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 Guarantee Company of North America (Organization)
Decision number (file number)	P2019-ND-163 (File #013318)
Date notice received by OIPC	May 28, 2019
Date Organization last provided information	May 28, 2019
Date of decision	November 20, 2019
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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in the incident: • name, • home address, • email address, • social insurance number and/or driver's license number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization learned that on February 27, 2019, one of its employee email accounts was accessed by an unauthorized individual and used to send phishing emails from the account.

	• The incident affected one email account, which was accessed for approximately five hours on February 27, 2019. No other employee accounts were affected. • The cause of the incident was determined to be a phishing email that had been sent to the employee from a known and trusted business partner whose system had been apparently exploited by an unauthorized individual. Once the unauthorized individual gained access to the employee's account, they changed the employee's email configuration to conceal their activity, synchronized the employee's email with a remote computer, and used the employee's email account to send the above-mentioned phishing emails to contacts in the employee's address book. • The incident was identified when the unauthorized individual sent the phishing email from the employee's account.
Affected individuals	The incident affected 194 individuals in Canada (including 64 individuals in Alberta).
Steps taken to reduce risk of harm to individuals	• Reported the incident to the Office of the Superintendent of Financial Institutions. • Notified all recipients of the unauthorized messages, advising them to delete the message or seek assistance from their IT staff, if they opened the message and provided their credentials. • Secured the affected account, and commenced an investigation. • Disabled and preserved the email account and blocked the employee's access from all systems; changed the employee's email account password; mandated password changes for all employees; sourced all email log and audit trail activity; quarantined the employee's laptop; advised the Organization's cyber insurer of the incident and engaged legal counsel to guide the investigation process; notified the trusted business partner of the phishing email. • Offering credit monitoring, including ID theft insurance coverage, to affected individuals for up to three years at no cost and providing additional information about steps that the individuals can take to further protect themselves. • Accelerated the implementation of enhanced anti-virus and malware detection software and multi-factor authentication sign-in technology. • Supplemented ongoing information security and awareness training to focus on employee awareness of phishing. • Improved daily monitoring of email and system activity. • Disabled access to email via protocols such as IMAP & SMTP. • Optimized its email security service.

Steps taken to notify individuals of the incident	The Organization reported that it "will notify the 194 affected individuals (and their insurance brokers where applicable) by regular mail tomorrow, May 29, 2019."
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 affected information … could give rise to a real risk of significant harm (in the form of identity theft or fraud)…". In my view, a reasonable person would consider that identity information (social insurance, driver's license) could be used to cause the significant harms of identity theft and fraud. 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 did not specifically assess the likelihood of harm resulting from this incident, but reported that it "…has no evidence that the unauthorized individual who accessed the account has misused any of the information". The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party (phishing) and the personal information was used to send additional phishing emails.
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 identity information (social insurance, driver's license) could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent by an unknown third party (phishing) and the personal information was used to send additional phishing emails. 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 affected individuals by mail on May 29, 2019. The Organization is not required to notify affected individuals again.	

Jill Clayton
Information and Privacy Commissioner