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	Quarterhill Inc. (Organization)
Decision number (file number)	P2020-ND-016 (File #013716)
Date notice received by OIPC	October 7, 2019
Date Organization last provided information	October 7, 2019
Date of decision	February 13, 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 the following information: • names; • addresses; • social insurance numbers; and • dates of birth. 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	• An employee responsible for Human Resource functions used a corporate owned laptop to access a file on the laptop in cloud storage containing personal information of current and former employees and directors. Due to the settings on the laptop, the file synced to the laptop's hard drive.

	• On August 29, 2019 at approximately 1:00 pm local time, an individual entered the Organization's Kitchener, Ontario premises through an unlocked door and stole the laptop and one other. • Access to the laptop computers was password protected. The file at issue was on the laptop's hard drive, which was not encrypted.
Affected individuals	The incident affected 103 current and former employees and directors, including 2 individuals who reside in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement. • Investigated and reset the user credentials to the laptop. • Offered credit monitoring and identity theft insurance to the affected individuals for 2 years at no cost. • Will continue to educate and train employees regarding the importance of compliance with policies relating to safety and security of workspaces, protecting privacy of personal information and ensuring confidentiality of information. • Reviewing physical and technical security measures and procedures and intends to introduce measures to reduce the chance of future security incidents.
Steps taken to notify individuals of the incident	The affected individuals were notified in writing on October 4, 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 disclosure of personal information at issue could potentially cause affected individuals to suffer from the harms of identity theft/ fraud, including a risk of phishing attacks". In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of 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 likelihood that harm may occur to affected individuals as it relates to the laptop computers is moderate. The personal information is accessible if an individual is able to bypass login security protections to the Employee's laptop and the sensitivity of the personal information contained within the laptop is high.*

	The context of the Incident is generally indicative of the laptop having stolen by the thief for resale, and there are no indications that the theft was targeted for the personal information at issue. However, while [the Organization] is not aware of any personal information of any affected individual being misused, it has not recovered the Employee's laptop computer and cannot determine if the personal information was accessed by a third party at any point in time. *Additionally the Incident was caused as a result of the theft of the laptops (malicious intent) rather than a mistake, which increases the likelihood that harm could result to affected individuals. There is minimal likelihood that the breach will cause harm.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident was the result of malicious action (theft) and the information has not been recovered. The Organization can only speculate as to the motives of the thief.

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 contact and identity information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased because the incident was the result of malicious action (theft) and the information has not been recovered. The Organization can only speculate as to the motives of the thief.

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

I understand the Organization notified the affected individuals in writing on October 4, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner