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	Westward Advisors Ltd. (Organization)
Decision number (file number)	P2020-ND-081 (File #014914)
Date notice received by OIPC	January 15, 2020
Date Organization last provided information	January 15, 2020
Date of decision	July 24, 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 the 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 located in British Columbia and 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: • name, • address, • telephone number, • email address, • personal financial information (including income and net worth, investment details, banking information, and tax returns), and • medical information. 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 November 25th, 2019, a "spear phishing" email was sent to some of the Organization's email addresses. • One employee clicked on an attachment that installed a rule in the Employee's Outlook account. As a result, the attacker collected a copy of certain emails addressed to the employee between November 25-December 31, 2019. • The attacker also created a similar but fake email address for the employee and contacted some of the Organization's clients while impersonating the employee and attempting to redirect premium payments via wire transfer to an offshore bank account. • The cyberattack was discovered On January 2, 2020, and the Organization identified the source and immediately closed it. • The Organization confirmed that the attacker did not gain access to any systems or user accounts. • A total of 264 emails were leaked. • The attacker still holds the breached information.
Affected individuals	The incident affected 29 individuals, including 4 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged external legal counsel. • Directed Security Officer to identify the source of the breach and identified leaked emails. Determined that the attacker has not penetrated any of its systems or gained access to any user accounts. • Notified all employees of the cyberattack and precautions to take going forward. • Notified affected individuals and cautioned them to be on heightened awareness for identity theft and fraudulent communications from the attacker posing as a trusted advisor. • Notified affected life insurance companies, provincial and federal privacy commissioners of the attack, and law enforcement. • Increasing staff training including third party Security Awareness Training courses. • Implementing Azure active directory premium subscription. • Blocking mail forwarding rules to external addresses. • Prohibiting copying outbound mail messages to oneself. • Considering secure email enhancements.
Steps taken to notify individuals of the incident	The affected individuals in Alberta were notified by letter from January 8 to January 13, 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: *The leaked information poses a risk of financial loss if the attacker successfully poses as a trusted individual to fraudulently obtain payments.* *The leaked information poses a risk of identity theft if it contains sufficient personal identifying information such as names, addresses, social insurance numbers, driver license numbers, bank account numbers, etc.* *The leaked information may pose some risk of reputational harm or embarrassment if it contains medical or health information, although the likelihood of medical information disclosure is low and medical information was not the attacker's target and so unlikely to be misused.* I agree with the Organization's assessment. A reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft, fraud and/or financial loss. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Medical information could be used to cause the harms of humiliation and embarrassment. These are all significant harms.
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 provide an assessment of the likelihood that significant harm would result from this incident. The Organization did report that "the likelihood of medical information disclosure is low and medical information was not the attacker's target and so unlikely to be misused." In addition, the Organization's notification letter to affected individuals included measures to minimize the risk of harm. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (spear phishing email) by an unknown third party and it appears the personal information may have been used to send emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized party viewed, read, copied, or downloaded the affected individuals' personal information. In addition, the personal information remains in the hands of the unauthorized party.

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 contact and financial information at issue could be used to cause the harms of identity theft, fraud and/or financial loss. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. Medical information could be used to cause the harms of humiliation and embarrassment. These are all significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (spear phishing email) by an unknown third party and it appears the personal information may have been used to send emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized party viewed, read, copied, or downloaded the affected individuals' personal information. In addition, the personal information remains in the hands of the unauthorized party. 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 the affected individuals by letter sent between January 8 -13, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner