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	Xpedient Logistics (Organization)
Decision number (file number)	P2020-ND-141 (File #014812)
Date notice received by OIPC	January 2, 2020
Date Organization last provided information	January 2, 2020
Date of decision	November 6, 2020
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 individual 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 the following information: • name, • social insurance number, • date of birth, • bank/financial account information, • contact information, • salary information, • username/email address and password, and • health data. This is information 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	• The Organization experienced an email phishing incident involving unauthorized access to employee email accounts that contained personal information. • The Organization's investigation found that an unauthorized individual gained access to the email accounts between April 25, 2019 and May 14, 2019. • The breach was discovered on November 27, 2019 when the Organization learned of irregularities with some of its payments to vendors and, upon examining some of the related email traffic, discovered that some of the email accounts may have been accessed by an unauthorized actor.
Affected individuals	The incident affected approximately 1,186 individuals, including 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the email accounts and investigated with the assistance of a cybersecurity firm. • Enhanced technical security, including firewalls, multi-factor authentication, encryption, etc. • Implemented spoofing email education and providing continuous education, discussion and communication on weekly site leadership calls outlining the importance of data security. • Provided credit monitoring and identity theft protection coverage and reminding affected individuals to be vigilant in monitoring their credit history.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on December 26, 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 "There is no indication based on available log data that the information about the Alberta resident was viewed, but we are notifying the individual out of an abundance of caution. If the threat actor did view the information about the Alberta resident it could be used to commit fraud or identity theft." In my view, a reasonable person would consider that contact, identity, financial, employment and health information could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. 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 "The likelihood that harm will result to the Alberta resident is low. The attack was focused on diverting payments between [the Organization] and its vendors and not at individuals. We cannot tell if the information of the Alberta resident was viewed, but out of an abundance of caution, have notified the individual and are providing a complimentary one-year subscription to credit monitoring services to mitigate any potential damages that may result from this incident." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the incident resulted from malicious action of an unknown third party (phishing). The Organization can only speculate as to the motives of the attacker and cannot confirm whether the information at issue was viewed or not.

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 contact, identity, financial, employment and health information could be used to cause the harms of identity theft and fraud. Credentials could be used to compromise other online accounts. These are all significant harms. The likelihood of harm resulting from this incident is increased because the incident resulted from malicious action of an unknown third party (phishing). The Organization can only speculate as to the motives of the attacker and cannot confirm whether the information at issue was viewed or not.

I require the Organization to notify the affected individual whose 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 letter on December 26, 2019. The Organization is not required to notify the affected individual in Alberta again.

Jill Clayton
Information and Privacy Commissioner