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	A.K. Ross Professional Corporation (Organization)
Decision number (file number)	P2021-ND-234 (File #018954)
Date notice received by OIPC	January 12, 2021
Date Organization last provided information	January 12, 2021
Date of decision	November 22, 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 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 operates in Alberta and 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: • name, • address, • social insurance number, and • income tax related 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 June 3, 2019, the Organization's internet service provider upgraded its modem to a newer model; however, the new modem was not set up with the same privacy settings as the old modem. • On February 19, 2020, the Organization was notified by one of its clients that a tax document from 2015 stored on the back-up

	drive at the Organization's office had been accessed by his bank's security department. • Upon review of the drive, it was determined that files belonging to the client and his family had been removed, but no other client files were missing. • A forensic investigation to determine the scope of the data potentially accessed and the extent of the potential compromise was inconclusive. • The Organization reported there was no malware or ransomware detected on the computer and there is no evidence that personal information other than those relating to the client and his family were actually removed from the back-up drive.
Affected individuals	The incident affected 190 individuals.
Steps taken to reduce risk of harm to individuals	• Immediately turned off the drive within an hour or so of being advised of the vulnerability. • Tested and corrected the modem's settings and a subsequent testing revealed no ability to breach the modem's firewall. • Offered credit monitoring and identity theft protection. • Coordinated future upgrades with the Organization's IT company. • Initiated a forensic investigation to determine the scope of the data at issue and the extent of the potential compromise.
Steps taken to notify individuals of the incident	Some affected individuals were sent a preliminary email communication on February 22, 2020. All affected individuals were notified by email between December 14-22, 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, "A breach of the individual's name, address and SIN could result in identity theft, fraud and financial loss." I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and tax information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.
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	The Organization reported, *We are of the view that the likelihood that harm could result is moderate. There is only proof that the three directly affected individuals had their tax folders and all of their contents removed from the NAS unit… there is no positive evidence that an unauthorized third party did or*

between the incident and the possible harm.	*did not view, read, copy or download the affected individual's personal information that was stored on my computer drive. While the vulnerability apparently was in existence for 8.5 months, there does not appear to have been any other access to my NAS unit other than as described above. There was no malware or ransomware installed on the computer before or during this incident.* In my view, a reasonable person would consider that the likelihood of significant harm resulting from this incident is decreased because the breach did not result from malicious intent. However, the information was accessed by at east one unauthorized party, and was potentially exposed for eight and a half (8 ½) months. The Organization cannot confirm definitively that the personal information stored on the drive was not further accessed, used or disseminated.

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 tax information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of significant harm resulting from this incident is decreased because the breach did not result from malicious intent. However, the information was accessed by at east one unauthorized party, and was potentially exposed for eight and a half (8 ½) months. The Organization cannot confirm definitively that the personal information stored on the drive was not further accessed, used or disseminated.

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 that some affected individuals were sent a preliminary email communication on February 22, 2020 and all affected individuals were notified by email between December 14-22, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner