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	Accuform Manufacturing Inc. and Safety Marketing Services LLC (Organization)
Decision number (file number)	P2017-ND-01 (File #001699)
Date notice received by OIPC	October 21, 2015
Date Organization last provided information	December 13, 2016
Date of decision	January 3, 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 incorporated in the United States and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • 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. The information was collected in Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 21, 2015, the Organization learned that its computer network had been accessed by an unauthorized third party.

	• The Organization believes the unauthorized access may have started as early as June 30, 2015 and that "one or more parties operating through foreign countries illegally accessed [the Organization's] computer network and exfiltrated copies of orders…". • The unauthorized individual[s] have not been identified or arrested. There have been no reports of fraud, identity theft or misuse of credit card information. • The Organization reported that the information at issue is primarily for corporate credit cards, but could also involve credit cards belonging to individuals.
Affected individuals	A total of 8,668 individuals were affected by this incident, including 342 Canadians. Of these, 47 individuals are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to US federal law enforcement authorities including the Electronic Crimes Task Force of the United States Secret Service. • Retained the services of a cyber security and forensic investigative firm to fully investigate the incident. • Took steps to further secure data by implementing additional security measures. • Increased staffing to improve rigor in testing. • Implemented server and software upgrades.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter beginning October 19, 2015.
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 reported that "If the credit card or other personal information is used as a result of this illegal cyberattack, it is quite possible that individuals … could suffer from fraud, identity theft, financial loss and negative effects on a credit record." I agree with the Organization's assessment. The personal information involved includes identity and financial information that could be used to cause the harms of identity theft, fraud, financial loss and negative effects on a credit record. In addition, email addresses could be used to cause the harm of phishing. 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.	As noted above, the Organization reported "it is quite possible that individuals … could suffer from fraud, identity theft, financial loss and negative effects on a credit record." In my view, the likelihood of harm resulting from this incident is increased because the attack was malicious (deliberate intrusion) and the information may have been exposed for 3 months before the Organization became aware of the breach.

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 involved includes identity and financial information that could be used to cause the harms of identity theft, fraud, financial loss and negative effects on a credit record. The likelihood of harm is increased because the attack was malicious (deliberate intrusion) and the information may have been exposed for 3 months before the Organization learned of the breach. 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 affected individuals on October 19, 2015. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner