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	The Portage la Prairie Mutual Insurance Company (Organization)
Decision number (file number)	P2021-ND-286 (File #012916)
Date notice received by OIPC	April 3, 2019
Date Organization last provided information	October 17, 2019
Date of decision	February 23, 2022
Summary of decision	Section 34.1(1) of PIPA states "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure." [my emphasis] The Organization initially provided a notice of the breach to my office "as a courtesy", saying that it "...does not accept that the privacy breach reporting provisions of the Personal Information Protection Act, 2003 C. P-6.5 are applicable in this matter". The Organization later clarified its position that "...there was not a real risk of significant harm to the two Albertans, given the non-sensitive nature of the information and the message that was communicated to them." The Organization provided additional information about the breach on October 17, 2019. In my view, a reasonable person would consider there is a real risk of significant harm to the individuals affected by this incident, thereby triggering the Organization's duty to provide notice to me under section 34.1(1). 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 the following information about two Alberta residents: • name, • address, • telephone number, • personal email address, and • information relating to the cost of property repairs in connection with an insurance claim. 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 December 6 and 7, 2018, the Organization learned two of its employee email accounts were accessed by an unauthorized individual and used to send a number of phishing messages. • The cause of the incident was determined to be phishing emails that had been sent to the two employees.
Affected individuals	The incident affected 14 Canadians, including 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• secured the affected accounts, • notified all recipients of the unauthorized messages, • commenced an investigation into the incident with the assistance of outside cybersecurity experts, • forced all users to reset their password, • disabled webmail for all but five users, • required multi-factor authentication for users for whom webmail is enabled, • limiting webmail access only to IP addresses within Canada and the USA, • implemented protocols to trigger alerts when there are potentially suspicious logins to employee email accounts, • added a "phish" alarm button to Outlook so users can have central IT support review any questionable emails prior to opening, • disabled email protocols that are not specifically required, • reported the incident to the Office of the Privacy Commissioner of Canada and the Office of the Superintendent of Financial Institutions.

Steps taken to notify individuals of the incident	Affected individuals were notified of the incident by email on December 15, 2018.
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 it "...considers that, under the Personal Information Protection Act in Alberta, there is no harm to the two Alberta residents that arises from this incident given the nature of the information that was affected." In my view, a reasonable person would consider that the contact and insurance information, particularly in conjunction with email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are 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 reported that "...there was not a real risk of significant harm to the two Albertans, given the non-sensitive nature of the information and the message that was communicated to them." In my view, a reasonable person would consider that the likelihood of significant harm resulting from this incident is increased because it resulted from malicious intent (deliberate action, phishing) and additional phishing emails were sent as a result.
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 insurance information, particularly in conjunction with email addresses, could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of significant harm resulting from this incident is increased because it resulted from malicious intent (deliberate action, phishing) and additional phishing emails were sent as a result. 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 that all affected individuals were notified of the incident by email on December 15, 2018. The Organization is not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner