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	Equifax (Organization)
Decision number (file number)	P2019-ND-128 (File #006786)
Date notice received by OIPC	October 12, 2017
Date Organization last provided information	March 1, 2018
Date of decision	August 8, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved various combinations of the following information: • name, • address, • credit score, • telephone number, • date of birth, • email address, • log-in credentials (user name, password, secret questions and answers. Believed to be several years old and for use of direct-to-consumer internet website), • social insurance number, • credit score, and • credit card numbers (but not expiry date or CVV). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 29, 2017, the Organization's security team observed suspicious network traffic relating to its Online Dispute web application. • The security team immediately blocked a range of IP addresses believed to be associated with the suspicious traffic and investigated. • On July 30, 2017, the Organization identified additional suspicious traffic and took the web application offline. • The incident occurred between May 13, 2017 and July 30, 2017.
Affected individuals	The incident affected 209,000 card holders, including 11,670 Canadians. Of these, 1,434 affected individuals are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the identified access vectors. • Patched the vulnerability. • Changed passwords for the affected database service accounts. • Enhancing controls for restricting and governing access to sensitive data in the environment. • Employing measures to increase security and further enhance ability to detect and respond to malicious activity. • Offered free credit monitoring to all persons affected. • Notified all credit card issuers and credit card numbers have been replaced and rendered usable. • Reported breach to law enforcement and data protection regulators. • Posted information about breach on website.
Steps taken to notify individuals of the incident	The Organization reported that "All [affected individuals] received individual letters … on October 23".
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 important, meaningful, and with non-trivial consequences or effects.	The Organization initially reported "… the information can be used for identity theft or fraud". In a later submission, the Organization said the type of harm(s) that may result was "None: all credit card issuers have been notified and credit card numbers have been replaced…For good measure, [the Organization] has offered free 12 months credit monitoring".

	In my view, a reasonable person would consider that the contact, identity and financial information at issue, particularly in combination with other information elements such as credit score, 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. Credentials could be used to compromise other online accounts. These are all 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 initially reported that "Considering the data is dated 2014 but that some data elements are sensitive (such as SIN) and were the object of a criminal attack, we assess the risk as high". Further… *…the attacker could not be identified but was clearly pursuing criminal intent. The information was never lost and therfoire [sic] did not have to be recovered. The vulnerability ewas immdediately [sic] addressed, however, in takingthe [sic] Disute websye [sic] offline and no hacking acvtivuity weas [sic] seen since then.* The Organization later reported that it was "highly unlikely" harm could result and also "The harm is not significant because the credit card issuers have been notified, all individuals affected have been notified and, most importantly, all credit cards have been rendered unusable". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party. Further, the information may have been exposed for over two months. While notifying credit card issuers and affected individuals may help to reduce the risk of credit card fraud, this will not entirely mitigate against the risks of identity theft, compromised online accounts and phishing.

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 that the contact, identity and financial information at issue, particularly in combination with other information elements such as credit score, 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 harm. Credentials could be used to compromise other online accounts. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an

unknown third party. Further, the information may have been exposed for over two months. While notifying credit card issuers and affected individuals may help to reduce the risk of credit card fraud, this will not entirely mitigate against the risks of identity theft, compromised online accounts and phishing.

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 the Organization notified affected individuals by letter on October 23, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner