of the request:-

(1) Comply with the DAR or DCR (by correction and supply of a copy of the corrected data) (Sections 19(1) and 23(1) of the Ordinance);

(2) Inform the requestors where the data user is unable to comply with the DAR or DCR (Sections 19(2) and 23(2) of the Ordinance); or

(3) Inform the requestors if it refuses to comply with the DAR or DCR for the reasons prescribed by the Ordinance (Sections 21(1) and 25(1) of the Ordinance).

5.98 Clause 3.18 of the Code supplemented that where a DAR is made by a consumer who advises that he has been refused credit by a credit provider to whom a credit report has been provided by the CRA, the CRA shall, as a recommended practice, seek to respond promptly to the DAR, and where such DAR is made at the office of the CRA, a copy of the requested data shall, if practicable, be provided immediately, or else be dispatched by mail no later than 3 working days from the date of the DAR.

5.99 The Code further gives the following guidance to CRA on the handling of requests for correction of Consumer Credit Data:

(1) Where the Consumer Credit Data were provided by a credit provider:

Upon receiving the request, the CRA shall promptly consult the relevant credit provider, and if the CRA does not receive from the credit provider any written confirmation or correction of the disputed data within 40 days from the request, the relevant data shall upon expiry of 40 days be deleted or otherwise amended as requested (Clause 3.19 of the Code).

(2) Where the Consumer Credit Data were public record data:

Upon receiving the request, the CRA shall wherever practicable verify the accuracy of the data by checking the relevant public records. If the verification cannot be obtained within 40 days from the date of the request, the data shall upon expiry of the 40 days be deleted or amended as requested (Clause 3.20 of the Code).

The Team's Findings on Handling of Consumer's Requests for Credit Report and Correction of Personal Data

5.100 Under the current practice of TransUnion, consumers may request for access to their Consumer Credit Data by requesting for copies of their credit reports ("**Request for Credit Report**") at a fee. Where a consumer's new application for credit has been denied upon the Subscriber's consideration of his credit report supplied by TransUnion, TransUnion would supply a copy of the credit report to the consumer for free.

5.101 A Request for Credit Report may be made:

(1) In person at TST Office, which is regulated by *DAR Application Handling Procedure*;

(2) By mail, which is regulated by *Mail-in Application Handling Procedure*;

(3) On-line.

5.102 In order to observe how a Request for Credit Report made in each of the above three channels is handled, the Team caused the respective Request for Credit Report to be made in June 2010 without notifying TransUnion in advance.

(1) Request in person

The Team designated an individual to go to the TST Office to make a Request for Credit Report. After completing the "Application Form of Credit Information Record", the designated person was attended by different Consumer Relations Officers twice in an enclosed interview room (*Annex F*) in which his identity was verified before his credit report was provided to him. The entire process took about 40 minutes.

The Team interviewed 37 consumers who obtained their credit reports in person. All of the interviewees told the Team that the Consumer Relations Officers of TransUnion had checked their identification documents and asked them questions relating to their credit portfolio to verify their identities before releasing the credit reports to them.

(2) Request by mail

A person designated by the Team submitted the "Consumer Credit Report Access Form" to TransUnion by mail to request for his credit report. A staff of TransUnion contacted the designated person in about 4 days and asked the designated person certain questions concerning his credit information and contact information for identity verification purposes. The requested credit report was sent to the designated person by registered mail about two weeks afterwards.

(3) Request on-line

The Team arranged an online request for credit report to be made through TransUnion's official website (http://www.transunion.hk). After the designated person entered his personal particulars and answered questions relating to his credit portfolio, a password was sent to his mobile phone for creating an online user account to access his Consumer Credit Data. Through this account, he was able to gain access to the requested credit report on screen and print the report by himself.

5.103 All of the three credit reports obtained from TransUnion for the purpose of this Inspection were provided within 40 days of the requests and none of them contain any inaccurate data that require correction.

5.104 Both the *DAR Application Handling Procedure* and the *Mail-in Application Handling Procedure* do not require the handling staff to comply with the Request for Credit Report or otherwise respond to it within 40 days

after its receipt. TransUnion advised the Team that it had all along been able to provide credit reports to consumers within 40 days.

5.105 In the *DCR Processing Procedure*, it is stated that a consumer is required to complete and sign a "Personal Data Correction Form" that is available in TST Office and website, and that the time limit for data correction by TransUnion's staff and verification by Subscribers is "*1 working day*" and "*40 working days*" respectively. Moreover, the *DCR Processing Procedure* does not require its staff to provide a copy of the corrected data to the requestor or inform the requestor in writing if TransUnion is unable to make the correction within 40 days after receiving the "Personal Data Correction Form".

5.106 The Team randomly selected the *Follow-up Worksheet* (worksheet recording the work done in handling a personal data correction request) in relation to a personal data correction received by TransUnion on 12 April 2010. The Team noted from the *Follow-up Worksheet* that TransUnion was confirmed by the relevant Subscriber only on 27 May 2010 (i.e. 45 days after receipt of the correction request) that the data were correct. In the circumstances, it seems that the relevant correction request might not have been complied with within 40 days.

Commissioner's Observations and Comments

5.107 Verification of the identity of a consumer is important to ensure that the Consumer Credit Data are released only to the relevant data subject (consumer). The Commissioner is pleased to note that no irregularity was observed in this verification process.

5.108 The Commissioner is concerned that, by requiring its Subscribers to verify the personal data requested for correction within "*40 working days*" as specified in the *DCR Processing Procedure*, TransUnion may be running an unnecessary risk of failing to comply with a DCR within 40 days, hence, contravening the requirements under the Ordinance. First, the calculation of 40 days under the Ordinance should be calendar days instead of working days; second, if the Subscriber could only make the verification close to the expiry of

the 40 days, correction and supply of the corrected data within 40 days would be difficult.

5.109 Although TransUnion advised the Team that it had all along been able to comply with the personal data correction request within 40 days, appropriate amendments should be made to the *DCR Processing Procedure* to ensure that the personal data correction requests could be complied with within 40 calendar days.

5.110 It is important for the staff handling the Request for Credit Report and personal data correction request to be fully aware that the requests should be complied with or appropriate notifications should be sent within 40 days. Without spelling out the time limit in the relevant operation procedures, TransUnion will create a risk of contravening the requirements under the Ordinance in relation to DAR and DCR. It is an offence to fail to comply with a DAR or DCR in accordance with the requirements (including the requirement as to time) under the Ordinance. The Team considered that it would be a good practice for TransUnion to include in all its procedures in relation to the handling of Request for Credit Report and personal data correction request specific instructions requiring the handling staff to reply to the requestors within 40 days after their receipt.

Recommendations

(12) TransUnion should specify in the *DAR Application Handling Procedure, Mail-in Application Handling Procedure, DCR Processing Procedure* and all other relevant written procedures/guidelines the time period (i.e. 40 calendar days) within which the request for access to credit report or correction of the data should be complied with or to inform the requestors in writing the reason why TransUnion is unable or refuses to comply with the requests.

(13) TransUnion should disseminate the revised written procedures or guidelines to the staff involved in handling request for access to or

correction of credit report, and remind the staff such amended procedures or guidelines regularly through training sessions, issuance of internal notices/emails/circulars and/or departmental briefings, etc.

The Team's Findings on Comparing Credit Reports for Subscribers and Consumers

5.111 TransUnion may supply Consumer Credit Data requested by a consumer in the form of a credit report as long as the credit report contains the requested data. It is however important to bear in mind that while a consumer may use the Request for Credit Report form designed by TransUnion to make their access request, the consumer may also use the data access request form designed by the PCPD in exercising his data access right.

5.112 In the Request for Credit Report of TransUnion, requestors are only required to provide their personal particulars and contact information. It does not require them to specify the requested data.

5.113 Since Consumer Credit Data relate to the financial status and creditworthiness of a consumer, in ordinary circumstances the amount of Consumer Credit Data to which the consumer may have access should be no less than those may be accessed by the Subscribers.

5.114 Under the practice of TransUnion, access to Consumer Credit Data by consumers and Subscribers is by reading the credit reports supplied by TransUnion. In the Inspection, the Team requested TransUnion to randomly select three consumers and generate a credit report for consumer (*Annex G*) and another for Subscriber (*Annex H*) in respect of each of these consumers. The Team noted that the credit reports for Subscribers contain the last repayment amount. However, the same data were not included in the credit reports for consumers.

5.115 In addition, the Team noted that credit reports for consumers only stated the "Start Date" and the "Latest Date" of the period during which Subscribers had accessed the consumers' Consumer Credit Data (except those

arising from the consumers' credit application). In other words, details of *each* access (e.g. name of Subscriber, date and reason for access) were missing. For example, in a credit report for a consumer, under the item "Other Enquiry" the only record shown is "*XXX Bank made enquiries since dd-mm-yyyy (i.e. Start Date) regarding your xxx (i.e. type of credit) facility for the purpose of review of existing credit facilities granted. The latest enquiry was made on dd-mm-yyyy (i.e. Latest Date).*" However, the credit report of the same consumer for access by Subscribers listed each and every enquiry made by Subscribers on the consumer in the past 2 years.

5.116 In response to the Team's enquiries about the discrepancies on the levels of details shown in the credit reports for consumers and Subscribers, TransUnion explained that, in the past many Subscribers often provided inaccurate data in the field of "last repayment amount" during regular account data contribution to TransUnion via the Database System. As a result, TransUnion from time to time needed to seek clarifications from the Subscribers and to correct the data if necessary. Provision of more detailed information in the credit report for Subscribers facilitates both the Subscribers and TransUnion to correct the data. TransUnion stated that it did not display the last repayment amount in the credit report for consumers in order to avoid the inaccurate data being shown in consumers' credit report while they were under clarification.

5.117 As for the partial inclusion of "Other Enquiry" information in the credit reports for consumers, TransUnion explained that the number of enquiries involved could be repetitive and numerous. As a result, it might take up a large and disproportionate amount of space in the credit report and give a "distorted view" of the report to consumers. In any case, consumers have been informed in the cover page of their credit reports that *"full details of 'Other Enquiry Information' of the Credit Report are also available upon request"*.

Commissioner's Observations and Comments

5.118 One of the important purposes of giving an individual's right of access to his personal data is to enable him to detect any inaccuracy of his data and request for correction. As long as personal data of a consumer are held by

TransUnion and the data are requested by the consumer for access, TransUnion should comply with the request. Withholding part of the personal data from a consumer would defeat the purpose of the data access right of the data subject. The current practice of TransUnion in not disclosing the last repayment amount to consumers may deprive the consumers' right of access to their personal data and request for correction of any inaccuracy.

5.119 Withholding information about the past incidents of access made by Subscribers to the Consumer Credit Data of a consumer will also prejudice the consumer's interest. With the omission of the number of incidents of access, the identities of the Subscribers who made the access and the reasons for the access, the consumer may not be able to identify any suspicious access to his Consumer Credit Data, e.g. the consumer may not be able to raise timely objection to access to his Consumer Credit Data by a Subscriber to whom he has not applied for any new credit facility or requested for increase of his existing credit.

5.120 Unless details of previous access to his Consumer Credit Data are expressly excluded in the consumer's Request for Credit Report or not within the scope of such Request, the Commissioner sees no reason why such information should be withheld from the consumer only. The fact that TransUnion informs consumers in the cover page of the consumers' credit reports that they may request for the "full details" of "Other Enquiry Information" may be regarded as only delaying the consumer's request.

5.121 TransUnion should take notice that consumers' right of access to their personal data is protected and regulated under section 18 of the Ordinance. Mere provision of credit reports in a format dictated by TransUnion shall not be taken as compliance with a DAR under section 18 of the Ordinance. Personal data that are withheld by TransUnion from disclosing in the credit reports for consumers are subject to full disclosure when so requested by the consumers in a DAR made under section 18 of the Ordinance. In the Commissioner's view, all personal data including Consumer Credit Data should be disclosed in the credit report for consumers. Alternatively, options for full or partial disclosure should be given to the consumers when they requested for their credit reports.

Recommendation

(14) TransUnion should make full disclosure of account repayment data and details of each and every access made by Subscribers in the credit report for consumers. Alternatively, TransUnion should give an option to consumers to request for full or partial disclosure when they made a request for credit reports.

Other Findings

5.122 The following findings revealed in the Inspection are outside the processing cycle of Consumer Credit Data of TransUnion. They relate to the general measures adopted by TransUnion in personal data protection. Specifically, the findings concern the aspects of document control, training record management and handling of CCTV and telephone recordings.

The Team's Findings on the Policies and Procedures

Inaccurate Procedures – *Individual/Company Particular Updating Procedure* and *Account Maintenance Procedure*

5.123 The *Individual/Company Particular Updating Procedure* requires the Data Administration Support Team to process update request forms submitted by *Subscribers*, but is silent on the processing of *consumers'* requests for updating their own personal data. Similarly, the *Account Maintenance Procedure* relates to the handling of request for update and removal of accounts raised by *Subscribers* only.

5.124 However, the Manager of the DAD confirmed that in fact both the *Individual/Company Particular Updating Procedure* and the *Account Maintenance Procedure* require its staff to process requests for data updating or removal made by *consumers* as well. Apparently, the two procedures have omitted those parts relating to the handling of the relevant requests from consumers.

Outdated Procedure - *On-line Credit Check Enquiry Handling Procedure*

5.125 The Team inspected the *On-line Credit Check Enquiry Handling Procedure*, which covers the handling of on-line credit check enquiry from a Subscriber in the event that its workstation connecting to the Database System for performing host-to-host and batch credit enquiries breaks down.

5.126 According to the *On-line Credit Check Enquiry Handling Procedure*, a Subscriber would submit a formal written request for On-line Credit Check Enquiry with reason, and the responsible staff of TransUnion would review and check the signature of the requestor and the reason for the request. When the request is found in order, the handling staff would print the requested credit report and fax it to the requesting Subscriber. All the requested documents and the credit reports would be filed after completing the request.

5.127 However, this procedure has not been followed in practice for two years. The current practice of TransUnion is that it would first send technicians to the Subscribers to attempt to repair their workstations. The *On-line Credit Check Enquiry Handling Procedure* would be followed if the attempted repair fails.

5.128 The Team noticed that the *On-line Credit Check Enquiry Handling Procedure* requires the staff of the OD to fax the requested credit report to the Subscriber after performing the on-line credit enquiry procedure, but it does not give any directions or guidance on any necessary security steps to avoid transmission of the credit reports to unintended recipients. The Manager of the OD explained that the handling staff would call the requesting Subscriber before and after sending the credit report to confirm safe receipt of the credit report. However, the Team learnt from a handling staff during the Inspection that no such telephone calls would be made.

Inconsistent Procedure - *Mail-in Application Handling Procedure*

5.129 The Security Policy is the company's general policy and should be read by all staff of TransUnion. Section 3 of the Security Policy provides that staff are not allowed to ask for a copy of customer's identity card, but under the

Mail-in Application Handling Procedure, consumers requesting for their credit reports by mail are required to provide copies of their Hong Kong Identity Cards. Apparently, the *Mail-in Application Handling Procedure* is inconsistent with the Security Policy. TransUnion explained that section 3 of the Security Policy is applicable to request made in person only, but this is not spelt out in the Security Policy itself.

Commissioner's Observations and Comments

5.130 Policies, guidelines and procedures are integral parts of an effective and sound management system. They are relied on by all staff in carrying out their daily job duties, so that they know what should be done in a given situation, and consistent practices of the organization are ensured. It goes without saying that these policies, guidelines and procedures should be as complete as possible, not contrary to statutory requirements and not inconsistent among themselves. Any omission or error may result in serious adverse consequences.

Recommendations

(15) TransUnion should amend the *Individual/Company Particular Updating Procedure* and *Account Maintenance Procedure* so that the fact that they apply to updating and maintenance requests from *both* Subscribers and consumers is clearly stated.

(16) TransUnion should amend the *On-line Credit Check Enquiry Handling Procedure* to include:-

(a) The current practice of instructing technicians of TransUnion to repair the workstation of Subscribers before performing the on-line credit check enquiry; and

(b) Guidelines on the steps to take to ensure safe transmission and receipt of the credit report supplied through the on-line credit check enquiry.

(17) TransUnion should take immediate steps to make appropriate amendments to the Security Policy (and / or the *Mail-in Application Handling Procedure)* so that the circumstances under which copies of Hong Kong Identity Cards may or may not be collected are clearly set out and not inconsistent with each other.

The Team's Findings on the Maintenance of Training Records

5.131 TransUnion provides training in relation to personal data protection to its staff through its orientation courses and refresher courses for new recruits and existing staff respectively. Both the orientation courses and refresher courses cover the requirements under the Ordinance (including the six DPPs) and the Code. The Human Resources Department is responsible for providing the orientation training about once every 5 months. Refresher courses are provided by the LC from time to time. Every department may organize and design its own training courses. The Human Resources Department would assist in arranging all departments' training courses but would not maintain any record of attendance for such training.

Commissioner's Observations and Comments

5.132 TransUnion's core business is the maintenance of a huge consumer credit database. It has to ensure that its staff are given adequate training and updated knowledge on data protection. Having a designated body to coordinate the training and keep detailed training record for individual staff enables TransUnion to identify the training needs of the staff on a continuous basis.

Recommendation

(18) TransUnion should in so far as it is reasonably practicable to do so, designate a department or a group of staff in TransUnion to (i) coordinate the data protection training for its staff, (ii) keep training records of individual staff, and (iii) provide necessary training tailored to meet their specific needs.

The Team's Findings on the use of CCTV and the Telephone Recording Systems

5.133 TransUnion has installed for security purpose CCTV cameras in the waiting area and individual interview rooms in the CRD to record interview process between its staff and consumers applying for Credit Report.

5.134 TransUnion has posted on the glass partition of each interview room a notice bearing the warning "Surveillance Recording System in Use", but no such notice or any warning to this effect is posted in the waiting area.

5.135 TransUnion has also installed a telephone recording system to record the contents of all incoming and outgoing calls of its enquiry hotline. Callers of the enquiry hotline are informed that contents of the telephone conversation might be recorded for the purpose of "maintaining service quality".

5.136 TransUnion advised the Team that it was its practice to retain the CCTV video images and the audio recordings of telephone conversations for a period of 90 days and 12-months respectively. TransUnion supplemented that Section 5.1 of its *Corporate Security Policy* dated 31 October 2009 devised by the Information Security Department of TransUnion LLC recommended that *"Closed Circuit TV (CCTV) and intrusion monitoring of the Level 3 facility area, including exterior entrances…to be retained a minimum of 30 days."* In addition, Section 5 of *the Security Policy* provides that *"the monitoring records will be retained for a period of time in accordance with industry practice or recommended by the related regulatory guidelines. However, the monitoring records may be retained longer should circumstances render or on a case-by-case basis."*

5.137 The two policies cited by TransUnion do not specify the retention period of the video and audio recordings, nor do they particularize the kind of "industry practice" and/or "regulatory guidelines".

5.138 Moreover, TransUnion confirmed that it did not have any written procedures in place for handling DAR for personal data collected through the CCTV and telephone recording systems.

Commissioner's Observations and Comments

5.139 Since consumers should be made aware of their being captured by the CCTV, they need to be explicitly informed of this arrangement and of the purpose for which the recordings may be used and the classes of persons to whom the recordings may be transferred.[20] The existing warning printed on the notices is too general and does not serve these purposes adequately.

5.140 Without a written policy to govern the retention of the captured CCTV images and the telephone conversation recordings, it would be difficult for TransUnion to ensure systematic and prompt disposal and destruction of these data and this may result in their being kept for a period longer than is necessary, and possible contravention of DPP2.

5.141 Besides, consumers may exercise their rights under the Ordinance to request for access to any personal data collected through the CCTV and the telephone recording system. Without any written procedures or guidelines for the handling of such DAR, it would be difficult for the staff of TransUnion to process such requests properly and efficiently.

Recommendations

(19) In respect of the use of the CCTV system, TransUnion should explicitly inform the individuals who may be captured by the CCTV using conspicuous notices drawing their attention to:-

(a) The fact that they are subject to CCTV surveillance; and

(b) The purpose of use of the CCTV recordings.

[20] See DPP1(3).

(20) As regards the CCTV and the telephone recording systems, TransUnion should:

(a) Devise policies and/or procedures specifying the retention period of the captured CCTV images and the telephone conversation recordings;

(b) Identify in the policies and/or procedures the staff who is/are authorized to access the captured CCTV images and/or the telephone conversation recordings; and

(c) Establish policies and procedures in relation to the handling of DAR for the CCTV and telephone conversation recordings.

Chapter Six

Conclusion

6.1 Consumer Credit Data are very personal and confidential information and it is of paramount importance that TransUnion have adequate controls to protect them. With this in mind, the Commissioner carried out an examination of the personal data system used by TransUnion by way of an inspection under section 36 of the Ordinance, to review compliance with the six DPPs and the Code and to make recommendations to promote compliance.

6.2 Due to resource limitations, PCPD was only able to take snapshots of the operations of TransUnion. The matters raised in this Report are not therefore a comprehensive and exhaustive statement of all weaknesses that exist or of all improvements that could be made. PCPD is not in a position to provide assurance as to TransUnion's day-to-day operation of the procedures and internal controls.

6.3 Bearing the above limitations in mind, the Commissioner is pleased to find that TransUnion has in place comprehensive and detailed policies, guidelines and procedures on the proper handling of Consumer Credit Data, and no major data security issues were found in the Inspection. Senior staff who are responsible for handling of Consumer Credit Data are experienced and conversant with the policies, guidelines and procedures underpinning their duties. There are, however, rooms for improvement identified by PCPD and the Commissioner has made a number of recommendations, among other things, for TransUnion to enhance its system of control in the areas of data collection, accuracy, retention, security and access, as well as IT security audit. In particular, the Commissioner has noticed an obvious slack in control where disposal and storage of Consumer Credit Data were arranged through contractors. He has made specific recommendations to address the problems identified.

6.4 Whilst finalising this Report, a public consultation on the revision of the Code to tie in with the proposal of the financial services industry to share

positive mortgage data is under way. With an enlarged credit database and greater sharing and use of the mortgage data under this proposal, the onus on TransUnion to demonstrate the integrity and reliability of its data protection system is even higher. Against this background, the Commissioner urges TransUnion to take timely and appropriate actions to implement his recommendations made in this Report, and to be prepared to provide additional privacy safeguards commensurate with the proposed sharing of positive mortgage data.

6.5 The Commissioner wishes to thank all members of TransUnion, who have provided facilities, information and other assistance to the Team, without which this Inspection would not have been carried out as smoothly as it had been.

Annex A – List of persons interviewed

(1) Director, Legal & Compliance
(2) Director, Sales & Marketing
(3) Senior Director, IT & Operations (East Asia)
(4) Manager, Information Technology
(5) Manager, Data Administration Department
(6) Manager, Operations Department
(7) Manager, Customer Relations Department
(8) Senior System Analyst
(9) Supervisor, Operations Department
(10) System Architect, Application Development
(11) Network/Security Administrative Officer
(12) Database/System Administrative Officer
(13) Support staff, Data Administration Department
(14) Officer of Compliance Department
(15) Manager, Human Resources Department

Annex B – Questions asked during interviews with walk-in consumers at TransUnion's Consumer Relations Department and Statistics on consumer interview

Questions asked during interviews with walk-in consumers at TransUnion's Consumer Relations Department

(1) What is your purpose of obtaining the credit report?

(2) Briefly describe the process/procedure for obtaining credit report at TransUnion's office.

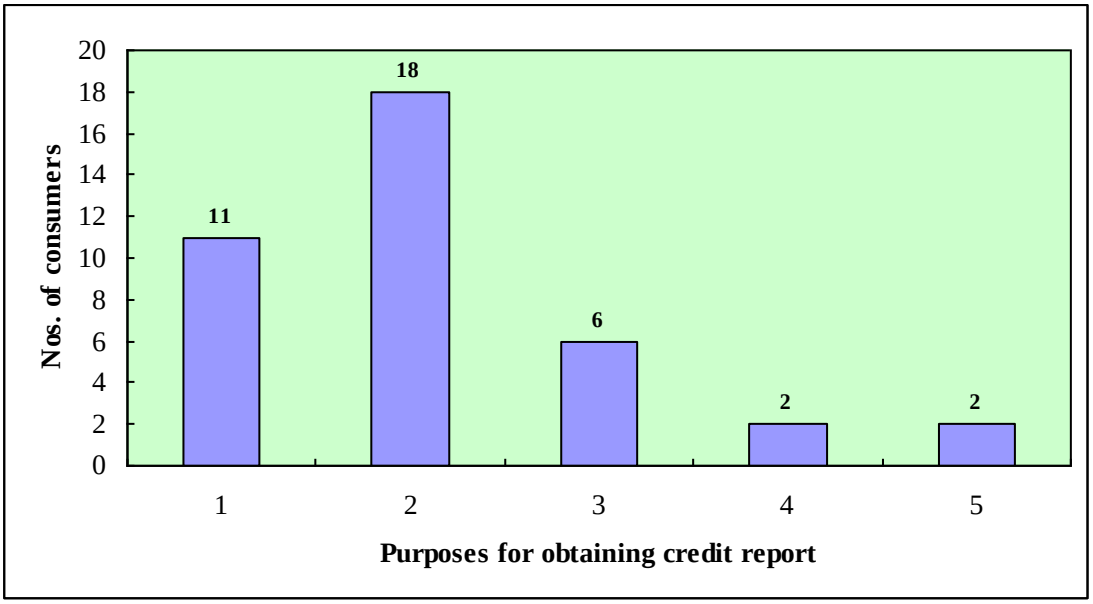
(3) How did the handling staff of TransUnion verify your identity?

(4) Did the staff explain the content of the credit report to you?

Annex B

Statistics on consumer interview

Purposes for obtaining credit report	Number of consumers
(1) Self-credit monitoring	11
(2) Job application / requested by employer	18
(3) Mortgage / loan application	6
(4) Debt repayment restructure / IVA	2
(5) Others*	2
Total Number:	37^



**Work visa application and checking the accuracy of the Consumer Credit Data*

^ one consumer stated that he/she obtained credit report for purposes 1,2 and 3

Annex C – Copy of credit report downloaded from www.transunion.hk

Credit Report for CHAN TAI MAN, A12345678 ID HKG

Here you will find the personal information contained in your credit file

1. Personal Information

The following is your personal information provided to us by TransUnion's members:

Name: CHAN TAI MAN
Identity No.: HONG KONG IDENTITY CARD A12345678
Date of Birth: 01-04-1975
Sex: MALE

1.1 Address History:

1.1.1 18C SKY BUILDING KOWLOON BAY
1.1.2 1101 LUCKY ESTATE SHATIN NT

1.2 Contact Number History:

1.2.1 86-100-98765432
1.2.2 90009999
1.2.3 23112300

1.3 Other Names Used:

1.3.1 PETER CHAN

1.4 Other Identity Document Number(s):

1.4.1 CANADA PASSPORT/TRAVEL DOCUMENT 13213213332

1.5 Directorship/Proprietorship/Partnership:

1.5.1 You are a Partner of POWERLINK COMPANY.

Here you will find the credit history and the current balance of your open, closed and past due credit accounts

2. Credit Account(s) Information

The following is your credit information provided to us by TransUnion's members:

2.1 Open Credit Account(s):

2.1.1 Hong Kong Island Bank Ltd. reported that on 12-05-2006, a Hire Purchase Loan HP16800A with credit amount of HKD 180,000 for 36 instalments of HKD 4,000 each was opened for you and that you had a credit relationship with them. You were a Principal of this commercial account.

Hong Kong Island Bank Ltd. made further reports on such account as follows:

On 11-11-2006, a scheme of arrangement was set up for 10 monthly payments of HKD 7,200 each.

On 30-06-2007, the outstanding balance of the account was HKD 28,800.

Credit Report for CHAN TAI MAN, A12345678 ID HKG

2.2 Closed Credit Account(s):

2.2.1 Capital Bank Ltd. reported that on 19-08-2006, a Private Label Card 000170886111xxxx with credit amount of HKD 20,000 was opened for you. You were a Principal of this consumer account.

On 30-04-2007, the maximum past due amount was HKD 5,500.

On 30-04-2007, the maximum past due days was 90.

Capital Bank Ltd. made further reports on such account as follows:

In 02-2007, it was past due for 30 day(s).

In 03-2007, it was past due for 60 day(s).

In 04-2007, it was past due for 90 day(s).

On 31-05-2007, it was advised that this account had been paid in full and closed.

2.3 Past Due Credit Account(s):

2.3.1 Bank of Credit Union Ltd. reported that on 13-02-2002, a Master Business Card 0000722447788xxxx with credit amount of HKD 30,000 was opened for you. You were a Principal of this consumer account.

On 15-05-2007, the maximum past due amount was HKD 12,000.

On 15-05-2007, the maximum past due days was 180.

Bank of Credit Union Ltd. made further reports on such account as follows:

In 05-2007, it was past due for 180 day(s).

On 15-05-2007, the past due amount of the account was HKD 12,000.

On 15-05-2007, the outstanding balance of the account was HKD 15,000.

On 15-05-2007, the account status was classified as 'Write-off'.

Here you will find the number of enquiries made by TransUnion's members into your credit file within the past 2 years

3. Credit Application(s) Enquiry Information

From our records, these are enquiries made by TransUnion's members arising from your credit application(s).

3.1 Asset Bank Ltd. made an enquiry on 13-07-2007 regarding your application for Hire Purchase Loan for the amount of HKD 180,000.

Credit Report for CHAN TAI MAN, A12345678 ID HKG

4. Other Enquiry Information

From our records, these are enquiries made by TransUnion's members other than those arising from your credit application(s). Please note that these enquiries do not impact on your credit score.

4.1 Bank of Credit Union Ltd. made an enquiry on 15-05-2007 regarding your Master Business Card for the purpose of monitoring of indebtedness.

4.2 Capital Bank Ltd. made an enquiry on 13-03-2007 regarding your Private Label Card for the purpose of renewal of existing credit facilities granted.

4.3 Hong Kong Island Bank Ltd. made an enquiry 10-10-2006 regarding your Hire Purchase Loan for the purpose of review of existing credit facilities granted.

The records are collected from the court, the filed bankruptcy petitions are maintained for 8 years, other public records for 7 years

5. Public Records of Potential Relevance

These are records that are publicly available from the court and are of potential relevance. Since no identity card number of the debtor/defendant is displayed on such records, we only matched such records with you by a comparison of English name and address only. TransUnion's members are aware of this fact and may use further means to verify this information.

5.1 Potentially Relevant Writ Information:

5.1.1 A Writ No. DCCJ3/2008 was taken out by WONG CHI KEUNG as plaintiff on 01-01-2007 in the Hong Kong District Ct for Rent & Surcharges.

Defendant 1 of the case: CHAN TAI MAN [as] the [sole/joint] trustee of/for DAVID LEE

The address of CHAN TAI MAN is 1) 1101 LUCKY ESTATE SHATIN NT

Notes:
1. words in square brackets, if any, refer to words that may or may not appear on the relevant public record
2. the use of "/" between words, if any, means the words are used together or separately on their own as appear on the relevant public record

Here you will find your credit score

6. Credit Score

Based on your credit data, your credit score as at 30-07-2007 falls into the C category. Statistically, in the period of the next 12 months, **99.58%** of population with such score will fulfill their commitment to make payment to credit providers.

Credit Report for CHAN TAI MAN, A12345678 ID HKG

Notes:

Credit score does not draw conclusion or provide credit decisions for credit providers. Credit score is only one piece of information used by credit providers in their credit assessment process. Other than the credit score, credit providers will also consider their own risk acceptance level in lending, their own internal credit score and the applicant's demographic and financial information. A credit score is a fluid number and is calculated based upon the latest information contained in a credit file at the time the score is requested. Since the credit information of a consumer may change from time to time, a score generated previously may not be the same as the current one. Moreover, the same credit applicant with the same score may be accepted by one credit provider, but rejected by another. Such decisions depend on the credit policy of the credit providers and other available information. We are not involved in any way in their credit decision process.

"Fulfilling commitment to make payment" means making payment by 90 days from the due date.

List of TransUnion's members wish to contact you

7. Request for Updated Contact Information

The following is a list of TransUnion's members who were unable to contact you and requested to be provided with updated contact information:

7.1 Bank of Credit Union Ltd. - Card Centre made the request on 13-07-2007.

Here you will find the number of enquiries alert deletion previously made by TransUnion's members

8. Enquiry Alert Deletion(s)

These are enquiry alert deletion(s) made by TransUnion's members:

8.1 Bank of Credit Union Ltd. - Card Centre made an enquiry on 15-05-2007 regarding your Master Business Card for the purpose of review of existing credit facilities granted.

On 20-05-2007, the enquiry alert record was deleted by Bank of Credit Union Ltd. for the following reason:

"Enquiry made without notification to consumer"

9. Consumer's Comment

Nil

Any consumer statement that you added to your report appears here

Note:

TransUnion only provides credit reports to credit providers based on information collected and does not approve or reject applications for credit. We simply report the information provided by the credit providers. Other than the credit report, credit providers may also consider their own risk acceptance level in lending, their own internal credit score and the applicant's financial and demographic information in considering applications for credit.

END

Annex D – Data Protection Principles and Part III of the Code

Data Protection Principles

Principle 1 – Purpose and manner of collection of personal data

(1) Personal data shall not be collected unless-

(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;

(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and

(c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are -

(a) lawful; and

(b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that -

(a) he is explicitly or implicitly informed, on or before collecting the data, of-

(i) whether it is obligatory or voluntary for him to supply the data; and

(ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and

(b) he is explicitly informed-

(i) on or before collecting the data, of-

(A) the purpose (in general or specific terms) for which the data are to be used; and

(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which they were collected, of-

(A) his rights to request access to and to request the correction of the data; and

(B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

Principle 2 – Accuracy and duration of retention of personal data

(1) All practicable steps shall be taken to ensure that-

(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;

(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used-

(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data are erased;

(c) where it is practicable in all the circumstances of the case to know that-

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and

(ii) that data were inaccurate at the time of such disclosure, that the third party-

(A) is informed that the data are inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

Principle 3 - Use of personal data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than-

(a) the purpose for which the data were 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).

Principle 4 – Security of personal data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing,

erasure or other 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 are stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any requirement in which the data are 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.

Principle 5 - Information to be generally available

All practicable steps shall be taken to ensure that a person can-

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

Principle 6 – Access to personal data

A data subject shall be entitled to-

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data-

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;

(f) be given reasons if a request referred to in paragraph (e) is refused; and

(g) object to a refusal referred to in paragraph (f).

Part III of the Code

The Handling of Consumer Credit Data by Credit Reference Agencies

Collection of consumer credit data by CRA

Scope of data to be collected

3.1 A CRA may, for the consumer credit reference service which it provides, collect the following items of personal data:

3.1.1 general particulars of an individual as follows: name, sex, address, contact information, date of birth, Hong Kong Identity Card Number or travel document number;

3.1.2 consumer credit data as permitted to be provided by a credit provider to the CRA under clause 2.4, including the identity of the credit provider and the date of the providing of such data;

3.1.3 public record and related data, being data in official records that are publicly available relating to any action for the recovery of a debt or judgements for monies owed entered against the individual, and any declaration or discharge of bankruptcy appearing on official records or as notified to the CRA by the individual pursuant to clause 3.3.2;

3.1.4 watch list data, being a list of credit providers who wish to be notified and provided information to assist in debt collection if an individual in default has reappeared in the system;

3.1.5 file activity data, being record of a credit provider accessing an individual's personal data held by the CRA under the consumer credit reference service provided;

3.1.6 credit score data, being the score that results or resulted from applying consumer credit scoring to an individual;

3.1.7 notification by the Transport Department under clause 3.10.2;

3.1.8 any other type of personal data as described in Schedule 3 subject to the conditions therein mentioned, as may from time to time be amended by the Commissioner.

Retention of consumer credit data by CRA

Retention of account general data

3.2 Where a CRA has collected from a credit provider any account data (comprising of account general data and account repayment data), the CRA may thereafter retain the account general data in its database for so long as there remain in such database any account repayment data relating to the same account.

Retention of account repayment data revealing default period in excess of 60 days

3.3 Where a CRA has collected from a credit provider any account repayment data relating to an individual that reveal a material default, the CRA may thereafter retain the account repayment data in its database until the earlier of:

3.3.1 the expiry of 5 years from the date of final settlement of the amount in default (including settlement of the amounts payable pursuant to a scheme of arrangement with the credit provider); or

3.3.2 the expiry of 5 years from the date of the individual's discharge from bankruptcy, as notified to the CRA by such individual and evidenced by the relevant certificate of discharge issued by the Court of First Instance or by a written notice from the Official Receiver stating that the Official Receiver has no objection to a certificate of discharge being issued to the individual,

irrespective of any write-off by the credit provider of the amount in default in full or in part at any time (if such be the case).

Retention of account repayment data not revealing default period in excess of 60 days

3.4 Where a CRA has collected from a credit provider any account repayment data that do not reveal a material default, the CRA may thereafter, in respect of each individual item of data collected, retain the same in its database for a period of 5 years from the date of creation of such data, provided that if the account is in the meantime terminated, then subject to clause 3.5.2, the CRA may continue to retain the account repayment data in its database until the expiry of 5 years after account termination.

Deletion of data after account termination pursuant to individual's request

3.5 Notwithstanding clause 3.4, if a CRA has collected any account data from a credit provider and within 5 years after the termination of the account the CRA receives from the credit provider a request under clause 2.15 for the deletion of the account data from its database, the CRA shall:

3.5.1 verify from its database as soon as reasonably practicable that there has not been, within 5 years immediately before account termination, any material default (whether or not such default period fell entirely within those 5 years); and

3.5.2 having thus verified from its database, delete as soon as reasonably practicable from its database any account data relating to such terminated account,

provided that if the CRA discovers from its database that there has apparently been a material default within 5 years immediately before account termination, the CRA shall then clarify the matter with the credit provider as soon as

reasonably practicable. The CRA shall, in the meantime, be under no obligation to delete the account data until it shall have clarified the matter with the credit provider.

Retention of other consumer credit data

3.6 Where a CRA has collected any consumer credit data other than account data, it may thereafter retain such data in its database for the following periods:

3.6.1 public record and related data under clause 3.1.3, except data relating to a declaration or discharge of bankruptcy: the period of 7 years from the date of the event shown in the official record;

3.6.2 public record and related data under clause 3.1.3 relating to a declaration or discharge of bankruptcy: the period of 8 years from the relevant declaration of bankruptcy;

3.6.3 credit application data under clause 2.4.2: the period of 5 years from the date of the reporting of the application;

3.6.4 credit card loss data under clause 2.4.4: the period of 5 years from the date of report of the loss of the credit card;

3.6.5 file activity data under clause 3.1.5: the period of 5 years from the date of creation of such data;

3.6.6 credit score data under clause 3.1.6: until the end of the next business day following the date of creation of such data;

3.6.7 general particulars of an individual: for as long as there are other consumer credit data related to the individual contained in the database of the CRA.

Retention of exempted data

3.7 For the avoidance of doubt, notwithstanding any provision to the contrary in the Code, in a situation where exemption from DPP3 under section 62 of the Ordinance applies to certain consumer credit data held by the CRA (including, for example, such data used or to be used by the CRA for the development of a consumer credit scoring model intended to be of general application), the data may continue to be retained by the CRA for so long as such exemption applies.

Use of consumer credit data by CRA

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 or 2.10, 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:

3.8.1 credit application data under clause 2.4.2, credit card loss data under clause 2.4.4 and file activity data under clause 3.1.5: confined to such data created for not more than 2 years; and

3.8.2 account data under clause 2.4.3 and the derivatives deriving directly from such account data :

3.8.2.1 the credit report shall not reveal the identity of the credit provider who provided such account data or the account number, unless the credit report is to be provided to that same credit provider;

3.8.2.2 the credit report shall not contain:

3.8.2.2.1 in relation to an active account, any account repayment data created more than 2 years before the date of providing the credit report; or

3.8.2.2.2 in relation to a terminated account, any account repayment data created more than 2 years before the account termination date;

unless there has been any material default within 5 years before the providing of the credit report, in which case, the credit report may contain, in addition to the account repayment data described in clause 3.8.2.2.1 or 3.8.2.2.2 (as the case may be), also the default data relating to such material default or material defaults;

3.8.2.3 the credit report, if provided at any time during the transitional period, shall not contain any account data other than the account data described in clause 2.10.5, 2.10.6 or 2.10.7, unless the credit report is provided to a credit provider who has confirmed to the CRA, pursuant to clause 2.11.1 above, that the access has been made under any of the circumstances provided for in clause 2.10.1, 2.10.2, 2.10.3 or 2.10.4; and

3.8.2.4 without prejudice to the generality of clauses 3.8.1, 3.8.2.1, 3.8.2.2 and 3.8.2.3 above and for the avoidance of doubt, in the case of the individual being a guarantor to the repayment of a consumer credit provided to another person, the credit report of such individual may contain, in addition to the consumer credit data relating to the individual as borrower, also the account general data and the remaining available credit or outstanding balance of the guaranteed credit facility relating to that other person..

Disclosure of disputed data

3.9 If any consumer credit data provided by a credit provider to a CRA are accompanied by an indication of the existence of a dispute over the data, then, in subsequently disclosing such data in a credit report, the CRA shall also reveal in the credit report the existence of the dispute.

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:

3.10.1 to provide notice and information to a credit provider on a watch list, when new data of the individual in default have 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 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:

3.10.5.1 in relation to an active account, any account data created more than 5 years before the carrying out of the scoring; or

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

<u>Data security and system integrity safeguards by CRA</u>

Measures to take in preparation for providing consumer credit reference service

3.11 On or before providing consumer credit reference service to a credit provider, a CRA shall take appropriate measures, including the following, to safeguard against any improper access to or mishandling of consumer credit data held by it:

3.11.1 enter into a formal written agreement with the credit provider as subscriber for such service, which shall specify:

3.11.1.1 the duty of both parties to comply with the Code in providing and in utilizing the consumer credit reference service;

3.11.1.2 the conditions under which the credit provider may access consumer credit data held by the CRA;

3.11.1.3 the controls and procedures to be applied when such credit provider seeks access to the CRA's database;

3.11.2 establish controls to ensure that only data to which a subscriber is entitled are released;

3.11.3 train staff in relation to the Ordinance and the Code and, in particular, good security practice;

3.11.4 develop written guidelines, and disciplinary or contractual procedures in relation to the proper use of access authorities by staff, external contractors or subscribers;

3.11.5 ensure that adequate protection exists to minimize, as far as possible, the risk of unauthorized entry into the database or interception of communications made to and from the database.

Measures to take in daily operations

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:

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;

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.

Log of access etc. by credit provider

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 were so accessed;

3.13.2.4 the circumstances provided for in clause 2.8, 2.9 or 2.10 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, 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.

<u>Compliance audit of CRA</u>

Compliance audit

3.14 As a recommended practice, a CRA shall consider engaging, 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 of the Ordinance and the Code.

The first compliance audit

3.15 The first of such compliance audits shall be carried out within 6 months from the effective date, with 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. In addition to the matters mentioned in clause 3.14, the first compliance audit shall address, in particular, the adequacy of the data handling system of the CRA in accordance with the provisions of the Code.

Commissioner's approval of report

3.16 If the Commissioner does not approve the first compliance audit report 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 of the Code and/or the Ordinance, thereafter to arrange for a further compliance audit 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.

Regular audits after Commissioner's approval

3.17 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 CRA shall continue to arrange for compliance audits 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.

Data Access and Correction Request to CRA

Compliance with data access request

3.18 As a recommended practice, a CRA shall seek to respond promptly to a data access request in respect of personal data held by it brought by an individual who advises that he has been refused credit by a credit provider to whom a credit report on him has been provided by the CRA. Where such an access request is made at the office of the CRA, the copy of the data held shall, if practicable, be provided forthwith to the individual, or else be dispatched by mail to the individual not later than 3 working days from the date of the request.

Verification with credit provider

3.19 Upon receiving a request for correction of consumer credit data provided by a credit provider, the CRA shall promptly consult the credit provider. If the CRA does not receive from the credit provider any written confirmation or correction of the

disputed data within 40 days from the correction request, the relevant data shall upon expiry of the 40 days be deleted or otherwise amended as requested.

Verification of public record data

3.20 Upon receiving a request for correction of consumer credit data being public record data, the CRA shall wherever practicable verify the accuracy of such data by checking the relevant public records. If no such verification is obtained within 40 days from the date of the correction request, the public record data shall upon expiry of the 40 days be deleted or otherwise amended as requested, except where the individual alleges any inaccuracy in the data which is not apparent on the face of the public records, it shall in that case be incumbent on the individual to provide proof of such inaccuracy.

Annex E – Photographs of sealed plastic bag and security box

Sealed plastic bag containing backup tapes of Consumer Credit Data

Security box for delivering backup tapes of Consumer Credit Data between TransUnion and the Security Company

Annex F – Photographs of interview rooms

Interview rooms in Customer Relations Department

CCTV cameras in an interview room of the Customer Relations Department

Annex G – Copy of credit report to consumer

TransUnion
環聯

TransUnion Limited
Consumer Relations Department
Suite 1006, Tower 6, The Gateway
9 Canton Road, Tsim Sha Tsui
Kowloon, Hong Kong

Credit Report

22-06-2010

Your ref: DAR/PCO1/10

Dear Sir,

Enclosed please find your TransUnion Credit Report. Please take the time to read the report and understand your credit profile. The information contained in your TransUnion Credit Report can help you enjoy more control over your financial health including your ability to obtain credit or detect early warning signs of fraud or identity theft. Managing your credit is important for achieving some of life's most important goals, such as buying a home or car, or financing an education.

TransUnion is an impartial third-party acting as an objective and trusted bridge for your credit providers to provide and share customer information. TransUnion collects, holds and uses personal data in accordance with the Code of Practice on Consumer Credit Data ("the Code") which was issued by the Privacy Commissioner for Personal Data. TransUnion does not take part in the credit decision-making process of any credit provider. Credit providers are also required by the Code to provide updated data on a regular basis.

Should you have any questions regarding your Credit Report, please contact our Consumer Relations Department at 25771816. Full details of "Other Enquiry Information" of the Credit Report are also available upon request. Please contact us within 30 days and have your reference number (as quoted above) ready at the time of calling us. Our hours are Monday to Friday from 9:00 AM to 5:30 PM. We are closed on public holidays.

Yours Sincerely,

Consumer Relations Department
TransUnion Limited

Note: This is a computer-generated printout and contains no signature.
With effect from 01-02-2007, our consumer credit report carries a prominent watermark of TransUnion's trademark on each page.

環聯資訊有限公司 — 個人資料查詢部
[illegible]

Page 1 of 8

1. Personal Information

The following is your personal information provided to us by TransUnion's members:

Name:
Identity No.:
Date of Birth:
Sex:

1.1 Address History:

1.1.1
1.1.2

1.1.3
1.1.4
1.1.5
1.1.6

1.1.7

1.2 Contact Number History:

1.2.1
1.2.2
1.2.3
1.2.4
1.2.5
1.2.6
1.2.7

2. Credit Account(s) Information

The following is your credit information provided to us by TransUnion's members:

2.1 Open Credit Account(s):

2.1.1 Standard Chartered Bank (HK) Ltd. reported that on 13-05-2010, a Card with credit amount of HKD 1,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

2.1.2 Industrial and Commercial Bank of China (Asia) Ltd. reported that on 22-07-2008, a Card with credit amount of HKD 100,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

2.1.3 Standard Chartered Bank (HK) Ltd. reported that on 30-05-2008, a Card with credit amount of HKD 4,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

Standard Chartered Bank (HK) Ltd. made further reports on such account as follows:

On 31-05-2010, the outstanding balance of the account was HKD 3,105.

2.1.4 Standard Chartered Bank (HK) Ltd. reported that on 29-04-2006, a Card with credit amount of HKD 1,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

2.1.5 Bank of East Asia Ltd. reported that on 19-10-2005, a Card with credit amount of HKD 80,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

2.1.6 The Hongkong and Shanghai Banking Corporation Ltd. reported that on 26-09-2005, a Card with credit amount of HKD 177,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

The Hongkong and Shanghai Banking Corporation Ltd. made further reports on such account as follows:

On 31-05-2010, the outstanding balance of the account was HKD 58,953.

2.1.7 Hang Seng Bank Ltd. reported that on 27-07-2004, a Card with credit amount of HKD 108,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

Hang Seng Bank Ltd. made further reports on such account as follows:

In 10-2007, it was past due for 1 day(s).

On 31-05-2010, the outstanding balance of the account was HKD 1,948.

2.1.8 The Hongkong and Shanghai Banking Corporation Ltd. reported that on 02-07-2004, a Card with credit amount of HKD 100,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

The Hongkong and Shanghai Banking Corporation Ltd. made further reports on such account as follows:

In 03-2007, it was past due for 1 day(s).

On 31-05-2010, the outstanding balance of the account was HKD 978.

2.1.9 DBS Bank (Hong Kong) Ltd. reported that on 23-06-2004, a Card with credit amount of HKD 1 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

2.1.10 DBS Bank (Hong Kong) Ltd. reported that on 26-07-2002, a Card with credit amount of HKD 219,999 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

DBS Bank (Hong Kong) Ltd. made further reports on such account as follows:

On 01-06-2010, the outstanding balance of the account was HKD 333.

2.1.11 Standard Chartered Bank (HK) Ltd. reported that on 07-05-2001, a Card with credit amount of HKD 127,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

Standard Chartered Bank (HK) Ltd. made further reports on such account as follows:

On 31-05-2010, the outstanding balance of the account was HKD 3,270.

2.1.12 Bank of China Credit Card (Intl) Ltd. reported that on 19-12-2000, a Card with credit amount of HKD 104,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

Bank of China Credit Card (Intl) Ltd. made further reports on such account as follows:

On 31-05-2010, the outstanding balance of the account was HKD 7,138.

2.1.13 Citibank, N.A. reported that on 01-07-1985, a Card with credit amount of HKD 100,000 was opened for you and that you had a credit relationship with them. You were a Principal of this consumer account.

Citibank, N.A. made further reports on such account as follows:

On 31-05-2010, the outstanding balance of the account was HKD 1,685.

2.2 Closed Credit Account(s):

2.2.1 Industrial and Commercial Bank of China (Asia) Ltd. reported that on 01-04-2008, a Card with credit amount of HKD 100,000 was opened for you. You were a Principal of this consumer account.

Industrial and Commercial Bank of China (Asia) Ltd. made further reports on such account as follows:

On 04-08-2008, this account was closed.

On 15-08-2008, the outstanding balance of the account was HKD -2.

2.2.2 Dah Sing Bank Ltd. reported that on 01-03-2008, a Facility with credit amount of HKD 100,000 was opened for you. You were a Principal of this consumer account.

Dah Sing Bank Ltd. made further reports on such account as follows:

On 09-03-2010, it was advised that this account had been paid in full and closed.

2.2.3 Bank of East Asia Ltd. reported that on 19-07-2007, a Facility with credit amount of HKD 500,000 was opened for you. You were a Principal of this consumer account.

Bank of East Asia Ltd. made further reports on such account as follows:

On 28-05-2010, it was advised that this account had been paid in full and closed.

2.2.4 DBS Bank (Hong Kong) Ltd. reported that on 08-05-2006, a Account with credit amount of HKD 1 was opened for you. You were a Principal of this consumer account.

DBS Bank (Hong Kong) Ltd. made further reports on such account as follows:

On 30-04-2010, it was advised that this account had been paid in full and closed.

2.2.5 Bank of East Asia Ltd. reported that on 19-10-2005, a Card with credit amount of HKD 5,000 was opened for you. You were a Principal of this consumer account.

Bank of East Asia Ltd. made further reports on such account as follows:

On 30-12-2006, it was advised that this account had been paid in full and closed.

2.2.6 American Express International Inc reported that on 01-10-2005, a Card was opened for you. You were a Principal of this consumer account.

American Express International Inc made further reports on such account as follows:

On 30-11-2006, it was advised that this account had been paid in full and closed.

2.2.7 Citibank, N.A. reported that on 14-06-2004, a Card with credit amount of HKD 50,000 was opened for you. You were a Principal of this consumer account.

Citibank, N.A. made further reports on such account as follows:

On 31-07-2006, it was advised that this account had been paid in full and closed.

2.2.8 Standard Chartered Bank (HK) Ltd. reported that on 14-10-2003, a Card with credit amount of HKD 1,000 was opened for you. You were a Principal of this consumer account.

Standard Chartered Bank (HK) Ltd. made further reports on such account as follows:

On 30-11-2009, it was advised that this account had been paid in full and closed.

2.2.9 DBS Bank (Hong Kong) Ltd. reported that on 20-06-2003, a Card with credit amount of HKD 33,000 was opened for you. You were a Principal of this consumer account.

DBS Bank (Hong Kong) Ltd. made further reports on such account as follows:

On 23-08-2005, this account was closed.

2.2.10 Bank of East Asia Ltd. reported that on 18-04-2002, a Card with credit amount of HKD 52,000 was opened for you. You were a Principal of this consumer account.

Bank of East Asia Ltd. made further reports on such account as follows:

On 30-04-2010, it was advised that this account had been paid in full and closed.

2.2.11 Citibank, N.A. reported that on 01-07-1985, a Card with credit amount of HKD 100,000 was opened for you. You were a Principal of this consumer account.

Citibank, N.A. made further reports on such account as follows:

On 28-02-2010, the outstanding balance of the account was HKD 290.

On 28-02-2010, this account was closed.

3. Credit Application(s) Enquiry Information

From our records, these are enquiries made by TransUnion's members arising from your credit application(s).

3.1 Standard Chartered Bank (HK) Ltd. made an enquiry on 18-02-2010 regarding your application for Mortgage for the amount of HKD 1,260,000.

3.2 Standard Chartered Bank (HK) Ltd. made an enquiry on 02-02-2010 regarding your application for Loan for the amount of HKD 300,000.

3.3 Bank of East Asia Ltd. made an enquiry on 04-08-2009 regarding your application for Mortgage for the amount of HKD 1,715,000.

3.4 Fubon Bank (Hong Kong) Limited. made an enquiry on 10-07-2009 regarding your application for Loan for the amount of HKD 300,000.

3.5 Public Bank (Hong Kong) Limited made an enquiry on 06-07-2009 regarding your application for Loan for the amount of HKD 300,000.

3.6 Industrial and Commercial Bank of China (Asia) Ltd. made an enquiry on 09-12-2008 regarding your application for Loan for the amount of HKD 300,000.

3.7 Bank of East Asia Ltd. made an enquiry on 27-11-2008 regarding your application for Loan for the amount of HKD 300,000.

3.8 China Construction Bank (Asia) Corporation Limited made an enquiry on 26-11-2008 regarding your application for Loan for the amount of HKD 300,000.

4. Other Enquiry Information

From our records, these are enquiries made by TransUnion's members other than those arising from your credit application(s). Please note that these enquiries do not impact on your credit score.

4.1 Bank of East Asia Ltd. made an enquiry on 21-03-2010 regarding your Card for the purpose of review of existing credit facilities granted.

4.2 Bank of East Asia Ltd. made enquiries since 24-01-2010 regarding your Facility for the purpose of review of existing credit facilities granted. The latest enquiry was made on 22-04-2010.

4.3 DBS Bank (Hong Kong) Ltd. made enquiries since 24-05-2009 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 25-04-2010.

4.4 Dah Sing Bank Ltd. made an enquiry on 23-04-2009 regarding your Loan for the purpose of review of existing credit facilities granted.

4.5 DBS Bank (Hong Kong) Ltd. made an enquiry on 22-04-2009 regarding your Account for the purpose of review of existing credit facilities granted.

4.6 Dah Sing Bank Ltd. made enquiries since 29-01-2009 regarding your Facility for the purpose of renewal of existing credit facilities granted. The latest enquiry was made on 26-01-2010.

4.7 DBS Bank (Hong Kong) Ltd. made an enquiry on 29-01-2009 regarding your Card for the purpose of review of existing credit facilities granted.

4.8 Bank of China Credit Card (Intl) Ltd. made enquiries since 21-01-2009 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 19-06-2010.

4.9 Dah Sing Bank Ltd. made an enquiry on 25-08-2008 regarding your Facility for the purpose of review of existing credit facilities granted.

4.10 Standard Chartered Bank (HK) Ltd. made enquiries since 15-08-2008 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 12-11-2008.

4.11 Citibank, N.A. made enquiries since 10-07-2008 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 25-05-2010.

4.12 Bank of East Asia Ltd. made enquiries since 19-04-2008 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 20-09-2009.

4.13 Hang Seng Bank Ltd. made enquiries since 15-04-2008 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 15-06-2010.

4.14 Standard Chartered Bank (HK) Ltd. made enquiries since 14-04-2008 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 14-06-2010.

4.15 The Hongkong and Shanghai Banking Corporation Ltd. made enquiries since 10-04-2008 regarding your Card for the purpose of review of existing credit facilities granted. The latest enquiry was made on 10-06-2010.

4.16 Bank of East Asia Ltd. made enquiries since 07-04-2008 regarding your Facility for the purpose of renewal of existing credit facilities granted. The latest enquiry was made on 02-04-2009.

5. Credit Score

Based on your credit data, your credit score as at 22-06-2010 falls into the C category. Statistically, in the period of the next 12 months, **99.51%** of population with such score will fulfill their commitment to make payment to credit providers.

Notes:

Credit score does not draw conclusion or provide credit decisions for credit providers. Credit score is only one piece of information used by credit providers in their credit assessment process. Other than the credit score, credit providers will also consider their own risk acceptance level in lending, their own internal credit score and the applicant's demographic and financial information. A credit score is a fluid number and is calculated based upon the latest information contained in a credit file at the time the score is requested. Since the credit information of a consumer may change from time to time, a score generated previously may not be the same as the current one. Moreover, the same credit applicant with the same score may be accepted by one credit provider, but rejected by another. Such decisions depend on the credit policy of the credit providers and other available information. We are not involved in any way in their credit decision process.

"Fulfilling commitment to make payment" means making payment by 90 days from the due date.

Note:

TransUnion only provides credit reports to credit providers based on information collected and does not approve or reject applications for credit. We simply report the information provided by the credit providers. Other than the credit report, credit providers may also consider their own risk acceptance level in lending, their own internal credit score and the applicant's financial and demographic information in considering applications for credit.

END

Annex H – Copy of credit report to Subscriber

INPUT:

TRANSUNION LIMITED
BASIC CREDIT CHECK
LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

DATE: 22-06-2010
TIME: 15:13

FOR:

CONTROL NO:

NAME:

BIRTH:

GENDER: MALE
ID NUMBER

ID TYPE
IDENTITY CARD

ISSUE COUNTRY
HKG

ADDRESS:

CAPTUREDT: 09-12-2008

CAPTUREDT: 24-07-2004

CAPTUREDT: 23-06-2004

CAPTUREDT: 05-11-2003

CONTACT NUMBER:

CNTRY AREA	CONTACT NUMBER	EXT/CALL	CAPTUREDT	LAST REPTDT	
			03-04-2008	03-04-2008	
852			26-08-2005	06-06-2010	*
			16-06-2005	12-06-2010	*
			05-11-2003	12-06-2010	
852			18-02-2002	18-06-2010	*
852			18-02-2002	18-06-2010	*

NOTE: * - CONTACT NUMBER CONTRIBUTED BY MORE THAN ONE SUBSCRIBER

CREDIT SCORE

TYPE	SCORE	GRADE	PROB	DISPUTED INFO	LIMITED HISTORY
CM02	3528	AA	0.11	N	N

SUMMARY COUNT

SAFE SCAN ALERT	000	ALIAS NAME ALERT	000
WATCH LIST ALERT	000	PAST DUE ACCOUNTS	000
NEW ACCOUNT ALERT	001	OPEN ACCOUNTS	012
CLOSED ACCOUNTS (ACCT HISTORY)	011	PUBLIC RECORDS	000
RELATED PARTIES	000	ENQUIRY ALERT	117

PAGE 1 of 8 INTERNAL USE ONLY

```
                                TRANSUNION LIMITED                DATE: 22-06-2010
                                BASIC CREDIT CHECK                TIME: 15:13
              LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

FOR:                                                        CONTROL NO:

NAME:                                                         BIRTH:

***INDIVIDUAL CREDIT EXPOSURE***

CURRENCY: HKD

*REVOLVING CREDITS*                        *TERMS & OTHER CREDITS*
TOTAL ACCOUNTS:                    13      TOTAL ACCOUNTS:                    0
TOTAL CRLMT:                1,122,000      TOTAL LNAMT:                       0
TOTAL USED CRLMT:              77,410      TOTAL O/BAL:                       0
TOTAL PAST DUE AMOUNT:              0      TOTAL INSAMT:                      0
                                           TOTAL PAST DUE AMOUNT:             0


***NEW ACCOUNT ALERT***

1. MEMBER            ACCOUNT                    REPTDT     AC OPENED  AC CLOSED
2. I/C ASSOC TYPE EXPIRED    CURR INSAMT        CRLMT/LNAMT  TERMS
3. ST PAYAMT        LAST UPDT  PAST DUE AMOUNT  O/BAL        DISPUTE
4. SCHARGMDT  SINSAMT      STERMS FREQ STTLAMT      SEXPIRED   INVESTDT
5. DELSDT     MAXPDAMT     MAXPDDT    MAXD MAXDDT
6. DAYS LATE PAYMENT HISTORY
1. SCB DFT                                        31-05-2010 13-05-2010
2. I   HI    5520              HKD                      1,000
3. A            0 10-06-2010                0             0
6. 000


***OPEN ACCOUNTS***

1. MEMBER            ACCOUNT                    REPTDT     AC OPENED  AC CLOSED
2. I/C ASSOC TYPE EXPIRED    CURR INSAMT        CRLMT/LNAMT  TERMS
3. ST PAYAMT        LAST UPDT  PAST DUE AMOUNT  O/BAL        DISPUTE
4. SCHARGMDT  SINSAMT      STERMS FREQ STTLAMT      SEXPIRED   INVESTDT
5. DELSDT     MAXPDAMT     MAXPDDT    MAXD MAXDDT
6. DAYS LATE PAYMENT HISTORY
1. CITIBANK DFT                                   31-05-2010 01-07-1985
2. I   HI    5510              HKD                    100,000
3. A         1,310 02-06-2010                0         1,685
6. 000 000 000


1. ICBC CCC                                       16-06-2010 22-07-2008
2. I   HI    5510              HKD                    100,000
3. A            0 18-06-2010                0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000


1. SCB TP                                         31-05-2010 30-05-2008
2. I   HI    5530              HKD                      4,000
3. A         3,105 11-06-2010                0         3,105
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000


                        PAGE 2 of 8   INTERNAL USE ONLY
```

```
                              TRANSUNION LIMITED                DATE: 22-06-2010
                              BASIC CREDIT CHECK                TIME: 15:13
          LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

FOR:                                                          CONTROL NO:

NAME:                                                         BIRTH:

***OPEN ACCOUNTS***

1. MEMBER            ACCOUNT                    REPTDT     AC OPENED  AC CLOSED
2. I/C ASSOC TYPE EXPIRED    CURR INSAMT        CRLMT/LNAMT  TERMS
3. ST PAYAMT        LAST UPDT  PAST DUE AMOUNT  O/BAL        DISPUTE
4. SCHARGMDT  SINSAMT      STERMS FREQ STTLAMT      SEXPIRED   INVESTDT
5. DELSDT     MAXPDAMT     MAXPDDT    MAXD MAXDDT
6. DAYS LATE PAYMENT HISTORY
1. BEA CCFD 6                                       31-05-2010 19-10-2005
2. I   HI    5510             HKD                       80,000
3. I             0 07-06-2010                0             0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000

1. SCB TP                                           31-05-2010 29-04-2006
2. I   HI    5500             HKD                        1,000
3. A             0 08-06-2010                0             0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000

1. HSBC COLLECTION                                  31-05-2010 26-09-2005
2. I   HI    5400             HKD                      177,000
3. A           232 03-06-2010                0          58,953
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000

1. HANG SENG BK DFT                                 31-05-2010 27-07-2004
2. I   HI    5520             HKD                      108,000
3. A         5,424 02-06-2010                0           1,948
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000

1. HSBC COLLECTION                                  31-05-2010 02-07-2004
2. I   HI    5510             HKD                      100,000
3. A        18,900 03-06-2010                0             978
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000

1. DBS BANK COLC                                    01-06-2010 23-06-2004
2. I   HI    5520             HKD                            1
3. I           435 06-06-2010                0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000

1. BOC DFT                                          31-05-2010 19-12-2000
2. I   HI    5510             HKD                      104,000
3. A         1,079 12-06-2010                0           7,138
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000
```

```
                              TRANSUNION LIMITED                DATE: 22-06-2010
                              BASIC CREDIT CHECK                TIME: 15:13
          LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

FOR:                                                        CONTROL NO:

NAME:                                                       BIRTH:

***OPEN ACCOUNTS***

1. MEMBER           ACCOUNT                          REPTDT     AC OPENED  AC CLOSED
2. I/C ASSOC TYPE EXPIRED    CURR INSAMT          CRLMT/LNAMT  TERMS
3. ST PAYAMT       LAST UPDT  PAST DUE AMOUNT  O/BAL         DISPUTE
4. SCHARGMDT  SINSAMT      STERMS FREQ STTLAMT      SEXPIRED   INVESTDT
5. DELSDT     MAXPDAMT     MAXPDDT    MAXD MAXDDT
6. DAYS LATE PAYMENT HISTORY
1. DBS BANK COLC                                     01-06-2010 26-07-2002
2. I   HI    5510              HKD                      219,999
3. A           590 05-06-2010              0              333
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000


1. SCB TP                                            31-05-2010 07-05-2001
2. I   HI    5510              HKD                      127,000
3. A         1,470 09-06-2010              0            3,270
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000

***CLOSED ACCOUNTS***

1. MEMBER           ACCOUNT                          REPTDT     AC OPENED  AC CLOSED
2. I/C ASSOC TYPE EXPIRED    CURR INSAMT          CRLMT/LNAMT  TERMS
3. ST PAYAMT       LAST UPDT  PAST DUE AMOUNT  O/BAL         DISPUTE
4. SCHARGMDT  SINSAMT      STERMS FREQ STTLAMT      SEXPIRED   INVESTDT
5. DELSDT     MAXPDAMT     MAXPDDT    MAXD MAXDDT
6. DAYS LATE PAYMENT HISTORY
1. ICBC CCC                                          15-08-2008 01-04-2008 04-08-2008
2. I   HI    5200              HKD                      100,000
3. C             0 19-08-2008              0              -2
6. 000 000 000 000 000


1. DAH SING BK RCD                                   31-03-2010 01-03-2008 09-03-2010
2. I   HI    5700 31-03-2010 HKD                      100,000
3. C             0 01-04-2010              0              0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000


1. BEA CCFD 1                                        01-06-2010 19-07-2007 28-05-2010
2. I   HI    5700 19-07-2010 HKD                      500,000
3. C             0 07-06-2010              0              0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000


1. DBS BANK PBD325                                   01-05-2010 08-05-2006 30-04-2010
2. I   HI    5710              HKD                        1
3. C        15,000 04-05-2010              0              0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000
```

```
                              TRANSUNION LIMITED                DATE: 22-06-2010
                              BASIC CREDIT CHECK                TIME: 15:13
          LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

FOR:                                                        CONTROL NO:

NAME:

***CLOSED ACCOUNTS***

1. MEMBER           ACCOUNT                      REPTDT     AC OPENED  AC CLOSED
2. I/C ASSOC TYPE EXPIRED    CURR INSAMT        CRLMT/LNAMT  TERMS
3. ST PAYAMT       LAST UPDT  PAST DUE AMOUNT  O/BAL        DISPUTE
4. SCHARGMDT  SINSAMT      STERMS FREQ STTLAMT      SEXPIRED   INVESTDT
5. DELSDT     MAXPDAMT     MAXPDDT    MAXD MAXDDT
6. DAYS LATE PAYMENT HISTORY
1. AE CARD DFT                                    30-11-2006 01-10-2005 30-11-2006
2. I   HI    4100            HKD                          0
3. C           162 09-12-2006               0             0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000


1. BEA CCFD 6                                     30-12-2006 19-10-2005 30-12-2006
2. I   HI    5200            HKD                      5,000
3. C             0 08-01-2007                 0             0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000


1. CITIBANK DFT                                   28-02-2010 01-07-1985 28-02-2010
2. I   HI    5510            HKD                    100,000
3. C         5,670 05-03-2010                 0         290
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000


1. CITIBANK DFT                                   28-02-2007 14-06-2004 31-07-2006
2. I   HI    5400            HKD                     50,000
3. C             0 02-03-2007                 0             0
6. 000 XXX XXX XXX XXX XXX XXX 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000


1. SCB TP                                         30-11-2009 14-10-2003 30-11-2009
2. I   HI    5530            HKD                      1,000
3. C             0 12-12-2009                 0             0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000


1. BEA CCFD 6                                     30-04-2010 18-04-2002 30-04-2010
2. I   HI    5100            HKD                     52,000
3. C             0 11-05-2010                 0             0
6. 000 000 000 000 000 000 000 000 000 000 000 000
6. 000 000 000 000 000 000 000 000 000 000 000 000


1. DBS BANK COLC                                  01-05-2007 20-06-2003 23-08-2005
2. I   HI    5400            HKD                     33,000
3. C        25,999 09-05-2007                 0
6. 000 XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX XXX
6. XXX XXX XXX XXX XXX XXX XXX XXX 000 000 000 000

                        PAGE 5 of 8   INTERNAL USE ONLY
```

TRANSUNION LIMITED DATE: 22-06-2010
BASIC CREDIT CHECK TIME: 15:13
LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

FOR: CONTROL NO:

NAME:

ENQUIRY ALERT

MEMBER	DATE	TYPE	PURPOSE	CURR	AMOUNT
BOC FIN-RCC-CR	19-06-2010	5511	REVIEW		
HANG SENG BK PR-RCC-CR	15-06-2010	5521	REVIEW	HKD	
SCB RC-RCC-CR	14-06-2010	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-06-2010	5511	REVIEW	HKD	
CITIBANK RCSOW-RCC-CR	25-05-2010	5511	REVIEW		
HANG SENG BK PR-RCC-CR	15-05-2010	5521	REVIEW	HKD	
SCB RC-RCC-CR	15-05-2010	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-05-2010	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	25-04-2010	5521	REVIEW	HKD	
BEA CCFD 4-RCC-CO	22-04-2010	5701	REVIEW	HKD	
SCB RC-RCC-CR	19-04-2010	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-04-2010	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-04-2010	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	25-03-2010	5521	REVIEW	HKD	
BEA CCFD 8-RCC-CR	21-03-2010	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-03-2010	5521	REVIEW	HKD	
SCB RC-RCC-CR	15-03-2010	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-03-2010	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	24-02-2010	5521	REVIEW	HKD	
SCB CE-MORTGAGE LOAN	18-02-2010	1100	NEW APP	HKD	1,260,000
HANG SENG BK PR-RCC-CR	15-02-2010	5521	REVIEW	HKD	
SCB RC-RCC-CR	12-02-2010	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-02-2010	5511	REVIEW	HKD	
SCB AP-CONSUMER LENDING	02-02-2010	3200	NEW APP	HKD	300,000
DAH SING BK RC-RCC-CO	26-01-2010	5701	RENEWAL	HKD	
BEA CCFD 4-RCC-CO	24-01-2010	5701	REVIEW	HKD	
DBS BANK PRC-RCC-CR	23-01-2010	5521	REVIEW	HKD	
CITIBANK RCSOW-RCC-CR	22-01-2010	5511	REVIEW		
SCB RC-RCC-CR	18-01-2010	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-01-2010	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-01-2010	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	21-12-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	17-12-2009	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-12-2009	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-12-2009	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	19-11-2009	5521	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-11-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	14-11-2009	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-11-2009	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	25-10-2009	5521	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-10-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	13-10-2009	5511	REVIEW	HKD	
CITIBANK PRC-RCC-CR	10-10-2009	5511	REVIEW		
HSBC CCR-RCC-CR	10-10-2009	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	22-09-2009	5521	REVIEW	HKD	
BEA CCFD 8-RCC-CR	20-09-2009	5401	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-09-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	15-09-2009	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-09-2009	5511	REVIEW	HKD	
BOC FIN-RCC-CR	22-08-2009	5511	REVIEW		

TRANSUNION LIMITED
BASIC CREDIT CHECK
LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

DATE: 22-06-2010
TIME: 15:13

FOR:

CONTROL NO:

NAME:

BIRTH:

ENQUIRY ALERT

MEMBER	DATE	TYPE	PURPOSE	CURR	AMOUNT
DBS BANK PRC-RCC-CR	21-08-2009	5521	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-08-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	15-08-2009	5511	REVIEW	HKD	
CITIBANK PRC-RCC-CR	12-08-2009	5511	REVIEW		
HSBC CCR-RCC-CR	10-08-2009	5511	REVIEW	HKD	
BEA COD-BANK A/C SERVICES	04-08-2009	1100	NEW APP	HKD	1,715,000
DBS BANK PRC-RCC-CR	22-07-2009	5521	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-07-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	14-07-2009	5511	REVIEW	HKD	
FUBON CCC-CREDIT/CHARGE CARD	10-07-2009	3100	NEW APP	HKD	300,000
HSBC CCR-RCC-CR	10-07-2009	5511	REVIEW	HKD	
PBHK BBD-BANK A/C SERVICES	06-07-2009	3100	NEW APP	HKD	300,000
DBS BANK PRC-RCC-CR	24-06-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	16-06-2009	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-06-2009	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-06-2009	5511	REVIEW	HKD	
DBS BANK PRC-RCC-CR	24-05-2009	5521	REVIEW	HKD	
BOC CRC-RCC-CR	19-05-2009	5511	REVIEW		
SCB RC-RCC-CR	15-05-2009	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-05-2009	5521	REVIEW	HKD	
CITIBANK PRC-RCC-CR	12-05-2009	5511	REVIEW		
HSBC CCR-RCC-CR	10-05-2009	5511	REVIEW	HKD	
DAH SING BK MKG-RCC-CR	23-04-2009	3201	REVIEW	HKD	
DBS BANK PRC-RCC-CR	22-04-2009	5711	REVIEW	HKD	
SCB RC-RCC-CR	16-04-2009	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-04-2009	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-04-2009	5511	REVIEW	HKD	
BEA CCFD 3-RCC-CO	02-04-2009	5701	RENEWAL	HKD	
BEA CCFD 8-RCC-CR	22-03-2009	5401	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-03-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	14-03-2009	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-03-2009	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-02-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	13-02-2009	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-02-2009	5511	REVIEW	HKD	
DAH SING BK RC-RCC-CO	29-01-2009	5701	RENEWAL	HKD	
DBS BANK PRC-RCC-CR	29-01-2009	5511	REVIEW	HKD	
BOC FIN-RCC-CR	21-01-2009	5511	REVIEW		
HANG SENG BK PR-RCC-CR	15-01-2009	5521	REVIEW	HKD	
SCB RC-RCC-CR	13-01-2009	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-01-2009	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-12-2008	5521	REVIEW	HKD	
SCB RC-RCC-CR	15-12-2008	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-12-2008	5511	REVIEW	HKD	
ICBC RCU2-CONSUMER LENDING	09-12-2008	3200	NEW APP	HKD	300,000
BEA CCFD 1-CONSUMER LENDING	27-11-2008	3200	NEW APP	HKD	300,000
CCBA CORP CBC-CONSUMER LENDING	26-11-2008	3200	NEW APP	HKD	300,000
HANG SENG BK PR-RCC-CR	15-11-2008	5521	REVIEW	HKD	
SCB RC-RCC-CR	12-11-2008	5501	REVIEW	HKD	
HSBC CCR-RCC-CR	10-11-2008	5511	REVIEW	HKD	

TRANSUNION LIMITED
BASIC CREDIT CHECK
LOAN RESTRUCTURING (CURRENT MATERIAL DEFAULT) - 1101

DATE: 22-06-2010
TIME: 15:13

FOR:

CONTROL NO:

NAME:

BIRTH:

ENQUIRY ALERT

MEMBER	DATE	TYPE	PURPOSE	CURR	AMOUNT
SCB RC-RCC-CR	20-10-2008	5511	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-10-2008	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-10-2008	5511	REVIEW	HKD	
SCB RC-RCC-CR	23-09-2008	5511	REVIEW	HKD	
BEA CCFD 8-RCC-CR	19-09-2008	5401	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-09-2008	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-09-2008	5511	REVIEW	HKD	
DAH SING BK MKG-RCC-CR	25-08-2008	5701	REVIEW	HKD	
BEA CCFD 8-RCC-CR	22-08-2008	5401	REVIEW	HKD	
SCB RC-RCC-CR	15-08-2008	5501	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-08-2008	5521	REVIEW	HKD	
HSBC CCR-RCC-CR	10-08-2008	5511	REVIEW	HKD	
BEA CCFD 8-RCC-CR	20-07-2008	5401	REVIEW	HKD	
HANG SENG BK PR-RCC-CR	15-07-2008	5521	REVIEW	HKD	
SCB RC-RCC-CR	12-07-2008	5511	REVIEW	HKD	
HSBC CCR-RCC-CR	10-07-2008	5511	REVIEW	HKD	
CITIBANK PRC-RCC-CR	10-07-2008	5511	REVIEW		

CAUTION ON SCORE USAGE

When a score is provided along with this report, the score should not be considered as a final or comprehensive conclusion of the report. The score should be read and considered together with the credit information provided in the report and any other information held by you or on your behalf. The Subscriber should use the score with caution when there is limited performance history. The Subscriber recognizes the fact that factors other than the score (such as the credit report, the individual account history, application information and economic factors) have to be considered in making a decision as to consumer credit. Score value may change as elements in the credit report change. Disputed account has not been taken into consideration in the score calculation.

*** Please direct consumer's request/complaint regarding access to or correction of personal data to the Consumer Relations Manager of TransUnion Limited at 2577 1816.

END OF REPORT: