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	Driver's Industrial Installations Ltd. (Organization)
Decision number (file number)	P2021-ND-148 (File #019496)
Date notice received by OIPC	February 12, 2021
Date Organization last provided information	May 18, 2021
Date of decision	June 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 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: • employee name, and • weekly pay. 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 January 7, 2021, an employee of a service provider to the Organization received a phishing email, prompting her to enter account credentials. • On January 11, 2021, an unauthorized third party used the credentials to log into the employee's email account, and send approximately 1,500 phishing emails. • The employee notified the service provider's IT team who took action to contain the breach.

	• Also on January 11, 2021, emails began transmitting from the service provider's email address advising recipients of an investment scheme opportunity. Recipients of these emails were asked to click on a linked attachment and enter their information. The service provider became aware of the issue when it began receiving calls asking if the emails were legitimate. Upon learning about the emails, the service provider's IT team took actions to contain the breach.
Affected individuals	The incident affected 348 residents of Alberta.
Steps taken to reduce risk of harm to individuals	<u>Service provider</u> • Locked the employee's account temporarily and changed password. • Blocked and removed the rogue actor, containing the breach. • Investigated, in order to mitigate risk and reduce harm. Engaged an external third party to assist with the investigation and to perform an audit. • Began systematic monitoring of the compromised email and the server. • Issued a company-wide alert warning of phishing emails coming from legitimate users, instructing users to delete the emails and not to click on any email or link, and notify IT immediately. • Implemented requirements for more complex passwords for all users with specific parameters. • Planning refresher training on cyber security measures for employees to reflect the current legal framework around privacy laws. • Implementation of protocol regarding the use of external hard drives and USBs. <u>Organization</u> • Reviewing privacy policy and arrangements with service providers. • Advised affected individuals to request a credit report, place a fraud alert on the credit report, and remain vigilant about suspicious activity. • Reviewing security measures, including recommendations made by its third party IT security consultant. • Implementing multiple factor authentication for system access.

Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 1, 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 include: (i) embarrassment, hurt or humiliation; and (ii) possibly damage to reputation." I accept the Organization's assessment. A reasonable person would consider that the employment information (salary) at issue could be used for the purposes of causing embarrassment, hurt and/or humiliation and possibly damage to reputation. These are 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 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 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 this did not directly affect our employees as none of our employee email addresses were accessed);* *2. the information appears to have been used for criminal purposes, such as for identity theft or fraud;* *3. salary information is generally considered sensitive information;* *4. the rogue's unauthorized access affected a large number of individuals; and* *5. 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 (phishing). The compromised email account was used to send additional phishing emails. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach.

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 employment information (salary) at issue could be used for the purposes of causing embarrassment, hurt and/or humiliation and possibly damage to reputation. These are 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 (phishing). The compromised email account was used to send additional phishing emails. Although the Organization has put additional safeguards in place, these were not in place at the time of the breach.

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 March 1, 2021 in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner