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	BC Investment Management Corp. (Organization)
Decision number (file number)	P2018-ND-013 (File #007364)
Date notice received by OIPC	December 20, 2017
Date Organization last provided information	December 20, 2017
Date of decision	January 11, 2018
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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • home address, • email address, • telephone number, • work experience, • education including scholarships and awards, • professional designations, • references to personal interests, and • GPA/GMAT scores. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected from residents of Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On November 9, 2017, between 7:30 pm and 9:45 pm., an employee of the Organization discovered that his personal vehicle had been broken into while it was parked in downtown Vancouver, British Columbia. A work-issued portable electronic device was stolen. • The device was password protected by not encrypted. • The incident was discovered on November 9, 2017. • To date the device has not been recovered. The Organization reported "no evidence exists to suggest that the information has been accessed."
Affected individuals	The incident affected a total of 500 individuals, including approximately 55 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported incident to law enforcement. • Engaged private investigative companies to locate and retrieve the device and determine if the information was accessed. • Changed the network password, and all employees have been instructed to remove personal information from the local drives of their work devices. In addition, changes to information technology procedures and a training and awareness campaign are being adopted across the Organization.
Steps taken to notify individuals of the incident	All individuals potentially affected by this incident were notified in writing, on December 19, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "Identity theft and fraud are the principal types of harm that could possibly result from the types of information involved in an incident of this kind." I agree with the Organization. The comprehensive profile information included in a resume (contact, educational and employment history) could also be used for identity theft and fraud, which are significant harms. Email addresses could be used for phishing purposes. Previous breach notification decisions issued by my office have identified phishing as a significant harm.
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 "An employee was the victim of a break-in to his personal vehicle by unknown parties who stole the Device containing the information … no evidence exists to conclude that the information has been accessed or that any individual has suffered actual harm. The theft was not targeted, rather, it was random and, although the information on the Device does not relate to highly sensitive information, all individuals whose resumes are stored on the Device have been notified."

	In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (vehicle break-in and theft). The device was not encrypted and has not been recovered.

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 as a result of this incident.

The comprehensive profile information included in a resume (contact, educational and employment history) could also be used for identity theft and fraud, which are significant harms. Email addresses could be used for phishing purposes. Previous breach notification decisions issued by my office have identified phishing as a significant harm. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (vehicle break-in and theft). The device was not encrypted and has not been recovered.

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that all individuals potentially affected by this incident were notified in writing, on December 19, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner