



**PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision**

Organization providing notice under section 34.1 of PIPA	AMA Agencies Ltd. o/a AMA Insurance Agency (Organization)
Decision number (file number)	P2022-ND-011 (File #021155)
Date notice received by OIPC	November 29, 2021
Date Organization last provided information	November 29, 2021
Date of decision	March 27, 2022
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 <i>Personal Information Protection Act</i> (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”	<p>The incident involved some or all of the following information:</p> <ul style="list-style-type: none">• customer name,• insurance policy numbers,• type of insurance,• premiums charged, and• expiry date of policies. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On April 2, 2021, two employees with the Organization were subject of a phishing attack. The employees received an email from a threat actor impersonating one of the Organization’s vendors, Premier Marine (Premier Group).• The email was sent by (staff name)@PrennierGroup.com (the correct domain name of the vendor is premiergroup.com).

	<ul style="list-style-type: none"> • The staff at Premier Group is a regular contact at Premier Group that handles issues related to account payment discrepancies. • The email requested the Organization switch from physical cheque payments to electronic fund transfer (EFT) to address outstanding invoices. • The email also asked for an update on the status of payments of outstanding invoices. • Both employees separately replied by email to the threat actor that the Organization had already set up EFT payments with Premier Group. • The employees sent documents containing the personal information of customers to the threat actor to substantiate that all invoices had been paid. • The Organization reported that “Not all customer information were individuals, as some information pertained to corporate clients”. • On May 4, 2021, the employees noticed the misspelled domain and reported the threat. • Premier Marine subsequently indicated that the email account (staff name)@premiergroup.com "has been compromised", which would be why the phishing attack appeared credible.
Affected individuals	The incident affected approximately 125 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Notified affected individuals. • Changed the policy file numbers with the Organizations and Premier Marine. • Employees involved in the breach to retake the available corporate privacy policy, fraud course and phishing course. • In the process of restricting the allowable information to be sent out by its finance team. • Activated a warning header system if an email comes in from an external source.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and email on May 14, 2021.
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: <i>The information could be used to contact affected individuals under the guise of being from Premier Marine or AMA Insurance Agency. Or the information could be used by someone contacting AMA Insurance Agency posing as the affected individual.</i>

<p>non-trivial consequences or effects.</p>	<p>In my view, a reasonable person would consider that the identity and insurance information at issue could be used to cause the harms of identity theft and fraud. These are significant harms.</p>
<p>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.</p>	<p>The Organization reported,</p> <p><i>Real risk of significant [sic] harm is unlikely as the information that was disclosed such as insurance policy number can only be used for something related to the insurance policy. Subsequent to this breach, the information is not usable [sic] at all as the policy numbers are being changed and AMA Insurance Agency, Premier Marine and the affected parties are aware and more cautious in any communications regarding these policies.</i></p> <p>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 into an employees' email account). The Organization confirmed that there was an unauthorized access to personal information.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>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.</p> <p>A reasonable person would consider that the identity and insurance information at issue could be used to cause the harms of identity theft and fraud. These are significant harms.</p> <p>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 into an employees' email account). The Organization confirmed that there was an unauthorized access to personal information.</p> <p>I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the affected individuals were notified by email on May 14, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.</p>	

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance