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	Zedi Canada Inc. (Organization)
Decision number (file number)	P2019-ND-203 (File #012581)
Date notice received by OIPC	March 22, 2019
Date Organization last provided information	March 22, 2019
Date of decision	December 17, 2019
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 the following information: • name, • home address, • social insurance number, • salary information, • income tax and, • other withholding information listed on tax forms. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization engaged a tax consulting service provider.

	• The Organization reported that, on February 27, 2019, its service provider determined that a former employee had surreptitiously and unlawfully downloaded data, some of which contained confidential information on the Organization's current and former employees, to a remote server during his short-term employment from January 28, 2019 to February 20, 2019. • The service provider informed the Organization about the breach on March 14, 2019. • The service provider's former employee has since been arrested and charged.
Affected individuals	The incident affected up to 3,000 individuals, including 191 current and former employees of the Organization.
Steps taken to reduce risk of harm to individuals	The Organization: • Offered, through the contractor, free credit monitoring through Equifax for 12 months. • Will ensure information provided to service providers is kept to the bare minimum. • Will ask the service provider and other providers to remove all employee data from its system after work has been completed. The Organization reported that its vendor: • Changed passwords on systems, devices and applications. • Shut down any remote access capability. • Installed additional security and monitoring software. • Remediated gaps in its security systems. • Intends to update training to its employees about cybersecurity risks and review policies to combat risks in the future.
Steps taken to notify individuals of the incident	Affected individuals (current and former employees) were notified by email on March 15, 2019, and in writing on March 18, 2019.
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 that "The primary risks that could potentially result from this incident, depending upon the personal information that may be determined to have been stolen, are those related to fraud, financial loss and identity theft." I agree with the Organization's assessment. A reasonable person would consider that the identity, tax and employment information at issue could be used to cause the significant harms of identity theft, financial loss and fraud, as well as 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 between the incident and the possible harm.	The Organization reported that its service provider… *… has informed us that to date, the extortion attempts have been directed at companies and not individuals and it is hoped that the quick identification of the employee and the CPS' plans to execute a search warrant will prevent further such attempts. However, there is currently a risk of similar extortion or other financial impacts to affected individuals. As noted below, [the service provider] has taken several steps to minimize the likelihood of harm from this incident…."* In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month. It appears that information was used for extortion (though not of individuals).

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 identity, tax and employment information at issue could be used to cause the significant harms of identity theft, financial loss and fraud, as well as hurt, humiliation and embarrassment. The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (theft). The information was apparently unlawfully downloaded over the course of almost a month. It appears that information was used for extortion (though not of individuals).

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 that affected individuals were notified by email on March 15, 2019, and in writing on March 18, 2019. . The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner