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	J.V. Driver Corporation Inc. (Organization)
Decision number (file number)	P2021-ND-150 (File #0020731)
Date notice received by OIPC	April 23, 2021
Date Organization last provided information	May 12, 2021
Date of decision	June 8, 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 some or all of the following information: • first and last name, • date of birth, • gender, • social insurance number/social security number, • postal address and email address, • telephone number, • job title/position, • employee code and employment status, • salary information, • banking information, • medical information (LTD/STD application materials for less than 50 individuals). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 17, 2021, the Organization learned it was the victim of a ransomware attack. The initial access appears to have been on January 6, 2021. • The source of the intrusion appears to be when an employee provided domain credentials in response to a phishing email and approximately 8 hours later, the attacker accessed the network remotely using these credentials. • It does not appear the attacker engaged in actual data theft until approximately March 10, 2021 and did not copy ransomware onto the network until approximately March 17, 2021. • On March 18, 2021, an email was received by various members of the executive leadership team that appeared to be from the attacker. • On April 8, 2021, the Organization confirmed that it was the victim of a sophisticated, illegal ransomware attack, which resulted in hackers gaining access to employee files containing personal information. • The Organization reported that it was unable to determine with absolute certainty the full scope of the personal information actually accessed.
Affected individuals	The incident affected approximately 30,000 individuals.
Steps taken to reduce risk of harm to individuals	• Shut down all servers and back-up server access to all users, in order to contain any further breach. • Identifying and implementing additional security measures to try to prevent an incident of this nature in the future. • Enabled multifactor authentication for all users. • Reviewed all active directory accounts and those deemed unnecessary were disabled. • Implemented new network access protocols. • Reviewing current privacy policies and procedures to identify improvements. • Reviewing and implementing cyber security training for all users of IT systems.
Steps taken to notify individuals of the incident	The affected individuals were notified by email and by mail, which was completed on May 12, 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 occur as a result of the breach depend on the specific personal information that was accessed for each individual. For example, with respect to personal information like date of birth and/or social insurance numbers, potential harm includes identity theft. Other categories of information that were potentially compromised are not sensitive and do not necessarily give rise to a risk of harm.* In my view, a reasonable person would consider that the contact, identity and financial information could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Salary, compensation and medical information could be used to cause embarrassment, hurt or humiliation and possibly damage to reputation. 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: *There is a risk of harm given the sensitivity of certain categories of the potentially compromised information and given that the potential compromise arises in the context of a ransomware attack.* 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, ransomware). Further, the unknown third party had access to the information for approximately 72 days.
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 could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Salary, compensation and medical information could be used to cause embarrassment, hurt or humiliation and possibly damage to reputation. 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, ransomware). Further, the unknown third party had access to the information for approximately 72 days.	

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 email and by mail, which was completed on May 12, 2021, in accordance with the *Regulation*. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner