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-131 (File #019494)
Date notice received by OIPC	February 12, 2021
Date Organization last provided information	April 14, 2021
Date of decision	May 18, 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 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 all or some of the following information: • name, • home address, • termination/severance information, • salary/compensation amounts, • social insurance number, • driver license information, • passport information, • life insurance information, • tax slip information and investigation, • investigation/fraud report submissions, • business and/or personal contacts of targeted user and whose personal information included title/position, email, telephone number and home address. This information is about identifiable individuals (employees, contractors, personal contacts) and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization also reported that some of the personal information was for business contacts. "Business contact

	information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As such, PIPA applies.
DESCRIPTION OF INCIDENT	
□ loss ☒ unauthorized access □ unauthorized disclosure	
Description of incident	• On January 7, 2021, an employee of the Organization received a phishing email which contained a link to a malicious 'github.io' sub-domain, which hosted a fake Microsoft account login page. The employee entered their account credentials into this phishing page. • On January 11, 2021, an unauthorized third party logged onto the employee's email account, and started to transmit about 1,500 phishing emails from the employee's email account. The employee notified the Organization's IT team. • The unauthorized third party attempted to log back in on January 11, 2021, but was blocked from doing so.
Affected individuals	The incident affected 2,389 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Locked employee's account temporarily and changed the password. • Blocked and removed the unauthorized third party. • Notified recipients of the phishing email issued from an Organization's email address. • Issued an Organization-wide alert warning of phishing emails coming from legitimate users. • Engaged an external third party to assist with the investigation and to perform an audit. • Required complex passwords for all users with specific parameters. • Required senior leadership to have discussions with employees about cyber security issues.

	• Plan to rollout refresher training on cyber security measures for employees to ensure content appropriately reflects the current legal framework around privacy laws. • Reviewing current Privacy Policy and organizational security measures, including recommendations made by third party IT security consultant.
Steps taken to notify individuals of the incident	The affected individuals were notified by email and mail in batches from February 5, 2012 to March 2, 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 depends on the personal information that has been accessed in an unauthorized manner...For example, with respect to much of the information disclosed (e.g. SIN, passport, drivers license, and), potential harms to affected individuals include financial loss, fraud, and identity theft / negative effects on a credit record. Indeed, personal contact information (e.g. email addresses), particularly when in combination with other personal information elements, could be used for phishing purposes, increasing vulnerability to fraud and identity theft / negative effects on a credit record...Finally, salary and compensation can result in: (i) embarrassment, hurt or humiliation; and (ii) possibly damage to reputation.* I agree with the Organization's assessment. 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 vulnerability to identity theft and fraud. Salary and compensation information could result in 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, *The following factors militate [sic] in favour of a low likelihood of harm:* *1. the information was not exposed for a long period -- the third party rogue had access to the applicable account for only a few hours;* *2. an external third party audit was performed which confirmed containment of the breach and also confirmed that appropriate remedial steps were taken in response to the breach;*

> *3. some of the information in the account was encrypted; and*
> *4. the personal information of no vulnerable persons was accessed by the rogue.*
>
> *The following factors militate [sic] in favour of a high likelihood of harm:*
>
> *1. there is evidence of malicious intent by the rogue -- the rogue sent a phishing email to 1500 individuals (but we note that [the Organization] promptly sent an email to each of the 1500 recipients of the rogue's phishing email requesting the deletion of that email);*
> *2. the information appears to have been used for criminal purposes, such as for identity theft or fraud.*
> *3. an individual's name, mailing addresses and email address are not, by themselves, generally sensitive information; but the fact that the rogue sent a phishing email to 1500 individuals suggests that such information is sensitive;*
> *4. salary information, tax information, passport information, SIN are generally considered sensitive information;*
> *5. the rogue's unauthorized access affected a large number of individuals; and*
> *6. the information accessed by the rogue was not recovered.*
>
> *Take together, the factors point to a high likelihood harm arising from this breach. Accordingly, we have elected to notify each of the affected individuals.*

I agree with the Organization’s assessment. 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). Further, the unknown third party had access to the information and sent phishing emails to 1,500 individuals.

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 vulnerability to identity theft and fraud. Salary and compensation information could result in 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). Further, the unknown third party had access to the information and sent phishing emails to 1,500 individuals.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email and mail from February 5, 2012 to March 2, 2021. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner