Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Trans Union Consumer Interactive, Inc. (the Organization)
Decision number (file number)	P2021-ND-083 (File #012358)
Date notice received by OIPC	March 1, 2019
Date Organization last provided information	August 15, 2019
Date of decision	March 16, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a U.S.-based wholly owned subsidiary of Trans Union, LLC, and operates online consumer-facing and credit monitoring subscription services. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported: *The personal information involved in this incident includes information contained in the individual's credit report, including names, mailing addresses, dates of birth, phone numbers, masked financial institution account numbers, available credit and payment details. In addition, email addresses may have been accessed as part of the TUCI account information.* This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization maintains that "it is not subject to the jurisdiction of the Office of the Privacy Commissioner of Alberta in relation to this incident", but did not explain why it believes this to be the case. In my view, the Organization is an "organization" as defined in PIPA, and the information at issue is "personal information" as

	defined in PIPA. To the extent the personal information was collected in Alberta by the Organization, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• In January 2019, the Organization determined that its Canadian consumer-facing website, https://mcmbcrs.transunion.ca had been the target of a "credential stuffing" attack. • The Organization investigated and, in February 2019, found that failed login attempts could be traced back to credential stuffing by an unknown and unauthorized third party. The Organization reported the attacker appears to have directed a cache of valid and invalid credentials at its systems for the purposes of identifying which credentials worked and which did not. Some of the credentials ended-up being valid (i.e. they were the same credentials that the user had also used on a third party's system) and these credentials were then used to access user accounts illegally and without authorization. • The Organization reported the attacks appear to have started no earlier than February 2018, and from the investigation it appears that access was generally obtained on a one-off basis.
Affected individuals	The Organization reported approximately 185 individuals in Alberta were affected.
Steps taken to reduce risk of harm to individuals	• Investigated the incident, including analysis of all failed login attempts back to January 2018. • Reviewed server logs to assist in identifying visits by automated scripts. • Enhanced safeguards to help combat any further credential stuffing attempts. • Implementing two-factor authentication. • Locked user accounts of affected individuals. • Providing affected individuals with one year of free credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by email beginning February 28, 2019.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be	The Organization did not specifically identify the potential harm(s) that might result from this incident, but reported its notification to affected individuals offered "identity theft insurance". In my view, a reasonable person would consider the contact, identity and financial information at issue could be used to cause

important, meaningful, and with non-trivial consequences or effects.	the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization did not provide its assessment of the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the risk of harm is increased as the incident was the result of deliberate credential stuffing attack. The Organization reported some of the credentials were valid and used to access user accounts illegally and without authorization. The attacks appear to have been ongoing for approximately a year before the Organization discovered the threat.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The risk of harm is increased as the incident was the result of a deliberate credential stuffing attack. The Organization reported some of the credentials were valid and used to access user accounts illegally and without authorization. The attacks appear to have been ongoing for approximately a year before the Organization discovered the threat.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand affected individuals were notified by email beginning February 28, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner