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	Entreprise Robert Thibert Inc. (Organization)
Decision number (file number)	P2021-ND-320 (File #021164)
Date notice received by OIPC	May 17, 2021
Date Organization last provided information	May 17, 2021
Date of decision	March 9, 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 a distributor, designer and manufacturer of wheels, tools, trailers, automotive and recreational vehicle accessories, and is also one of the largest axle and trailer assembly manufacturers in Canada. The Organization has employees in Canada and the United States of America. 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 all or some of the following information of current and past employees: • full name, • email and residential address, • date of birth, • banking information provided for payroll, • health information, • social insurance number, • government identification, and • full name and date of birth of relatives designated on group insurance request forms, where applicable. 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 25, 2021, the Organization discovered that an unauthorized party gained access to a directory that contained employee personal information. • The Organization reported, "This directory does not contain any structured files of personal information, which significantly reduces the risk of malicious use." • The Organization discovered the incident on January 25, 2021 when it noticed that some of its computer systems were encrypted and no longer accessible.
Affected individuals	The incident affected 1,140 individuals, including 419 individuals whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Contained the incident and retained the services of IT and cybersecurity experts to investigate and make recommendations to strengthen security. • Changed the passwords on all user accounts. • Addressed vulnerabilities identified by experts on its IT infrastructure. • Closely monitoring systems and security enhancement opportunities will be seized as they are discovered. • Offered a 12 month subscription to credit monitoring services to all potentially affected individuals, where applicable. • Established a contact center to respond to telephone calls and email inquiries from potentially affected individuals. • Notified local law enforcement agencies and privacy regulators.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on April 26, 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 consequences might include an increased risk of phishing or other social engineering attacks, and an increased risk of fraudulent transactions." In my view, a reasonable person would consider the contact, identity, financial, medical and employment information at issue could be used to cause the significant harms of identity theft, fraud, financial loss, hurt, humiliation and embarrassment. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. 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: *While there is no indication that the personal information affected by the incident was or will be misused, there is a possibility that the harm described under Question 12 could materialize, given the nature of the incident.* *Furthermore, the fact that the potentially affected information was not structured and that a significant portion of that information was handwritten limit the likelihood that the harm will result.* 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, encryption). The Organization reported that the cybercriminal gained access to personal information its directory. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make public the personal information at issue.

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 the contact, identity, financial, medical and employment information at issue could be used to cause the significant harms of identity theft, fraud, financial loss, hurt, humiliation and embarrassment. Email addresses could be used for 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, encryption). The Organization reported that the cybercriminal gained access to personal information its directory. The Organization can only assume that cybercriminal did not or will not misuse, disseminate or otherwise make public the personal information at issue.

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 April 26, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner