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	Kroto Inc., dba iCanvas (Organization)
Decision number (file number)	P2021-ND-041 (File #016324)
Date notice received by OIPC	June 29, 2020
Date Organization last provided information	June 29, 2020
Date of decision	March 2, 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 the 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 located in Illinois, USA, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involves some or all of the following information: • name, • credit or debit card number, expiry date, and security/verification codes. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 28, 2020, the Organization discovered that unauthorized script was placed on the checkout page of its website. • The script potentially allowed for the capture of information submitted by customers if the customer was using the credit card payment function and the "place your order" button was selected.

	• The Organization reported that the unauthorized script was likely placed on its website on or about May 10, 2020.
Affected individuals	The incident affected 92 individuals in Canada, including 8 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Removed unauthorized script from the website. • Patched the vulnerability that allowed the threat actor to gain access to the Organization's environment. • Retained legal counsel. • Notified the FBI and the Organization's merchant bank, which in turn notified credit card networks. • Offering a one-year subscription for identity theft and credit monitoring services to all affected parties, free of charge. • Implementing additional security measures (e.g. additional training for personnel, internal security audit of custom code base, adjusting backup and log retention time frames, rotating access keys and changing applicable passwords, reviewing and reviewing and requiring additional security measures from third party providers).
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 26, 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 that the harm that may occur as a result of the breach is "Fraudulent misuse". In my view, a reasonable person would consider that the contact and financial information (credit card information) at issue could be used to cause the harms of identity theft and fraud. 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, *The likelihood that the harm identified above will result is moderate. At this stage, [the Organization] does not have direct evidence that the personal information has been misused as a result of the unauthorized access. Nonetheless, the personal information involved was sensitive and and [sic] there is a possibility of misuse by threat actors.* 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 an

	unknown third party (deliberate intrusion). Further the information may have been exposed for about three (3) 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.

A reasonable person would consider that the contact and financial information (credit card information) at issue could be used to cause the harms of identity theft and fraud. These are 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). Further the information may have been exposed for about three (3) weeks.

I require the Organization to notify the affected individuals 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 by email on June 26, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner