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	MNP LLP and related subsidiaries and affiliates (Organization)
Decision number (file number)	P2020-ND-099 (File #015676)
Date notice received by OIPC	April 14, 2020
Date Organization last provided information	July 10, 2020
Date of decision	September 3, 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 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 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, • Social Insurance Number, and • historical tax information. 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 April 5, 2020, the Organization found its systems were encrypted as a result of a cybersecurity incident.

	• The Organization immediately shut down access to its systems and engaged external experts to work alongside its internal IT response team. • The Organization reported that the incident occurred as a result of a phishing email and involved only a small subset of information that was potentially accessed by the attacker. Further, there is no evidence of any data theft or exfiltration.
Affected individuals	The incident affected 1,813 Canadians of which 19 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Engaged cybersecurity experts to investigate the incident and assist with containment. • Shut down access to and quarantined all systems across the firm, including laptops, email and phone systems and effected a mandatory firm-wide password reset. • Recovered systems individually, tested them and provided a clean bill of health prior to being brought back online. • Offered complimentary credit monitoring for one year to all affected individuals. • Reported the incident to privacy commissioners' offices, and to law enforcement. • Leveraging artificial intelligence to assist with ongoing monitoring. • Continuing to look for opportunities to add layers of security within its ecosystem, be vigilant about the security of its environment and the protection of data.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on May 29, 2020.
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 that, although it is "… not aware of any misuse of the information, the potential harm that may occur as a result of the breach includes financial fraud and identify theft". I agree with the Organization's assessment. A reasonable person would consider the contact, identity and financial 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	The Organization reported: *Given that the incident involved only a small subset of information that was potentially accessed by the attacker and the fact that there is no evidence of any data theft or*

cause and effect relationship between the incident and the possible harm.	*exfiltration…the likelihood that the harm will result is low to medium.* 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 the malicious action of an unknown third party (phishing, encryption). The Organization cannot rule out the possibility that the unknown third party exfiltrated personal information. The lack of reported incidents of harm to date is not a mitigating factor as identity theft and fraud can occur months and even years after a data breach.

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 and financial 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 personal information was compromised due to the malicious action of an unknown third party (phishing, encryption). The Organization cannot rule out the possibility that the unknown third party exfiltrated personal information. The lack of reported incidents of harm to date is not a mitigating factor as identity theft and fraud can occur months and even years after a data breach.

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 on May 29, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner