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-331 (File #022759)
Date notice received by OIPC	August 10, 2021
Date Organization last provided information	August 10, 2021
Date of decision	March 9, 2022
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 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 headquartered in Mississauga, Ontario, and 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, • telephone number, • mailing address, • email address, and • bank account 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. I note the Organization reported that "By and large the information was business contact information." Business contact information is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e-mail address, business fax number and other similar business information".

	Section 4(3)(d) of PIPA says that the Act does not apply to "the collection, use or disclosure of an individual's business contact information if the collection, use or disclosure, as the case may be, is for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose". In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business and for no other purpose." As such, the information is not excluded from the Act and PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 28, 2021, the Organization was the subject of a ransomware attack. The Organization's IT department discovered the incident that day "when the encryptor was executed across systems." • An investigation determined that the initial compromise likely occurred in early February and may have been related to a phishing / spear-phishing campaign. • The Organization could not rule out the possibility that data was exfiltrated during the attack.
Affected individuals	The incident affected 187 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement. • Involved external cybersecurity and incident response firms. • Implemented multi / two-factor authentication. • Enhanced backup procedures. • Removed "service accounts". • Implemented staff training about phishing. • Hired additional security expertise. • Provided credit monitoring services to some affected individuals. • Engaged a vendor to conduct dark web monitoring.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail or email on March 13, 2021 and August 10, 2021.

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 related to this attack relate primiarily [sic] to phishing (using the email and other contact information to impersonate the individual in dealings with other companies, for example).* In my view, a reasonable person would consider the contact and financial 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 affected individuals' vulnerability to fraud and identity theft. 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: *The sensitivity of the information is low and it was scattered across many systems, files, and folders. Any person wishing to obtain the information would need to have engaged in an extensive data minining/forensic [sic] exercise. It was also not entirely clear from the investigation which information was in fact exfiltrated, if any. The risk of harm to Albertans cannot be entirely excluded but is low given the information at issue.* *The forensic investigation found no conclusive evidence of data exfiltration or access but this could not be entirely ruled out.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (phishing, ransomware). Further, the Organization could not rule out the possibility that data was exfiltrated.
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 and financial 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 affected individuals' vulnerability to fraud and identity theft. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (phishing, ransomware). Further, the Organization could not rule out the possibility that data was exfiltrated.	

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 mail or email on March 13, 2021 and August 10, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner