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	Elliott Company (Organizations)
Decision number (file number)	P2021-ND-321 (File #020871)
Date notice received by OIPC	May 10, 2021
Date Organization last provided information	May 10, 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 the individual 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's head office is in Jeannette, PA, USA. 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, • email and/or physical address, • telephone number, • date of birth and, • U.S. Social Security number. 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 March 29, 2021, a threat intelligence vendor notified the Organization about a potential data compromise resulting from a malware attack on the Organization's computer systems in Sparks, Nevada.

	• The Organization investigated to determine the nature and extent of the incident and what data had been compromised. • The Organization believes (but has not been able to confirm) that the security of some archived human resources was compromised. • The Organization reported the breach occurred on February 15, 2021.
Affected individuals	The incident affected 878 individuals, including one (1) whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Enhancing security to prevent similar occurrences in the future, including through the engagement of cybersecurity consultants and the implementation of additional layers of cybersecurity threat monitoring. • Arranged for identity protection services, including credit monitoring, at no charge to the affected individuals for twenty-four (24) months.
Steps taken to notify individuals of the incident	The affected individuals were notified by letter and email on May 10, 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 result from the breach are "Identity theft / fraud." In my view, a reasonable person would consider the contact and identity information could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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 likelihood of misuse of a U.S. Social Security number for a Canadian resident seems relatively low, although vigilance is still recommended. The risk of harm is mitigated to some extent by the identity protection and credit monitoring services offered free of charge.* 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 (malware attack).

	Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the compromised information were to be used for fraudulent purposes.

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 individual.

A reasonable person would consider the contact and identity information could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. 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 (malware attack). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the compromised information were to be used for fraudulent purposes.

I require the Organization to notify the affected individual 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 the affected individual by letter and email on May 10, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner