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	Ebbs, Roberts, Head & Daw Inc. (Organization)
Decision number (file number)	P2018-ND-132 (File #009751)
Date notice received by OIPC	September 17, 2018
Date Organization last provided information	September 17, 2018
Date of decision	September 27, 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 individuals whose 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 located in New Mexico, USA, and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved the following information: • name, • date of birth, • telephone number, • address, • social security number, • financial account information, and • bank account information including account number and routing information. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or about July 27, 2018, the Organization discovered that a data security incident may have affected some of its files, which included personal information. • Based on its investigation, the Organization believes a phishing attack may have been the cause of a compromise to its information systems resulting in access to personal information. • The breach was discovered July 27, 2018 when clients notified the Organization "that fraudulent tax return was [sic] filed in their name."
Affected individuals	The incident affected 4,200 individuals, including one Canadian resident.
Steps taken to reduce risk of harm to individuals	• Conducted investigation with third party law firm to determine affected parties and personal information. • Reported to the Internal Revenue Service, and updated account information with the IRS and the Organization's third party vendor. • Updated anti-virus software and full scans of system to eliminate any viruses. • Updated policies and procedures related to data security and breaches. • Provided training for employees on data security and breaches. • Offered credit monitoring service to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent September 18, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "Personal information could be used for fraudlent [sic] reasons, including to file fraudulent tax returns." In my view, a reasonable person would consider that 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 cause and effect relationship between the incident and the possible harm.	In assessing the likelihood of harm resulting from this breach, the Organization reported "Low risk". In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing) and it appears the personal information may have been used to file fraudulent tax returns.

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 as a result of this incident. A reasonable person would consider that 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 as the breach was the result of malicious intent (phishing) and it appears the personal information may have been used to file fraudulent tax returns. I require the Organization to notify any affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that affected individuals were notified by letter sent September 18, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner