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	Northbridge General Insurance Corporation (Organization)
Decision number (file number)	P2018-ND-090 (File #008942)
Date notice received by OIPC	June 13, 2018
Date Organization last provided information	June 13, 2018
Date of decision	July 27, 2018
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 in Alberta 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported that the breach was limited to information in electronic form only, namely emails received and sent by an employee, and attachments to the employee's emails. It identified several categories of information involved, reporting the following: *The personal information involved in the breach consisted of social insurance numbers, dates of birth, home contact information, work contact information, payroll information, personal net worth statements, income tax information, bank information, and driver's license information.* *The type of personal information involved in the breach was not the same for all individuals.* This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 6, 2018, an employee in the Organization's Toronto office received a phishing email from a known and trusted business partner whose system had been exploited by an outside party. • The phishing email convinced the employee to provide his email login credentials, which resulted in the outside party gaining unauthorized access to the employee's email account. • The outside party used access to the employee's email account to send phishing emails to the contacts in the employee's address book. During the period the outside party had access to the employee's email account, they had the ability to access the emails in the employee's email account which consisted of correspondence with business partners and business customers. • Further investigation subsequently uncovered mail forwarding rules in the employee's email account on March 12. • The Organization has not found any evidence that the outside party reviewed, read, or downloaded emails from the compromised email account. • The Organization became aware of the issue on March 7, 2018 when the employee started to receive emails from his contacts asking if he had sent the unauthorized emails.
Affected individuals	A total of 1,127 individuals across Canada were affected, including 100 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately changed account credentials and the laptop quarantined and examined for malware. • Developed and executed a communications plan to raise internal awareness of phishing incidents. • Communicated with the originating partner that sent the email as well as the parties that received emails and all of the Organization's users. • Online learning modules for security and the information security policy. • Provided short awareness sessions at Town Hall sessions and in the major offices across the country. • Engaging a third party to provide malware and phishing training sessions online at the employee's desk. • Engaging a third party to perform phishing campaigns against the Organization to test awareness and employee understanding of the threat. • Offered affected individuals one year of credit monitoring and fraud alert services and provided them with contact information for obtaining further information, as well as contact information for Canadian privacy regulators.

Steps taken to notify individuals of the incident	• On March 14, 2018, sent an email to all of the persons in the employee's email address book notifying them that an unauthorized email had been sent from the employee's account and advising them to delete the email. • From May 7 to May 11, notified the insurance broker for each affected individual by telephone, followed by a written notification. • On May 17, 2018, mailed notification letters directly to the affected individuals.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "The type of harm that could result from the breach is fraud and identity theft, and financial loss resulting therefrom. Depending on how much information we held on an individual, it is possible that an outside party extracting that information could attempt to assume the identity of the individual for the purpose of fraudulent activity". The Organization also said "We regard the social insurance numbers, payroll information, personal net worth statements, income tax information, bank information, and driver's license information as being more sensitive, owing to the fact that if accessed, it could be used to assume the identity of an individual for the purpose of fraudulent activity. We regard the home and work contact information, and date of birth information to be less sensitive than the foregoing information." Finally, the Organization reported "We are unable to confirm that data was extracted in this breach, and as a result, are unable to confirm that there has been actual loss. However, we are not able to rule out the possibility that data could have been extracted. Accordingly, to the extent that an outside party could have extracted the information and used it to effect identity theft or fraud, it is our assessment that there a real risk of significant harm." Overall, I agree with the Organization's assessment. The comprehensive contact, identity (including social insurance numbers, driver's license numbers, and date of birth), financial and employment information at issue could be used to cause the significant harms of identity theft, fraud and phishing.
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 provided a thorough and comprehensive assessment of risk, reporting in part: *There is no evidence that [the Organization] has … that the outside party reviewed, read, or downloaded emails from the compromised account. …* *That Information was exposed for up to 15 hours. The information was not lost or contaminated and [the*

	Organization] has backups of this data. *We are unable to confirm that data was extracted in this breach, and as a result, are unable to confirm that there has been actual loss. However, we are not able to rule out the possibility that data could have been extracted. Accordingly, to the extent that an outside party could have extracted the information and used it to effect identity theft or fraud, it is our assessment that there a real risk of significant harm.* I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (social engineering and compromised credentials, generation of phishing emails), the length of exposure (up to 15 hours), the Organization cannot rule out the possibility that data could have been extracted, and a relatively large number of individuals were affected.

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 as a result of this incident.

The comprehensive contact, identity (including social insurance numbers, driver's license numbers, and date of birth), financial and employment information at issue could be used to cause the significant harms of identity theft, fraud and phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (social engineering and compromised credentials, generation of phishing emails), the length of exposure (up to 15 hours), the Organization cannot rule out the possibility that data could have been extracted, and a relatively large number of individuals were affected.

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that on May 17, 2018, the Organization mailed notification letters directly to the affected individuals. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner