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	Aerium Analytics Inc. & Aerium SPV Inc. (Organization)
Decision number (file number)	P2021-ND-323 (File #020726)
Date notice received by OIPC	April 23, 2021
Date Organization last provided information	April 23, 2021
Date of decision	March 9, 2022
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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved some or all of the following information: • name, • employment contract, • social insurance number, • date of birth, • family information from benefits form, • blank cheques, and • other personal information disclosed to accounting. 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	• Between April 13 - 21, 2021, one of the Organization's email accounts was regularly accessed by an unauthorized party, using the correct password. The Organization reported it does not know how the credentials were obtained. • The account was used to send an unauthorized email on April 13, 2021 requesting payment of an invoice; the breach was discovered when the email recipient contacted the Organization to verify the request. • The Organization reported that the "unauthorized user had used a mail rule on the account to redirect mail with the relevant subject to the 'RSS Feeds' folder (which commonly exists and is unused, a good place to hide files) and mark them as read."
Affected individuals	The incident affected 22 individuals.
Steps taken to reduce risk of harm to individuals	• Enabled two factor authentication. • Asked employees to change passwords. • Will consider migrating users to a password manager and whenever possible substituting biometric access. • Planning to provide credit protection service to affected employees for a reasonable period of time.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on April 23, 2021.
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, "Identity theft is the only identified possible harm." In my view, a reasonable person would consider that the contact, identity, financial and employment information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, 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, "Identity theft attempts are absolutely possible and reasonably likely." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion into an employee's email account, attempted fraud). The information appears to have been exposed for approximately 7 days.

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, financial and employment information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion into an employee's email account, attempted fraud). The information appears to have been exposed for approximately 7 days. 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 the Organization notified the affected individuals by email on April 23, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner