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	RGF Integrated Wealth Management Ltd. (Organization)
Decision number (file number)	P2019-ND-099 (File #012492)
Date notice received by OIPC	March 15, 2019
Date Organization last provided information	March 15, 2019
Date of decision	July 16, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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 Organization reported: *The information of Alberta residents that was involved falls into two categories.* *Category 1 - Individuals for whom an email address was contained within Advisor's 0365 Exchange online account (6 impacted individuals)* *Category 2 - Individuals who had email address and personal information contained within the Advisor's 0365 Exchange online account. The extent of information varies by individual however it may have contained name, address, telephone number, financial account information and tax information and content that would be typical in email exchanges between a Financial Advisor and their Client (7 impacted indivudals) [sic].* 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 February 7, 2019, the Organization discovered that an Advisor's online account credentials had been compromised, resulting in unauthorized access to their email account. • As a result, phishing emails (which appeared to come from the Advisor) were sent to 8 Alberta residents. The emails included links which ultimately, requested the recipient to enter their email credentials. • The unauthorized user may have been able to access the contents of the Advisor's email account. The email account contained information dating back to April 18, 2018. • A third party forensic audit determined that the Advisor received a phishing email containing a malicious URL link in December 2018, and the user had accessed the link in December 2018. No malware or software of any kind was uploaded to the desktop that was used to access the suspicious link. No further activity was identified on the account until early February 2019, when the phishing emails were sent. • The incident was discovered when an individual who had received the phishing email informed the Organization.
Affected individuals	The incident affected 13 individuals.
Steps taken to reduce risk of harm to individuals	• Changed impacted account credentials, and for all user accounts. • Notified recipients of the phishing emails • Blocked IP address of the unauthorized user and commenced an investigation with a third party auditor. • Enhanced security. • Offered free identity theft and monitoring services. • Mandatory training for all staff. • Reported to data protection and industry regulatory authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by email, letter and telephone between February 7 and 13, 2019.
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	The Organization reported: *Category 1- The email addresses can be used for phishing which could potentially be at risk of identifty [sic] theft and/or fraud.* *Category 2 - If an unauthorized user uses the personal and*

non-trivial consequences or effects.	*financial information contained within the Advisor's email, there is risk of identity theft and/or fraud. In addition, as some of the information contained salary, financial and/or tax information, there is a risk of hurt, humiliation and/or embarassement [sic].* I agree with the Organization's assessment. A reasonable person would consider that contact and financial information 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: *The risk assessment is based on the extent of personal and financial information impacted and the fact that the incident resulted from a malicious attack on the Advisor's 0365 exchange online account.* *Category 1 - If a phishing attempt is successful, Significant Risk* *Category 2 - If the personal information contained within the Advisor's 0365 account is inappropriately disclosed or used, Real risk [sic] of Significant Harm* 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) and additional phishing emails were sent. The information has not been recovered.

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 and financial information 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) and additional phishing emails were sent. The information has not been recovered.

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 individuals were notified by email, letter and telephone between February 7 and 13, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner