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	Moore Stephens Tiller, LLC (Organization)
Decision number (file number)	P2018-ND-102 (File #009339)
Date notice received by OIPC	July 30, 2018
Date Organization last provided information	July 30, 2018
Date of decision	August 7, 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 the individuals 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported "The types of PII relating to Alberta residents determined to be stored within the impacted email account were not identical for every potentially affected individual, and they included the following: name, Social Security 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.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On or around April 9, 2018, the Organization became aware of suspicious activity relating to an employee's email account, possibly related to a malicious phishing email. • The Organization investigated, and determined that an unknown individual accessed the email account of an employee on April 6 and April 9, 2018.

	• The investigation was unable to determine which email messages may have been seen or taken by the unauthorized individual.
Affected individuals	The incident affected two (2) residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reset email login credentials for all employee email accounts to prevent further unauthorized access. • Blocked the website associated with the malicious phishing email, and notified all employees to delete suspicious emails. • Implemented multi-factor authentication on all employee email accounts, and currently implementing additional training and education for employees to prevent similar future incidents. • Offering affected individuals complimentary access to one year of free credit monitoring and identity restoration services. • Providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact authorities and report any attempted or actual identity theft and fraud. • Will notify other state regulators.
Steps taken to notify individuals of the incident	On July 23, 2018, the Organization began mailing written notice of the incident to potentially impacted individuals.
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 it "is providing potentially affected individuals with information on how to protect against identity theft and fraud". In my view, a reasonable person would consider that the identity 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.	The Organization did not specifically address the likelihood of harm resulting from this incident, but, as noted above, "is providing potentially affected individuals with information on how to protect against identity theft and fraud". In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to a suspected malicious phishing email. The information was subject to unauthorized access on two separate occasions. The Organization has been unable to determine which email messages may have been seen or taken by the unauthorized individual.

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 identity 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 a suspected malicious phishing email. The information was subject to unauthorized access on two separate occasions. The Organization has been unable to determine which email messages may have been seen or taken by the unauthorized individual. I require the Organization to notify the affected individuals whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that on July 23, 2018, the Organization began mailing written notice of the incident to potentially impacted individuals. The Organization is not required to notify the affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner