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 and Federated Insurance Company of Canada (Organization)
Decision number (file number)	P2018-ND-127 (File #009650)
Date notice received by OIPC	September 6, 2018
Date Organization last provided information	September 6, 2018
Date of decision	September 26, 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 information at issue was stored in an employee's emails and consisted of: • credit card numbers, • bank account numbers, • contact information, and • insurance premium 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. PIPA applies to the extent the personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 25, 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 her email login credentials, which resulted in the outside party gaining unauthorized access to the employee's email account on June 12, 2018. • Once the outside party gained unauthorized access, they changed the employee's email configuration to hide the outside party's activity, and synchronized the employee's email with a remote computer. • The outside party used their 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 email account, they had the ability to access the emails in the employee's email account. • The Organization has not found any evidence that the unauthorized party reviewed, read, or downloaded emails from the compromised email account. No parts of the Organization's systems or business were affected by the breach other than the employee's email account. • The breach occurred from June 12, 2018 to June 13, 2018. The incident was discovered on June 13, 2018.
Affected individuals	The incident affected 92 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Changed the employee's account credentials. • Quarantined and examined the laptop for malware. No malware was discovered. • Notified the sender of the phishing email so that they could detect the compromise and remediate it in their environment. • Notified the 134 individuals who were in the employee's address book and who received phishing emails. • Offered credit monitoring and fraud alert services to affected individuals whose credit card numbers or bank account numbers were exposed. • Notified the Organization's credit card processor. • Provided notification of the breach and guidance as to how to guard against a pretexting call to affected individuals whose contact information and insurance premium information alone were exposed. • Updated plan to increase employee awareness of phishing, and reduce the risk of breach, including implementation of multi-factor authentication.
Steps taken to notify individuals of the incident	• On June 15, 2018, an email was sent 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.

	• Notified insurance brokers for the affected individuals by telephone during the week of August 6, 2018, and in writing the following week. • During the weeks of August 13 and 20, 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 may result from the breach is identity theft and financial fraud. Where an individual's credit card number or bank account number combined with contact information was exposed, 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. Where an individual's credit card number or bank account number alone was exposed, it is possible that an outside party may use these numbers to make fraudulent financial transactions. Finally, it is also possible, though unlikely, that where an individual's insurance premium information and contact information was exposed, an outside party may use the information to contact the individual on the pretext of being [the Organization] and attempt to obtain further personal information from the individual." I agree with the Organization's assessment. The financial and contact information at issue could be used to cause the significant harms of identity theft, fraud and pretexting (social engineering).
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 "There is no evidence that the outside party reviewed, read, or downloaded emails from the compromised account" but also "There were then a number of connections to install …mail rules to hide the attackers actions." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (social engineering, compromised credentials, and efforts to hide the attackers actions). The Organization cannot rule out the possibility that data could have been reviewed, read, or downloaded.
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 financial and contact information at issue could be used to cause the significant harms of identity theft, fraud and pretexting (social engineering). The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (social engineering, compromised credentials, and efforts to hide the attacker's actions). The Organization cannot rule out the possibility that data could have been reviewed, read, or downloaded.	

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 affected individuals were notified by email, telephone and in writing between June 15, 2018 and August 20, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner