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-145 (File #020854) |
| **Date notice received by OIPC** | May 4, 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:<br><br>• full name,<br>• date of birth,<br>• gender,<br>• social insurance number/social security number,<br>• home address and postal address,<br>• email address,<br>• telephone number,<br>• job title/position,<br>• employee code and employment status,<br>• salary information, and<br>• banking information.<br><br>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 April 8, 2021, the Organization learned that one of its service providers had been the victim of a ransomware attack which resulted in hackers gaining access to employee files containing personal information.<br>• The source of the intrusion appears to be when an employee provided their domain credentials in response to a phishing email and approximately 8 hours later, the attacker used the credentials to access the network remotely. This initial access appears to have been on January 6, 2021.<br>• The attacker does not appear to have engaged in actual data theft until approximately March 10, 2021 and did not copy ransomware onto the network until approximately March 17, 2021.<br>• On March 18, 2021, various members of the service provider's executive leadership team received an email that appeared to be from the attacker. The email included limited information about data files that the attacker alleged to have stolen from the network because of the ransomware attack.<br>• On April 8, 2021, the service provider determined the nature and extent of the personal information impacted by this breach. |
| **Affected individuals** | The incident affected 2,455 individuals. |
| **Steps taken to reduce risk of harm to individuals** | <u>Service Provider:</u><br><br>• Shut down all server and back-up server access to all users.<br>• Notified all users of the system outage.<br>• Had multiple discussions with cyber security experts to ensure the breach was contained and that the attacker was no longer in the network.<br>• Carried out a network-wide analysis and monitoring to ensure the attacker was no longer in the network and could no longer access the network data.<br>• Required employees to change passwords.<br><br><u>Organization</u>:<br><br>• Identifying and implementing additional security measures to try to prevent an incident of this nature in the future.<br>• Enabled multifactor authentication for all users.<br>• Disabled all active directory accounts deemed unnecessary.<br>• Increased restrictions on access to the network.<br>• Monitoring the network multiple times a day.<br>• Reviewing current privacy policies and procedures to identify improvements. |

| | |
|---|---|
| | • Reviewing and implementing cyber security training for all users of IT systems.<br>• Contacted the RCMP.<br>• Provided affected individuals with information on how to request a credit report and how to place a fraud alert on their credit report. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by email and letter on May 7, 2021 and May 10, 2021. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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:<br><br>*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.*<br><br>*Other categories of information that were potentially compromised are not sensitive and do not necessarily give rise to a risk of harm.*<br><br>In my view, a reasonable person would consider that the contact, identity, financial and employment information at issue could be used for the purposes of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms. |
| **Real Risk**<br>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:<br><br>*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.*<br><br>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, 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 that the contact, identity, financial and employment information at issue could be used for the purposes of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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, 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 email and letter on May 7, 2021 and May 10, 2021, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner