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	Custom Electric Ltd. (Organization)
Decision number (file number)	P2021-ND-001 (File #018846)
Date notice received by OIPC	January 5, 2021
Date Organization last provided information	January 6, 2021
Date of decision	January 26, 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 those individuals 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 incident involved the following information: • name, • home address, • year to date earnings, • source deductions, • RRSP contribution amounts, • bonus amounts, and • an internal employee reference number. 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 December 22, 2020, a payroll administrator sent an email attaching employee payroll earning statements to the operations manager and the president. • Earlier that day, the operations manager had received a phishing email; the sender represented themself as the Organization's president. • As a result, when the payroll administrator sent the email to the operations manager and the president, the cache in her inbox attached the phishing email address rather than the president's correct email address. • The operations manager saw the mistake and immediately contacted the sender to recall the email. However, because the operations manager had already opened the email, the recall was unsuccessful. The Organization cannot confirm whether that is because the third party opened it or whether it was because the operations manager opened the email. • The email with the attachment was not encrypted.
Affected individuals	The incident affected 184 residents of Alberta.
Steps taken to reduce risk of harm to individuals	Considering an alternate method for the review process so that the Organization is not exposed to phishing email errors.
Steps taken to notify individuals of the incident	The Organization reported affected individuals would be notified by email on January 8, 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 the possible harms that might result from the breach as, "Name and home address of each employee along with earning values." In my view, a reasonable person would consider that the contact, financial and employment information at issue could be used to cause the harms of identity theft, fraud, or financial loss. 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 "It is not clear whether the email recall was successful to the phishing email address." In my view, a reasonable person would consider that the risk of harm is increased because the breach occurred as a result of malicious activity (phishing) and the information was sent to an unintended recipient. The Organization cannot confirm the email was successfully recalled.

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, financial and employment information at issue could be used to cause the harms of identity theft, fraud, or financial loss. These are significant harms. The risk of harm is increased because the breach occurred as a result of malicious activity (phishing) and the information was sent to an unintended recipient. The Organization cannot confirm the email was successfully recalled. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by email on January 8, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner