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	Cervus Equipment Corporation (Organization)
Decision number (file number)	P2019-ND-190 (File #013311)
Date notice received by OIPC	May 23, 2019
Date Organization last provided information	May 23, 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 information at issue varies by individual but may have included: • full name, • address, • email address, • telephone number, • salary information, • performance metrics, • job title, • employment status and dates of employment, • information related to contractual guarantees, • information related to employee incentive plan shares, • information related to employee share purchase plan, including account number(s) related to the administration of the plan. 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 8, 2019, the Organization was alerted to a potential unauthorized breach of an employee's email account. An unidentified third party enabled an email forwarding rule, which enabled incoming mail to be surreptitiously forwarded to the unauthorized party's email account between the period of November 12, 2018 - February 8, 2019. • A portion of the emails that are believed to have been forwarded contained personal information belonging to a number of current and former employees and directors and officers with the Organization. • The identity of the unauthorized third party who installed the email forwarding rule is not known.
Affected individuals	The incident affected 717 individuals, including 341 in Alberta.
Steps taken to reduce risk of harm to individuals	• Terminated and disabled the forwarding rule and changed the employee's password. • Undertook a comprehensive review of all inbound emails received by the affected account to determine which contained personal information and which individuals needed to be notified.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and mail between April 30 and May 10, 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 "Depending on the nature of the personal information contained in the email, affected indivduals [sic] may face potential harms including financial fraud where account information was disclosed, identity theft, and phishing and other social engineering attacks." I agree with the Organization's assessment. A reasonable person would consider that the contact and employment information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. 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 it has "…determined there is a real risk of significant harm to the affected individuals due to the sensitive nature of the personal information affected and because of the breach was perpetrated by an unauthorized party with unknown and potentially malicious intentions." I agree with the Organization. A reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, email forwarding rule) and allowed an unauthorized party to gain access to email account information. The account was compromised for almost three months.

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 and employment information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, email forwarding rule) and allowed an unauthorized party to gain access to email account information. The account was compromised for almost three months.

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 email and mail between April 30 and May 10, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner