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	JYSK Canada (Organization)
Decision number (file number)	P2018-ND-093 (File #009318)
Date notice received by OIPC	July 27, 2018
Date Organization last provided information	July 27, 2018
Date of decision	August 1, 2018
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 in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and 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, • email address, • telephone number, • delivery address, and • credit card information (number and expiry date). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta in-store and online.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 29, 2018, an employee of the Organization received a suspicious email from a random domain that looked like a phishing email and contained the address of one of the Organization's physical locations.

	• The employee shared the information internally with the e-commerce team, and reported the email to the information technology department**.** • The Organization's investigation indicates that an unauthorized person gained access to the back end of the e-commerce platform remotely, and placed a script allowing the collection of order information as the order was placed. It appears the unauthorized third party was able to access the e-commerce platform remotely using the username and password of an employee with administrator privileges. • Customers who used the online e-commerce platform at www.jysk.ca between June 4 and June 29, 2018 were affected.
Affected individuals	The incident affected approximately 741 customers residing in the province of Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the unauthorized script on the day it was discovered. • Informed payment processor of the incident. • Retained an independent cyber forensics audit firm to assist in its investigation. • Whitelisted IP addresses for employees who work from home as well as any other employee from the ecommerce department who needs home access - therefore blocking all other accesses. • Access to certain functions in the backend of the platform was further restricted and usernames and log-in procedures were strengthened. • Audited the employee's electronic devices whose credentials were used, reset all employees' credentials (username and password) and implemented new security measures to ensure that the passwords for access to the e-commerce platform are automatically changed on a monthly basis. • Reported the incident to Canadian privacy commissioners.
Steps taken to notify individuals of the incident	The potentially affected individuals were directly notified in writing on Friday July 27, 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 "The type of personal information compromised and the context of such access (use of employee credentials by an unauthorized third party), is such that [the Organization] believes that the risk of harm is enough to reach the threshold where there is a real risk of significant harm to the affected individuals: risk of fraud/ID theft or risk of phishing depending on the information collected." I agree with the Organization's assessment. The contact and financial information at issue could be used to cause the harms of

	identity theft and fraud. Email addresses could be used for phishing purposes. 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.	As noted above, the Organization reported that "The type of personal information compromised and the context of such access (use of employee credentials by an unauthorized third party), is such that [the Organization] believes that the risk of harm is enough to reach the threshold where there is a real risk of significant harm to the affected individuals…". I agree with the Organization. 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, use of employee credentials and malware). Further, the information may have been exposed for over three weeks.

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 and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. 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, use of employee credentials and malware). Further, the information may have been exposed for over three weeks.

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

I understand the Organization notified potentially affected individuals were directly notified in writing on Friday July 27, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner