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	Grant Thornton LLP (Organization)
Decision number (file number)	P2021-ND-158 (File #017984)
Date notice received by OIPC	November 12, 2020
Date Organization last provided information	July 8, 2021
Date of decision	August 25, 2021
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 is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported the incident involved some or all of the following information: • name, • contact information, and • social insurance number and/or date of birth. for a small portion of these individuals: • driver's license number, • passport number, • bank account number and/or credit card number. 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 April 30, 2020, the Organization learned that an unauthorized individual accessed one of its employee's email accounts. • The unauthorized individual sent phishing emails from the account to others at the Organization and later gained access to eight other employee email accounts. • The Organization reported that no other employee accounts were affected, nor were other parts of the Organization's system or business. • The Organization reported that it has no evidence that any information was accessed, or that the unauthorized individual was seeking personal information.
Affected individuals	The incident affected 4,296 individuals, including 108 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Activated Cybersecurity Incident Response Team. • Disabled all user accounts and reset all employee passwords (with very limited and verified exceptions). • Blocked access to a broad range of resources. • Blocked all emails meeting the characteristics of the phishing emails sent in this incident. • Blocked all IP addresses outside of Canada from accessing the environment. • Quarantined the computers of all affected employees. • Offered credit monitoring and ID theft insurance to affected individuals for one year at no cost. • Provided additional information about steps that individuals can take to further protect themselves. • Implementing other information security policies, solutions, and training.
Steps taken to notify individuals of the incident	The affected individuals were notified by email or mail on November 11, 2020 and by letter on or about March 24, 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 non-trivial consequences or effects.	In its letter to this office, the Organization did not specifically identify any harm that might result from this incident, but did report that it offered credit monitoring and ID theft insurance to affected individuals for one year at no cost, and provided additional information about steps that the individuals can take to further protect themselves. In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.

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 it… *… considers the risk of harm to individuals from this incident to be low based on the attacker's apparent motivation to harvest login credentials rather than collect personal information as well as the short compromise window for eight of the nine accounts compromised.* 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 employee's email account). The Organization said it "... has no evidence that the unauthorized individual who accessed the accounts has misused any of the information..."; however, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Although the Organization reported "...the attacker's apparent motivation to harvest login credentials rather than collect personal information as well as the short compromise window for eight of the nine accounts compromised," I do not find this to be reassuring. The Organization can only speculate as to the motives of the intruder.

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, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.

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 employee's email account). The Organization said it "... has no evidence that the unauthorized individual who accessed the accounts has misused any of the information..."; however, the lack of reported incidents resulting from this breach to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Although the Organization reported "...the attacker's apparent motivation to harvest login credentials rather than collect personal information as well as the short compromise window for eight of the nine accounts compromised," I do not find this to be reassuring. The Organization can only speculate as to the motives of the intruder.

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 the affected individuals by email or mail on November 11, 2020 and by letter on or about March 24, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner