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	The Stevens Company Limited (Organization)
Decision number (file number)	P2022-ND-039 (File #022863)
Date notice received by OIPC	August 18, 2021
Date Organization last provided information	August 18, 2021
Date of decision	May 18, 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 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, • address, • social insurance number, • date of birth, • tax forms, and • payroll information (hours paid, gross salary, average salary per hour, job title, hire date, benefits, payroll deposit forms, sick days, leave information, offer letters, and information change forms.) 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 10, 2021, the Organization discovered that it was the victim of a cybersecurity attack by an unauthorized third party. The malicious actor deployed ransomware to encrypt the Organization's technology infrastructure and to exfiltrate data. • The Organization's IT team noticed anomalies on the system during regular process checking. • The incident occurred from March 13, 2021 to April 10, 2021.
Affected individuals	The incident affected 474 individuals, including 53 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	Steps taken by the Organization include but are not limited to: • Disconnected its systems from the internet and VPN. • Engaged legal counsel and a leading cyber forensic firm to conduct a comprehensive investigation. • Conducted a detailed investigation and implemented an incident response plan. • Offered credit monitoring services to the affected individuals for a period of 24 months. • Rebuilt its entire corporate network. • Re-imaged workstation devices and securely added to the network. • Reset users' passwords, enabled multi-factor authentication and enabled security certificates on all remote VPN devices.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or letter on August 17, 2021 and August 18, 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, *It is Stevens' assessment that there is a risk of identity theft, fraud, financial loss, hurt, humiliation and embarrassment since the potential personal information involved in the incident is contact, identity, financial and employment information.* I agree with the Organization's assessment. A reasonable person would consider the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, financial loss, hurt, humiliation and embarrassment.
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	The Organization reported, *Stevens is of the view that the likelihood that harm could result is low to moderate. While Stevens has no evidence confirming that the personal information at issue has been compromised or misused by the external actor, the personal information*

between the incident and the possible harm.	*involved in the incident is nonetheless sensitive and could be used for the purposes identified above.* *The fact that the incident was caused as a result of the actions of an unknown actor with malicious intent additionally increases the likelihood that harm could result*. In my view, a reasonable person would consider 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). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. The attacks appear to have been ongoing for approximately one month before the Organization discovered the threat.

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 and financial information at issue could be used to cause the significant harms of identity theft, financial loss, hurt, humiliation and embarrassment.

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). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. The attacks appear to have been ongoing for approximately one month before the Organization discovered the threat.

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 or letter on August 17, 2021 and August 18, 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