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	K2 Corrosion Fasteners Incorporated (Organization)
Decision number (file number)	P2022-ND-035 (File #024161)
Date notice received by OIPC	November 30, 2021
Date Organization last provided information	March 30, 2022
Date of decision	May 13, 2022
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 headquartered in Burnaby, British Columbia, 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: For current and former employees: • name, • date of birth, • social insurance number, • residential address, • email address, • telephone number, • salary, • date of hire, • tax information, and • banking information. For prospective employees: • name, • residential address, • email address, • telephone number, and • resumes.

	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 October 15, 2021, the Organization discovered they were victim to a ransomware attack. • The Organization did not determine how the threat actor compromised their network. • An investigation did not rule out the possibility that data was accessed or exfiltrated.
Affected individuals	The incident affected 197 of individuals, including 24 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Offered credit monitoring and identity theft services to affected individuals who were employed at the time of the incident. • "Provided all affected individuals with information about steps they can take to protect themselves against harm." • Reported the incident to law enforcement. • Engaged a cyber security firm to secure the Organization's network. • Established mandatory security awareness training. • Migrated to a cloud-based system. • Implemented additional technical safeguards and hardened certain policies and practices.
Steps taken to notify individuals of the incident	Employees were notified verbally or by text message on October 18, 2021. Employees and former employees were notified in writing on October 28, 2021. Prospective employees were notified in writing on November 18, 2021. A supplemental written notice containing contact information for someone at the Organization who could answer questions in relation to the incident was provided on November 30, 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	The Organization reported: "The information could be used for the purpose of fraud, including identity theft, credit/bank fraud and social engineering."

also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	I agree with the Organization's assessment. A reasonable person would consider that identity (date of birth, social insurance number), contact, employment (salary), and financial (banking, tax) information at issue could be used to cause the harms of identity theft, fraud, financial loss, and have a negative effect on a credit record. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to the above. 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: *Unknown. Any assessment of the likelihood of harm would require speculation, given that it is unknown whether any persional [sic] information was in fact accessed or exfiltrated by the threat actor. However, the circumstances of the incident (malicious threat actor, ransomware malware) raise the possibility that any compromised persional [sic] information may be used to illigitimate [sic] purposes which could result in harm to affected individuals.* 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 a threat actor (deliberate intrusion, deployment of ransomware). The Organization could not rule out the possibility that records were exfiltrated.

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 identity (date of birth, social insurance number), contact, employment (salary), and financial (banking, tax) information at issue could be used to cause the harms of identity theft, fraud, financial loss, and have a negative effect on a credit record. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to the above. 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 a threat actor (deliberate intrusion, deployment of ransomware). The Organization could not rule out the possibility that records were exfiltrated.

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 phone and/or in writing between October 18, 2021 and November 30, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance