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	Quarry Wealth Management Ltd./ Raintree Financial Solutions (Organization)
Decision number (file number)	P2019-ND-063 (File #003549)
Date notice received by OIPC	August 12, 2016
Date Organization last provided information	August 12, 2016
Date of decision	May 3, 2019
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 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"	Depending on the extent of the access, the incident may have involved some or all of the following types of information: • name, • address, • telephone number, • email address, • date of birth, • social insurance number, • banking information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On July 4, 2016, the Organization realized an employee's email account had been breached, resulting in a phishing email sent to email addresses in the employee's Outlook contacts. • In addition a rule was set up in the Outlook account, which redirected all incoming emails to the deleted items folder. • The incident is believed to have resulted when the employee clicked on a phishing email on November 20, 2015. As a result, the Organization suspects the intrusion was unnoticed for 7 months. • The incident was discovered when the employee received a telephone call from one of the recipients of the phishing email sent from the compromised account.
Affected individuals	The Organization did not report the total number of potentially affected individuals.
Steps taken to reduce risk of harm to individuals	• Assisted 2 clients to remove the virus. • Removed the computer from the network and replaced it with a new one. • Searched all computers and the server and found them to be free of the virus. • Changed all passwords.
Steps taken to notify individuals of the incident	The Organization reported that all clients in its database were notified by email within a few hours of the discovery of the breach.
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 did not specifically identify the potential harms that might result from the incident, but did report "Our IT professinoal [sic] believes that the email addresses of clients was the most sensitive information lost to the hacker. Address and phone numbers may have been obtained but these are widely available in the public domain". The Organization also reported that some clients received a phishing email, purportedly from the Organization. In my view, a reasonable person would consider that contact, identity and financial information, if accessed, could be used to cause the significant harms of fraud and identity theft. Email addresses could be used for phishing purposes, 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 "We do not believe any significant harm will result from this phishing event". Further, the Organization said "Our IT contractor carefully checked our server and found no evidence of intrusion, the only corruption was found on the one computer…Our clients only reported two instances of opening the corrupted document and our IT professional assisted both clients in removing the virus". In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and unauthorized third party). The harm (in the form of phishing emails) has already occurred. The incident was not noticed for 7 months.

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 contact, identity and financial information, if accessed, could be used to cause the significant harms of fraud and identity theft. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and unauthorized third party). The harm (in the form of phishing emails) has already occurred. The incident was not noticed for 7 months.

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 all clients in the Organization's database were notified by email within a few hours of the discovery of the breach. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner