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	VersaCold Logistics Services (Organization)
Decision number (file number)	P2020-ND-130 (File# 013801)
Date notice received by OIPC	May 23, 2019
Date Organization last provided information	May 23, 2019
Date of decision	October 30, 2020
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 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, • email address, • home address, • date of birth, • salary, • position, • bank account information (bank account number but not financial institution or branch identification number) and, • in some cases, social insurance 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 May 12, 2019, a person or persons broke into the Organization's office premises and stole eight laptop computers. The laptops were password protected. • The incident was discovered on May 13, 2019 when employees arrived at work.
Affected individuals	A total of 3,200 individuals were affected, including 371 in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported incident to law enforcement. • Offered credit monitoring to all impacted current and former employees. • Will encrypt all laptops that are used to store personal information and enhance office security.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on May 17, 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 "The names and SIN could be used for identity theft and fraud" and "The email addresses could be used in phishing attempts". In my view, a reasonable person would consider the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud.
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 risk is real but modest. While there is evidence of malicious intent because this was a theft, there is no evidence the theft was targeted at obtaining personal information and the laptops were password protected. The mitigation steps, including alerting the affected individuals to be vigilant about suspicious activity and phishing attempts and offering credit monitoring, will further mitigate the risk." 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 malicious action (break-in and theft). The Organization can only speculate as to the motives of the thieves. The Organization did not report that the laptops were encrypted, nor that they were 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.	

A reasonable person would consider the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action (break-in and theft). The Organization can only speculate as to the motives of the thieves. The Organization did not report that the laptops were encrypted, nor that they were recovered.

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.* I understand affected individuals were notified by mail on May 17, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner