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	Institute of Management Accountants (Organization)
Decision number (file number)	P2016-ND-51 (File #003533)
Date notice received by OIPC	August 16, 2016
Date Organization last provided information	August 16, 2016
Date of decision	August 24, 2015
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 a worldwide association of accountants and financial professionals working in business. Although headquartered in Montvale, New Jersey, the Organization provides services to members and customers throughout the United States and Canada. The Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • mailing address, • email address, • telephone number, • credit card number, security code and expiry date. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.

DESCRIPTION OF INCIDENT	
☒ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 20, 2016, the Organization was informed that one of its vendors had been the victim of a potential computer intrusion. • An unauthorized user gained administrative access to the vendor's systems on April 23-24, 2016, and issued commands to delete all the data housed on the vendor's servers. That data may have included the information at issue, which had been collected by the vendor on the Organization's behalf. • There is no evidence indicating that credit card data was accessed or acquired by an unauthorized user or that the unauthorized user intended to steal data. However, the vendor is not able to definitively rule out any unauthorized access to or acquisition of data because data potentially relevant to its forensic investigation was deleted by the unauthorized user.
Affected individuals	A total of 308 individuals were potentially affected, including 2 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The vendor launched an investigation to determine whether a security incident had occurred. • The matter was referred to appropriate law enforcement. • Consumer credit card information is no longer contained in or accessible via the vendor's systems. • The Organization terminated its relationship with the vendor. • Offered one (1) year of complimentary credit monitoring.
Steps taken to notify individuals of the incident	• The Organization reported it "will be providing notice to the two (2) potentially affected Alberta residents." • Established a call center so that customers can ask questions and to receive further information regarding the incident.
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,	The Organization did not specifically assess the type of harm that might result from this incident, although it did report that it "does not believe that "there exists a real risk of significant harm to" these individuals or that notification is required under Section 34.1 of the Personal Information Protection Act…". In my view, the financial information involved in this incident

meaningful, and with non-trivial consequences or effects.	could be used to cause the harms of identity theft, fraud and financial loss. In addition, email addresses could be used for phishing purposes. 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 specifically assess the likelihood of harm resulting from this incident but, as noted above, reported that it "does not believe that "there exists a real risk of significant harm to" these individuals or that notification is required under Section 34.1 of the Personal Information Protection Act…". The Organization also reported that while there is no evidence indicating that credit card data was accessed or acquired by an unauthorized user or that the unauthorized user intended to steal data, its vendor is not able to "definitively rule out any unauthorized access to or acquisition of data because data potentially relevant to its forensic investigation was deleted by the unauthorized user." In my view, there is a real risk of harm resulting from this incident. While the Organization reported there is no evidence the unauthorized user intended to steal data, this cannot be known for sure. The incident was the result of malicious intent (deliberate unauthorized access) and the Organization cannot confirm that information was not acquired because it was deleted by the unauthorized user.

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 information involved in this incident could be used to cause the significant harms of identity theft, fraud, financial loss and phishing. While the Organization reported there is no evidence the unauthorized user intended to steal data, this cannot be known for sure. The incident was the result of malicious intent (deliberate unauthorized access) and the Organization cannot confirm that information was not acquired because it was deleted by the unauthorized user.

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) and provide me with written confirmation that it has done so on or before September 9, 2016. I understand the Organization "will be providing notice to the two (2) potentially affected Alberta residents."

Jill Clayton
Information and Privacy Commissioner