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	Mother Parker's Tea & Coffee Inc. (Organization)
Decision number (file number)	P2021-ND-080 (File #016690)
Date notice received by OIPC	October 7, 2019
Date Organization last provided information	October 7, 2019
Date of decision	March 16, 2021
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: Employee and former employee: • name, • address, • telephone number, • personal email address, • date of birth, • social insurance number, • salary, and • other employment-related information. Applicant information: • name, • residential address, • telephone number, • email address, • date of birth, • work history, and • information submitted during a job application.

	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 July 21, 2019, an employee of the Organization was on a plane from Fort Worth to Houston, TX. The employee had a company laptop and was using it during the flight. • Sometime after departing the plane after arrival, the employee noticed that the laptop was not in their carry-on luggage. • The Organization assumes the laptop was left on the plane. • The laptop was password protected (with a strong password) but not encrypted. • The employee notified the Organization of the loss on July 22, 2019. • The Organization reported efforts to retrieve the laptop have been unsuccessful to date.
Affected individuals	The incident affected 1,823 individuals of which 5 were residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Changed password and disabled laptop from Active Directory. • Monitored Office 365 for new connections, unusual incoming and outgoing email traffic and moves, deletes and downloads of One Drive documents. • Monitored VPN and Active Directory logs for access attempts from the laptop in question and the use of the individual's old password. • Engaged a third party IT service provider to assist in deploying device encryption. • Deploying a device management platform and multi-factor authentication for all mobile devices. • Providing employee training on cybersecurity. • Provided free credit monitoring for 12 months.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and email (where mailing address not available) on October 7, 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 harm that could result from misuse of the information at issue is identity theft and fraud (misuse of contact information and personal identifiers such as SIN) and damage to reputation, as well as humiliation (based on the salary and other employment-related information involved).* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Employment information (e.g. salary) could also be used to cause hurt, humiliation or embarrassment. These are all 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, *The laptop has not been recovered as of date; given the location of the likely loss (on the plane) the most likely cause of the loss was that it was left on the plane as opposed to a targeted theft. The likelihood (sic) that the laptop was recovered by an individual who was then both interested and also capable of bypassing the password-secured device is assessed as being quite low.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is decreased because the breach did not result from malicious action, but rather the laptop was likely left on the plane. However, the laptop has not been recovered and is protected only by a logon password, and not encrypted. The fact that the laptop has not been turned in suggests a real possibility that anyone who may have found it has decided either to keep it for personal use or to sell for profit. If the finder is of this mindset, and considering that personal information stored on the laptop could be accessed if the password protections were bypassed, I believe there is a real risk of significant harm to the affected 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 contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Employment information	

(e.g. salary) could also be used to cause hurt, humiliation or embarrassment. These are all significant harms.

The likelihood of harm resulting from this incident is decreased because the breach did not result from malicious action, but rather the laptop was likely left on the plane. However, the laptop has not been recovered and is protected only by a logon password, and not encrypted. The fact that the laptop has not been turned in suggests a real possibility that anyone who may have found it has decided either to keep it for personal use or to sell for profit. If the finder is of this mindset, and considering that personal information stored on the laptop could be accessed if the password protections were bypassed, I believe there is a real risk of significant harm to the affected 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 the Organization notified affected individuals by letter and email on October 7, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner