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	Bird Construction, Inc. (Organization)
Decision number (file number)	P2020-ND-142 (File #014746)
Date notice received by OIPC	December 13, 2019
Date Organization last provided information	March 9, 2020
Date of decision	November 6, 2020
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 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 some or all of the following information: • name, • address, • telephone number, • date of birth, • Social Insurance Number, • direct deposit banking information, • copies of driver's licences and health cards, • resume and other information in personnel file. In addition, two former employees also had their passport information accessed and downloaded by the unauthorized third party. This is information 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 2, 2019, files in a number of the Organization's systems were encrypted by an unauthorized third party who demanded a ransom payment in exchange for the keys to decrypt the files and to destroy data that the unauthorized party claimed to have taken from the Organization's systems. • The Organization reported that it believes that the unauthorized third party gained access to its IT infrastructure on November 20, 2019. • The Organization later confirmed that certain data, including employee files, was accessed by the unauthorized third party and downloaded to the unauthorized third party's server. The Organization's forensic experts confirmed that this information was deleted from the unauthorized third party's server, but the Organization cannot rule out the possibility that a copy of the information remains with the unauthorized third party.
Affected individuals	The incident affected approximately 498 current and former employees in Alberta.
Steps taken to reduce risk of harm to individuals	• Assembled a crisis management team to oversee a coordinated approach to investigation, containment, remediation and restoration efforts. • Launched a forensic investigation and engaged external security and privacy experts. • Implemented containment strategy, taking systems offline, commencing network and systems segmentation, reconfiguring enhancements to its firewall policy, and enhancements to systems monitoring controls. • Implementing a systems cleansing and restoration strategy. • Reported the incident to law enforcement and the Canadian Cyber Security Centre. • Offering credit monitoring to employees. • Reviewing security policies and procedures with a view to making enhancements, where necessary.
Steps taken to notify individuals of the incident	Affected individuals were notified in December 2019.

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 did not specifically identify the harm(s) that might result to individuals from this incident, but its notice to employees said "… out of an abundance of caution, we are taking the proactive step of providing all personnel with access to credit monitoring and identity theft restoration services", and "we urge you to review and consider implementing the identify theft and fraud prevention steps outlined in the attached, "Additional Resources and Fraud Alerts"." In my view, a reasonable person would consider that 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 did not specifically provide an assessment of the likelihood of harm resulting from this incident but did report that it "…cannot rule out the possibility that a copy of this information remains with the unauthorized third party." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the incident resulted from malicious action of an unknown third party (deliberate action, ransom demand). The Organization confirmed personal information was accessed and downloaded to a third party's server and cannot rule out the possibility that a copy of the information remains with the third party.

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, 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 incident resulted from malicious action of an unknown third party (deliberate action, ransom demand). The Organization confirmed personal information was accessed and downloaded to a third party's server and cannot rule out the possibility that a copy of the information remains with the third party.

I require the Organization to notify the affected individuals whose 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 in December 2019. The Organization is not required to notify the affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner