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	Speciality Equipment Market Association (Organization)
Decision number (file number)	P2017-ND-78 (File #003534)
Date notice received by OIPC	August 16, 2016
Date Organization last provided information	October 7, 2016
Date of decision	June 14, 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 a trade association headquartered in Diamond Bar, California and providing services to members and customers throughout the United States and Canada. It qualifies as an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • organization ID, • organization type, • organization name, • organization address, • telephone number, • website address, • personal name, • membership information (including join and return join date, effective date, expiration date, dues package information), • credit card number, expiry date and security code (CVV). Some of this this information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent personal information of Alberta residents was collected in Alberta, I have jurisdiction in this matter.

DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 27, 2016 the Organization learned that one of its vendors had been the victim of a potential computer intrusion. • An unauthorised 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 unauthorised user or that the unauthorised user intended to steal data. However the vendor is not able to definitively rule out any unauthorised access to or acquisition of data because data potentially relevant to its forensic investigation was deleted by the unauthorised user.
Affected individuals	The incident affected 490 individuals in the U.S.A. and 12 Canadians, including three (3) Albertans.
Steps taken to reduce risk of harm to individuals	• Launched an investigation to determine whether a security incident had occurred. • Reported the matter to law enforcement. • Terminated relationship with the vendor. • Offered affected individuals independent credit monitoring services for 12 months. • Established a call centre for customers with questions regarding the incident to contact.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident by letter on July 14, 2016.
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 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 and profile (membership) information involved in this incident could be used to cause the harms of identity theft, fraud and financial loss. 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 financial and profile (membership) information involved in this incident could be used to cause the significant harms of identity theft, fraud and financial loss. 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).

I understand the Organization notified affected individuals by letter on July 14, 2016. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner