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, LLC (Organization)
Decision number (file number)	P2022-ND-050 (File #022088)
Date notice received by OIPC	April 5, 2021
Date Organization last provided information	January 31, 2022
Date of decision	August 29, 2022
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 (address, email address, telephone number), • date of birth, • partner identification number, • social insurance number, • social security number, • certain tax documents or drafts of tax documents, • income information (salary, wage amount investment income, taxable benefits and expenses), • financial account numbers, • driver's license number, and/or • signature. 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	• On June 5, 2020, an employee's email account was accessed by an unauthorized individual. • The unauthorized individual then sent phishing emails from the account to others at the Organization. • The Organization secured the affected account, and immediately commenced an investigation with the assistance of third-party cybersecurity experts. • The Organization reported that no other employee accounts were affected. No other parts of the Organization's system or business were affected by the incident.
Affected individuals	The incident affected 675 individuals in Canada, which includes eight (8) individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Activated its Cybersecurity Incident Response Team. • Identified and deleted the phishing email from the system. • Blocked the IP address used to send the phishing emails. • Quarantined the affected account and changed the login credentials. • Disabled a legacy protocol that may have been used. • Checked for unauthorized access to the affected account. • Offered credit monitoring, including ID theft insurance coverage, to notified individuals for one year at no cost. • Provided information about steps individuals can take to further protect themselves. • Implemented additional security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter between March 25, 2021 and April 7, 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.	The Organization reported: *Although Grant Thornton has no evidence that the unauthorized individual who accessed the account has misused any of the information, Grant Thornton notified the 675 individuals by either email or physical mail.* *Grant Thornton is offering credit monitoring, including ID theft insurance coverage, to notified individuals for one year at no cost and providing 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 harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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: *Grant Thornton considers the risk of harm to individuals from this incident to be low based on the unauthorized individual's apparent motivation to harvest login credentials rather than collect personal information.* 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 confirmed that there was an unauthorized access to personal information. Additionally, the information may have been exposed for approximately 7 days.

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.

The contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

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 confirmed that there was an unauthorized access to personal information. Additionally, the information may have been exposed for approximately 7 days.

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 letter between March 25, 2021 and April 7, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner