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	Pasquini & Associates Consulting Ltd. (Organization)
Decision number (file number)	P2018-ND-001 (File #005480)
Date notice received by OIPC	April 25, 2017
Date Organization last provided information	April 25, 2017
Date of decision	January 2, 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • telephone number, • Social Insurance Number, and • bank account information. 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	• On or about April 14, 2017, the Organization's office was broken into and a laptop and tablet were stolen. • The laptop may have contained the personal information of some of the Organization's employees.

	• On or about April 16, 2017, the Organization's office was again broken into and 6 more laptops/tablets were stolen. These devices may have contained personal information of the individual assigned the laptop/tablet by the Organization. • The laptops and tablets were password protected but not encrypted. • One tablet was recovered by police but the hard drive was wiped clean. • The first incident was discovered April 15, 2017, and the second incident was discovered April 17, 2017.
Affected individuals	The incident affected 15 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Filed police reports and serial numbers of the stolen computers were provided. • Changed locks to exterior doors of the building. • Installed security cameras with video surveillance in the office. • Added strike plates to the card key access doors so the locks cannot be tampered with. • Advised employees to report any suspicious activity. • Implementing new security protocol measures. • Requiring employees to take laptops and tablets home daily. • Provided instructions on how affected individuals can monitor their credit files and provided access to fraud specialists.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally on April 17, 2017 and by email on April 24, 2017.
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 might result from this incident include "Fraud, identity theft, negative credit record, propery [sic] loss." I agree with the Organization. The identity and financial information at issue could be used to cause the harms of identity theft, fraud, and negative effects on a credit rating. 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 that "the harm would only be significant if the SIN numbers were made public. The key concern would be identity theft. Police recovered one of the stolen tablets and it was wiped clean. This would suggest that the information/date is not the main target." Further, "The main purpose of the theft appears to be property which can quickly be turned into cash. All computers were password protected. The risk is if access to the information can be obtained. Then identity theft or fraud could occur with the information." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious actions of an unknown third party. In addition the laptops/tablets were not encrypted and only one tablet has been recovered. Although the Organization does not believe the information/data was the target of the theft, it is impossible to know for sure.

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.

The identity and financial information at issue could be used to cause the harms of identity theft, fraud, and negative effects on a credit rating. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious actions of an unknown third party. In addition the laptops/tablets were not encrypted and only one tablet has been recovered. Although the Organization does not believe the information/data was the target of the theft, it is impossible to know for sure.

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

I understand the Organization notified affected individuals verbally on April 17, 2017 and by email on April 24, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner