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	Morningstar Inc. (Organization)
Decision number (file number)	P2013-ND-35 (File #P2348)
Date notice received by OIPC	May 29, 2013
Date Organization last provided information	September 30, 2013
Date of decision	January 23, 2014
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 incorporated in Illinois, USA. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and collected personal information from Alberta residents.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information of 2,300 customers, including three Alberta residents: • first and last name, • mailing address, • email address, • password, and • unencrypted credit card number. The following information for 182,000 customers, including 15 Alberta residents, is at issue: • first and last name, • mailing address,

	• email address, and • unencrypted password. This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 21, 2013, a customer contacted the Organization to report that an abnormal file was found on the Morningstar Document Research (MDR) system. • The Organization investigated and concluded that someone hacked into the MDR and gained access to personal information about the Organization's MDR customers. It was determined that the intrusion occurred on or around April 3, 2012. When the incident occurred, credit cards and passwords were stored in MDR as plain text and were not encrypted.
Affected individuals	• The total number of customers whose names, addresses, email addresses, passwords and credit card numbers were compromised as a result of the intrusion was approximately 2,300. Three of these customers were Alberta residents. • The total number of customers whose names, addresses, email addresses and passwords were compromised as a result of this intrusion was approximately 182,000. Of these customers, 15 were Alberta residents.
Steps taken to reduce risk of harm to individuals	• The Organization reported this incident to the police. Since the intrusion and prior to its discovery of the malicious attack, the Organization shut down the old servers which hosted the MDR product at the time of the attack and moved the data to a more secure infrastructure. • All passwords were automatically reset. • The Organization notified its payment processor of the incident.
Steps taken to notify individuals of the incident	• Letter notification was sent on June 17, 2013 to the three affected individuals whose personal information included credit card numbers. • Email notification was sent on June 18, 2013 to the 15 affected individuals whose personal information included name, address, email address and password but no credit card information.

	• The Organization provided affected individuals with a telephone number to call regarding questions or concerns about the incident. • The Organization posted questions and answers about the incident on its website.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 recognized that name, address, email address, unencrypted password and unencrypted credit card number could be used to cause the harms of identity theft and fraud. In its report to my Office, the organization did not identify a risk of phishing; however, it did note this in the notification letter it sent to these affected individuals. In my view, the personal information above is highly sensitive. I agree that the type of harm that could result from unauthorized access to this personal information is identity theft or fraud. Since a significant number of email addresses were involved (2,300 emails in this group and 182,000 emails in the second group), the affected individuals may also be at risk for phishing. In my view, these are significant harms. The Organization also recognized that name, address, email address, and unencrypted password could be used to cause harm in the form of phishing In my view, this personal information is of low to moderate sensitivity. However, it could be used to cause harm in the form of identity theft and fraud. In addition, as noted above, given the significant number of email addresses involved, these affected individuals may also be at risk for phishing. In my view, 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 due to the high sensitivity of the personal information involved, it considered there to be a real risk of significant harm to the individuals whose personal information included name, address, email address, passwords, and credit card information. The Organization submitted it did not believe there was a real risk of phishing or identity theft to those individuals whose personal information involved name, address, email address, and unencrypted password but no credit card numbers. It submitted it did not believe it had an obligation to notify these individuals under PIPA given the small number of individuals involved and the lack of a sensitive data element (such as a

	credit card number). It stated that any possibility of phishing or identity theft with these limited data elements was speculative. However, out of an abundance of caution, it notified these individuals. In my view, there is a real risk of significant harm resulting from this incident to all of the affected individuals. This incident involved a deliberate hack, perpetrated by unauthorized individuals with nefarious intent. Given the combination of personal information and high number of email addresses involved in this incident, all of the affected individuals are at risk for identity theft, fraud and phishing. The risk is increased because the credit card numbers and passwords were stored in plain text at the time of the incident.

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. The personal information involves sensitive information, such as name, address, email address, password, and in some cases credit card information. The information was hacked and the credit cards numbers and passwords were stored in plain text. In previous breach notification decisions (P2012-ND-31, P2013-ND-11, P2013-ND-14, P2013-ND-15 and P2013-ND-18) involving similar circumstances and personal information, I found there was a real risk of significant harm resulting from the incident. These factors contributed significantly to my decision.

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

I understand the Organization notified the three affected Alberta residents in a letter dated June 17, 2013, and the 15 affected Alberta residents in an email dated June 18, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner