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	Belden Canada ULC (the Organizations)
Decision number (file number)	P2021-ND-043 (File #018289)
Date notice received by OIPC	November 20, 2020
Date Organization last provided information	December 16, 2020
Date of decision	March 2, 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 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, • date of birth, • government-issued identification number (for example, social security / national insurance), • bank account information (of North American employees), • home address, • email address, and • other general employment-related information. 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 November 5, 2020, an unauthorized third party gained access to the Organization's business servers located in St Louis (USA). • On November 12, 2020, the Organization's IT team noticed anomalies and investigated. • On November 13, 2020, the Organization found suspicious software running on an internal system. The system was also seen to be generating outbound traffic to an unknown IP address. • The Organization reported that human resource related identity information might have been targeted and some data of current and former employees was exfiltrated.
Affected individuals	The incident affected 2 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Blocked traffic to the identified external IP via firewall and implemented additional firewall rules to block all traffic using client software. • Instructed a forensic company to revoke the access, protect the assets, and investigate what happened and what was accessed. • Conducting forensic audits of the systems to ensure that the threat has been mitigated and learn more precisely the content of the data that was extracted from its systems. • Ongoing investigations to inform further actions and next steps. • Working with regulatory and law enforcement officials to investigate the matter and have engaged legal counsel to help notify appropriate regulatory authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by way of employee communication on November 24, 2020 and in writing on December 14, 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 harm that may occur as a result of the breach is "Risk of identity fraud." In my view, a reasonable person would consider that 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 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 reported, *From the potential personal data categories involved, data subjects could be at risk of fraud from external actors. [The Organization] is monitoring the situation and will provide an update once the full extent of the breach is known.* 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). In this case, the personal information at issue was exfiltrated and may have been exposed for approximately one (1) week.

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 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 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). In this case, the personal information at issue was exfiltrated and may have been exposed for approximately one (1) week.

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 letter on May 17, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner