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	Lorne Steinberg Wealth Management Inc. (Organization)
Decision number (file number)	P2020-ND-062 (File # 014856)
Date notice received by OIPC	January 30, 2020
Date Organization last provided information	January 30, 2020
Date of decision	June 5, 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 for 4 individuals: • name, • date of birth, • email address, • social insurance number, and • banking information (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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• In late November 2019, the Organization and forensic IT experts identified suspicious activity with respect to two email accounts. • The Organization determined that an unknown external actor gained access to the email accounts in late September 2019 and appeared to have forwarded emails from these accounts to illegitimate email accounts for the purpose of attempting wire fraud. • The Organization does not currently have any evidence that the external actor was successful in its wire fraud attempts.
Affected individuals	The incident affected 25 individuals, of which 4 were Alberta residents.
Steps taken to reduce risk of harm to individuals	• Investigated and implemented an incident response plan. • Reviewed all email in the email accounts to determine what personal information was affected. • Advised affected individuals that their account number could be changed at their request and offered identity theft and credit monitoring services for one (1) year. • Conducting a review of security and cybersecurity measures to improve security safeguards and ensure adequate measures to respond to potential breaches of personal information.
Steps taken to notify individuals of the incident	Affected individuals were notified verbally on January 14 and January 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 … *…since the information of … Clients located in Alberta involved in the Incident includes financial and contact / identification information, there are potential risks of identity theft, fraud and financial loss for part of the individuals affected….In addition, given that the information of the …Clients located in Alberta involved email addresses, there is the potential risk of phishing.* 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, fraud, and financial loss. Email address could be used for phishing, increasing vulnerability to 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 reported that … *… the likelihood that harm could result to the …Clients located in Alberta is moderate. While [the Organization] has no evidence that the personal information at issue has been misused by the external actor in any way and has reasons to believe that the unknown actor was attempting wire fraud, the personal information involved in the Incident is nonetheless sensitive and could be used for the purposes of identity theft and fraud, and certain of the personal information could be used for the purposes of phishing. The fact that the Incident was caused as a result of the actions of an unknown actor with malicious intent additionally increases the likelihood that harm could result to the affected individuals.* 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 (deliberate intrusion). Although the Organization reported that it has no evidence that the personal information at issue has been misused nor that the wire fraud attempts were successful, 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, fraud, and financial loss. Email address could be used for phishing, increasing vulnerability to 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 (deliberate intrusion). Although the Organization reported that it has no evidence that the personal information at issue has been misused nor that the wire fraud attempts were successful, 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 verbally on January 14 and 29, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner