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	Landstar System, Inc. (Organization)
Decision number (file number)	P2016-ND-34 (File #002818)
Date notice received by OIPC	March 31, 2016
Date Organization last provided information	May 25, 2016
Date of decision	June 21, 2016
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is a corporation operating in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • social insurance number (SIN), • social security number (SSN), • amount of income earned, • tax withholdings for 2015. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• The Organization reported that in two separate incidents, an employee of the Organization received phishing emails. One email appeared to be from the Organization's Vice President and Chief Financial Officer and a second email appeared to be from the Organization's President and CEO. • The first incident occurred on February 24, 2016, and the second on March 18, 2016. • Both emails requested 2015 W-2 forms and T-4 forms for the Organization's employees. • The employee responded to both emails, including copies of the Internal Revenue Canada W-2 forms and Canada Revenue Agency T-4 forms of the Organization's employees. • After the employee responded to the March 18 email, the employee received a third email, which again appeared to be from the CEO of the Organization. This email requested 2015 W-2 forms and T-4 forms. • The employee then called the CEO of the Organization to confirm if he had received the W-2 forms and T-4 forms that the employee believed she had previously sent to the CEO. The conversation confirmed that the CEO did not make any request on March 18. • The employee also told the CEO of the February 24, 2016 request that appeared to have been made by the Vice President and Chief Financial Officer.
Affected individuals	• In total, 1,367 individuals (employees) were affected; 1,362 of the affected individuals are residents of the United States and 5 are residents of Canada. • Of the 5 residents of Canada, 1 is a resident of Alberta.
Steps taken to reduce risk of harm to individuals	• On March 18, 2016, the Vice President, General Counsel & Secretary were notified of both incidents and immediately launched an internal investigation. • The Organization notified the United States Federal Bureau of Investigation. • The Organization offered the affected individuals three years of identity protection services, at no cost. It also provided information to affected individuals for protecting themselves from identity theft, and tax fraud and information to contact the Canada Revenue Agency and Service Canada, for further information.

	• The Organization is conducting a thorough review of its security measures, internal controls, and safeguards and is making changes to existing policies and procedures, including training and awareness programs, in an effort to help prevent a similar incident in the future.
Steps taken to notify individuals of the incident	On March 24, 2016, written notification was sent to all affected individuals about the incident.
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.	Subsequent to the Organization's original report to this Office, it learned from its employees that there were attempts to file fraudulent tax returns using W-2 forms that had been disclosed. The Organization noted that it is not aware of any attempts to file fraudulent tax returns using T-4 forms that were disclosed. The Organization characterized the information on the T-4 forms as "highly sensitive because SINs can be used to commit identity theft or identity fraud". I agree with the Organization's assessment. The personal information involved is sensitive identity information that could be used to cause the harms of identity theft, fraud, and financial loss. 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 reported that "Based on the nature of these incidents, and Landstar's understanding that attempts to file fraudulent returns may have already occurred, Landstar believes the criminals may continue to attempt to file fraudulent tax returns". I agree that there is a real risk of harm resulting from this incident. The incident is the result of malicious intent (deliberate actions of third parties to send three phishing emails within a period of 23 days to obtain sensitive personal information). Some of the compromised personal information (W-2 forms) was used to file fraudulent tax returns.
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 personal information involved is sensitive identity information that could be used to cause the significant harms of identity theft, fraud and financial loss. The incident is the result of malicious intent (deliberate actions of third parties to send three phishing emails within a period of 23 days to obtain sensitive personal information). Some of the compromised personal information (W-2 forms) was used to file fraudulent tax returns.	

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals in accordance with the Regulation on March 24, 2016. The Organization is, therefore not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner