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	International Union of Bricklayers and Allied Craftworkers (Organization)
Decision number (file number)	P2021-ND-325 (File #019371)
Date notice received by OIPC	February 8, 2021
Date Organization last provided information	October 25, 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 is located in Washington, DC, USA and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • first and last name, • residential address, • date of birth, • social insurance number, • financial account number, • passport number, and • driver's license number. 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 June 29, 2020, the Organization discovered suspicious activity relating to a number of employee email accounts.

	• An investigation determined that the accounts were subject to unauthorized access between June 4, 2020 and July 10, 2020, but could not rule out access to any emails or attachments within the accounts. • The Organization reviewed the email accounts to determine whether they contained any sensitive information and to whom the information relates. • The Organization reported, "To date, we have no indication that any personal information has been subject to actual or attempted misuse in relation to this incident."
Affected individuals	The incident affected 11,152 individuals, including 1,505 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Changed passwords for the email accounts and began an investigation with assistance from outside computer forensics specialists to determine the nature and scope of the incident. • Implementing multi-factor authentication. • Reviewed policies and procedures and implemented additional safeguards to further secure the information on its systems. • Implemented security hardening measures including the deployment of an endpoint monitoring solution on all systems. • Notified affected regulatory authorities. • Offered affected individuals twelve (12) months of complimentary access to credit monitoring, fraud consultation, and identity theft restoration services.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on December 30, 2020.
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 consequences might include identity theft, fraud, loss of confidentiality of personal data and phishing." The Organization also said "phishing was reported as a potential risk due to the phishing emails received internally by individuals within the organization as part of the Incident as well as the presence of a number of email address/username combinations that were involved. However, we now understand that the potential compromise of these combinations was affecting US residents only and not any Canadian or Alberta residents." In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of 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 no indication that any personal information has been subject to actual or attempted misuse in relation to 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). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately 5 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, identity and financial information at issue could be used to cause the harms of 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). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately 5 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).

I understand the Organization notified the affected individuals by mail on December 30, 2020, accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner