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	Institute for Supply Management (Organization)
Decision number (file number)	P2019-ND-012 (File #008268)
Date notice received by OIPC	April 11, 2018
Date Organization last provided information	December 5, 2018
Date of decision	February 14, 2019
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 located in Tempe, Arizona. The Organization operates on a not-for-profit basis, but is not a "non-profit" organization as defined in PIPA, such that it would only be subject to PIPA in relation to personal information collected, used and disclosed in connection with a commercial activity. 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, • email address, and • credit or debit card numbers if used in transactions appearing in affected emails. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or about January 25, 2018, an unauthorized sender caused "phishing" emails to be sent to email addresses contained in an employee's email contacts list, which was contained on or accessed by a mobile computing device used by that employee for exchanging emails with certain customers of the Organization. • The phishing emails contained links to an apparently fake "Docusign" website, the purpose of which was to trick recipients into clicking on a link that would have requested the recipient provide information or otherwise comply with a fraudulent request for information or transfers of funds. • The Organization said it is not aware of any indication that the senders of the phishing emails tried or were able to gain access to the Organization's computer networks or obtain the actual contents of the Organization's customers' emails. • Although the Organization said it does not have direct evidence that senders of the phishing emails caused a breach and obtained personal information, out of an abundance of caution, the Organization notified its customers because it said it could not rule out this risk at this time based on the information it currently has.
Affected individuals	The incident affected 246 individual customer email addresses, including one individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Commissioned a review by a leading cybersecurity consultant to determine the level of exposure and provide recommendations for remediation. • Engaged law firm to review the circumstances and prepare the necessary notifications. • Required all employees to reset their passwords. • Advanced its rollout of an already planned implementation of two-factor authentication to access company email accounts.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by email on March 16, 2018.

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 that "While we do not currently have any direct evidence that the following occurred, if an Organization's customers' credit or debit card information was contained in an email and if senders of the phishing emails obtained access to the contents of such an email, then the risk exists that that information could be used to attempt to use the credit or debit card number for an unauthorized transaction." I agree with the Organization's assessment. A reasonable person would consider that the contact and financial information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. 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 that "The information currently available is consistent with the potential breach being limited to a goal of obtaining access to email addresses for the purpose of sending those addresses phishing emails in furtherance of some kind of phishing scheme intended to lure recipients into providing additional information or making financial transferred. However, it is impossible at this time to determine whether any personal information has been breached. By notifying the Organization's customers who potentially may be at risk, the Organization has taken the step to ensure those customers may be vigilant to mitigate the risk of harm in the event there was an actual breach." In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (social engineering) by an unknown third party and it appears the personal information may have been used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized sender accessed, read, copied, or downloaded the personal information within customer emails.
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 and financial information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. 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 as the breach was the result of malicious intent (social engineering) by an unknown third party and it appears the personal information may have been used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized sender accessed, read, copied, or downloaded the personal information within customer emails.

I require the Organization to notify the affected individual 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 individual in an email dated March 16, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner