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	Lithion Power Group Ltd. (Organization)
Decision number (file number)	P2021-ND-116 (File #014649)
Date notice received by OIPC	January 17, 2020
Date Organization last provided information	April 24, 2020
Date of decision	April 20, 2021
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 Calgary, Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • contact information (address, email address, telephone number), and • resume and academic transcripts. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The three (3) affected individuals reside in the United States; however, the personal information was collected by the Organization in Alberta, via email. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On June 25, 2019, an employee with the Organization was corresponding with a client who advised that they had made wire transfer payments to the Organization. • The Organization did not receive any payments. • On July 2, 2019, the Organization discovered that an employee's email inbox had been breached by an unknown third party, and an email forwarding rule was enabled which forwarded all inbound emails to an unknown gmail account. • The Organization also discovered that the unknown third party had sent emails from the employee's account, including to a client of the Organization regarding payments and banking info for fraudulent purposes and to divert funds. • On July 5, 2019, the Organization discovered additional forwarding rules were enabled on the employee's account on July 2. The Organization immediately disabled them. • The Organization undertook a comprehensive review of all emails forwarded to the unknown gmail account during the relevant periods (May 27 - July 2 and July 2 - 5, 2019) and determined that three (3) emails potentially contained personal information.
Affected individuals	The incident affected three (3) individuals whose information was collected in Alberta
Steps taken to reduce risk of harm to individuals	• Deleted the forwarding rules and changed passwords for the employee's email account. • Enabled two-factor authentication and re-set passwords company-wide. • Reported the incident to HSBC Bank and the RCMP anti-fraud division. • Reviewed all of the forwarded emails to determine if any contained personal information requiring notification and reporting under Canadian, US, or other applicable law. • Updated password group to force a regular password reset. • Created extra notification alerts on its email platform, including for when a forwarding rule is created so that IT can review and confirm the creation of the rule with the user. • Created a notification email alert to users when they send an email with any type of bank reference or information such as an SIN which allows them to review and confirm that they did in fact send the original email.
Steps taken to notify individuals of the incident	The Organization reported that the affected individuals were not notified because "the 3 affected individuals were all residents of the US and the applicable state and federal privacy laws did not require notification to those individuals."

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, "US counsel reviewed the emails and advised that the information contained in the emails did not trigger any obligations to notify the individuals or report to any regulatory or other bodies under applicable US state and federal laws." The Organization was asked to identify the potential harms and likelihood of risk to the affected individuals in this case. The Organization reported, *For two of the affected individuals, the personal information disclosed was in the nature of personal contact information, including personal email address and personal email address plus phone number. The last affected individual had applied for a job ... and sent a copy of his resume and academic records, which included the individual's address, email, phone number, and details relating to his education and work experience.* *The potential harms that may arise from disclosure of this personal information include phishing (where personal contact info. was disclosed) and identity theft (where info. relating to the individual's work history was provided).* In my view, a reasonable person would consider that the contact information along with email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Employment and education information (work history and academic transcripts) could be used to cause the harms of identity theft and fraud, as well as potentially embarrassment and damage to reputation. These are all 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 did not specifically assess the likelihood that significant harm would result from this incident. 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 and email forwarding rule). The Organization reported "the unknown third party had sent emails from the employee's account, including to a client regarding payments and banking info for fraudulent purposes and to divert funds". The information may have been exposed for approximately five weeks.

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 information along with email address, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Employment and education information (work history and academic transcripts) could be used to cause the harms of identity theft and fraud, as well as potentially embarrassment and damage to reputation. These are all 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 and email forwarding rule). The Organization reported "the unknown third party had sent emails from the employee's account, including to a client regarding payments and banking info for fraudulent purposes and to divert funds". The information may have been exposed for approximately five weeks. 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). **The Organization is required to confirm to my office in writing, within 10 days of the date of this decision, that it has done so.**

Jill Clayton
Information and Privacy Commissioner