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	Emco Corporation (Organization)
Decision number (file number)	P2019-ND-191 (File #013222)
Date notice received by OIPC	May 9, 2019
Date Organization last provided information	May 9, 2019
Date of decision	December 13, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected in Alberta 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 Organization reported the following information may be at issue: • home address, • date of birth, • social insurance number, • credit and/or banking information written on Credit Application Forms, Credit Card Authorization Forms or personal cheques (the Organization reports it has "no proof that any of the emails containing this information were viewed by the unauthorized individuals"). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On February 27, 2019, the email account of an employee was accessed by an unauthorized individual. The employee's password was changed (by the employee) on February 28, 2019 and the account was not re-accessed by any unauthorized individual thereafter. The Organization has no knowledge of any of the employee's emails having been accessed and it is not clear whether the unauthorized individual did anything in the account. • On March 19, 2019, the email account of another employee was accessed by an unauthorized individual. It appears that the unauthorized individual had access to the account for fewer than 10 minutes before the issue was detected and an alert sent to the IT department, who disabled the account. The Organization has no knowledge of any of the emails having been accessed and it is not clear whether the unauthorized individual did anything in the account. • The first incident was discovered on March 29, 2019 by the Organization's IT department while investigating the second incident.
Affected individuals	The incident affected 47 individuals.
Steps taken to reduce risk of harm to individuals	• Offered affected individual no charge credit monitoring for a period of one year. • Consulted with an experienced IT security firm and external privacy counsel and have developed a comprehensive plan to improve organizational protocols.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter May 1, 2019.
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 "It is possible that if sufficient personally identifiable information were to be contained on an accessed record (we have no ability to detect which, if any, records were accessed during the intrusions) that an affected individual could be a victim of identity theft." I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud.

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 "Because we have no positive evidence that any records containing personal information were accessed, and due to the restricted timeframes during which the unauthorized individuals had access to our employees' accounts, our best assessment at this time with the facts we have is that there is a low likelihood that harm will result." In my view, a reasonable person would consider the likelihood of harm resulting from these incidents is increased as they resulted from malicious intent (deliberate action, unauthorized access to email accounts) and because the Organization cannot confirm whether emails were accessed.

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.

A reasonable person would consider that the contact, identity and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud.

The likelihood of harm resulting from these incidents is increased as they resulted from malicious intent (deliberate action, unauthorized access to email accounts) and because the Organization cannot confirm whether emails were accessed.

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

I understand affected individuals were notified by letter May 1, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner