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	Walton Global Holdings, Ltd. (Organization)
Decision number (file number)	P2021-ND-223 (File #018109)
Date notice received by OIPC	September 11, 2020
Date Organization last provided information	September 20, 2021
Date of decision	November 12, 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 those 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 incident involved all or some of the following information: • name, • address, • offers of employment, and • employment information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 4, 2020, a threat actor used a compromised Organizational email account to fraudulently request a large wire transfer. The employee(s) who received the wire transfer request sought verbal confirmation from the requestor. Upon doing so, it was discovered that the request was fraudulent. • The Organization's investigation determined that the threat actor had access to two email accounts between April 7 and May 20, 2020. The email accounts contained personal information which would have been accessible to the attacker. • It is reported that the email accounts were compromised by a phishing attack.
Affected individuals	The incident affected 3 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Retained an IT firm to conduct a forensic investigation. • Reviewed and audited IT environment, including security. • Implemented mandatory use of multi-factor authentication. • Enhanced threat detection, access logging, and alerting. • Implemented additional network access restrictions. • Implemented quarterly IT Security presentations. • Notified police. • Arranged identity theft protection and credit monitoring services for affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 15, 2020.
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 incident could result in the possible harm of "Identity theft." In my view, a reasonable person would consider the contact and employment information at issue could be used to cause the significant harms of identity theft or fraud.
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: *Notice of the incident has been provided to the indivdiuals [sic]. Given that the individuals have been notified, and will be monitioring [sic] the uses of their information, we believe there is a limited risk of harm.*

	In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (email account compromise, fraudulent money transfer request). Further, the threat actor had access to two of the Organization's email accounts for over 30 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.

A reasonable person would consider the contact and employment information at issue could be used to cause the significant harms of identity theft or fraud.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (email account compromise, fraudulent money transfer request). Further, the threat actor had access to two of the Organization's email accounts for over 30 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 affected individuals by letter in August 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner