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	RS Energy Group Canada, Inc. and RS Energy Group, Inc. (Organization)
Decision number (file number)	P2017-ND-166 (File #007320)
Date notice received by OIPC	December 11, 2017
Date Organization last provided information	December 11, 2017
Date of decision	December 15, 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 the affected 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 Alberta 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, • home address, • email address, • signature (for 5 of the 57 affected individuals), and • identification as a stockholder. 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	• On October 30, 2017, an individual located in Africa gained unauthorized access to the email account of the Organization's Co-CEO.

	• Forensic analysis of the email account showed that the individual accessed the email account three separate times on the morning of October 30, 2017. • The purpose of the unauthorized access was to plant an email chain which included fake correspondence and a request for a wire transfer of funds to a bank in Hong Kong. The email chain was then forwarded from the email account to the Organization's CFO. • The recipient immediately recognized the email as suspicious and notified IT staff who determined the email originated from an IP address in Africa. • The password for the compromised account was immediately changed, thwarting another attempted unauthorized sign-in. • The email account was quarantined on November 1, 2017, and forensic analysis confirmed that the email in the account was never independently saved or downloaded, but that emails viewed included the personal information at issue.
Affected individuals	A total of 57 individuals (employees and stockholders) were affected.
Steps taken to reduce risk of harm to individuals	• Immediately on discovery, changed the password on the email account. • Contacted Equifax to provide credit monitoring services to affected individuals. • Increased computer security systems, including implementing new password policy and encrypted password management, and enabling multifactor authentication. • Implemented additional Advanced Threat Protection ("ATP") for all employee mailboxes. • Retained third-party forensic analysis services and monitoring for additional malware or related activity.
Steps taken to notify individuals of the incident	All current employees of the Organization were notified generally of the incident via email on November 3, 2017. The Organization is now contacting each of the affected employees to provide more specific information and is locating other individuals (non-employees) to notify them by telephone of email.

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 given "The type of harm that could potentially result from the breach would be identity theft…None of the emails viewed contained personal information which could cause humiliation or damage to reputation, loss of employment or business or professional opportunities. Any harm would be limited to the potential of identify [sic] theft for the 57 individuals, and any financial loss associated with such identify theft." The organization also noted that "…five of the 57 individuals had their name, home address, email address and a copy of their signature affected by the breach…these individuals are acknowledged to be subject to a higher liklihood [sic] that harm could result from the breach." I accept the Organization's assessment that the information at issue could be used to cause the harm of identity theft and associated financial loss. In addition, email addresses, particularly in combination with profile information (e.g. identification as a stockholder) could be used for phishing purposes. 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 their "The information in the emails was not exposed for very long, and forensic analysis confirmed the emails and their attachments (which included the personal information) were not downloaded during the breach. It is therefore unlikely the individual has copies of the emails or attachments. However, there is evidence of malicious intent or purpose, as the breach was the result of a hack with the intent of financial gain… 47 of [the affected individuals] work for [the Organization] and have already been notified and offered protection by Equifax. This protection lowers the liklihood [sic] that any harm could result as a consequence of the breach." In my view, there is a real risk of significant harm in this case due to the general sophistication of the attack, and evidence of malicious intent (deliberate intrusion with the intention of financial gain), despite the relatively short exposure and the forensic conclusion that the information was viewed, but not downloaded.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the overall circumstances as reported by the Organization, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident.	

The information at issue could be used to cause the harm of identity theft and associated financial loss. In addition, email addresses, particularly in combination with profile information (e.g. identification as a stockholder) could be used for phishing purposes. These are significant harms. The likelihood of harm is increased due to the general sophistication of the attack, and evidence of malicious intent (deliberate intrusion with the intention of financial gain), despite the relatively short exposure and the forensic conclusion that the information was viewed but not downloaded.

I require the Organization to notify affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* and confirm to my office, within 10 days of the date of this decision, that it has done so. I understand current employees of the Organization were notified generally of the incident via email on November 3, 2017 and the Organization is now contacting affected employees to provide more specific information and is locating other individuals (non-employees) to notify them by telephone of email.

Jill Clayton
Information and Privacy Commissioner