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	IHS Markit (Organization)
Decision number (file number)	P2017-ND-68 (File #005636)
Date notice received by OIPC	May 23, 2017
Date Organization last provided information	May 23, 2017
Date of decision	May 31, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
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 following information was involved in this incident: • username, and • password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information is associated with online customer accounts.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 23, 2017, the Organization became aware that a hacker had gained access to its systems and downloaded a malicious executable file to a number of servers and workstations. • The Organization reported the unauthorized access occurred on January 11, 2017.
Affected individuals	The Organization reported the incident affected 105 individuals.

Steps taken to reduce risk of harm to individuals	• Retained data security experts to conduct forensic investigation. • Servers removed from service, completely rebuilt and relaunched with enhanced security measures. • Potentially affected passwords were invalidated and reset. • Password requirements have been enhanced.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident in writing or by email on May 15, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 reported that the harm that could result from this incident was "Potentially identity theft or fraud." In my view, the credentials at issue in this matter (usernames and passwords) could be used to compromise other online accounts where individuals may have used the same credentials, potentially causing further harms of 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 reported that "… at this time, we are not aware of any instances of fraud, identity theft, or other harm to any individual as a result of this incident." Further, "The harm to consumers is not significant because all passwords have been reset and the affected accounts may no longer be accessed using the affected passwords." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was exposed for almost 2 weeks before the incident was discovered. Although passwords were reset and could no longer be used to access accounts with the Organization, many individuals use the same credentials across various online accounts and those accounts remain vulnerable.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The credentials at issue in this matter (usernames and passwords) could be used to compromise other online accounts where individuals may have used the same credentials, potentially causing further harms of identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware) and the information was exposed for almost 2 weeks before the incident was discovered. Although passwords were reset and could no longer be used to access accounts with the Organization, many individuals use the same credentials across various online accounts and those accounts remain vulnerable.	

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

I understand the Organization notified affected individuals of the incident in writing or by email on May 15, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner