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	CDN Controls Ltd. (Organization)
Decision number (file number)	P2021-ND-042 (File #018680)
Date notice received by OIPC	December 11, 2020
Date Organization last provided information	February 19, 2021
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 those 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 all or some of the following information: • name, • address, • telephone number, • bank account information (in some cases), • social insurance number (in some cases), and • payroll documentation (in some cases). 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 December 5, 2020, the Organization suffered a ransomware attack on its computer network. • A high percentage of the organization's information technology infrastructure was infected, with several servers and endpoints encrypted. • A malicious external actor committed the cybersecurity breach. • The Organization reported that it did not find any evidence of misuse of personal employee information; however, it did find evidence that personal employee information was exfiltrated from its network and posted to the threat actor's data leak website. • The Organization determined there is no evidence of malware or vulnerabilities relevant to this incident remaining in its network environment.
Affected individuals	The incident affected 870 Albertans.
Steps taken to reduce risk of harm to individuals	• Shut down all servers to prevent propagation on its network. • Changed all passwords. • Engaged a team of cybersecurity experts. • Rebuilt impacted servers. • Installed antivirus, detection, and response software on all workstations and servers. • Deployed firewall and multifactor authentication. • Review of configurations and controllers. • Provided 12 months of credit monitoring to affected individuals. • Engaged all relevant authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on December 29, 2020 and January 13, 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 may be suffered by the individuals affected by the breach include: loss of control of personal information, identity theft, fraud and loss of confidentiality of information protected by professional secrecy.* In my view, a reasonable person would consider the contact, identity, financial and employment information at issue could be used to cause the significant harms of identity theft and fraud.

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… *… did not find any evidence of misuse of personal employee information, however, it did find evidence that personal employee information was exfiltrated from its network and posted to the threat actor's data leak website.* In my view, 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, ransom demand). In addition, personal information was accessed and stolen.

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 the contact, identity, financial and employment information at issue could be used to cause the significant harms of identity theft and fraud. 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, ransom demand). In addition, personal information was accessed and stolen.

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 affected individuals by letter on December 29, 2020 and January 13, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner