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	KURU Footwear (Organization)
Decision number (file number)	P2017-ND-74 (File #005693)
Date notice received by OIPC	May 26, 2017
Date Organization last provided information	May 26, 2017
Date of decision	June 9, 2017
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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • card number, expiry date, CVV code. 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 e-commerce website. To the extent the information was collected in Alberta, I have jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On February 2, 2017, the Organization began investigating unusual activity reported by its credit card processor.

	• On February 23, 2017, the Organization discovered that it was the victim of a cyber-attack that resulted in the potential compromise of some customer's debit and credit card data used at www.kurufootwear.com between December 20, 2016 and March 3, 2017.
Affected individuals	The Organization reported the incident may have affected 10 Canadians. The Organization did not report the number of affected Alberta residents.
Steps taken to reduce risk of harm to individuals	• Worked with third-party forensic experts to investigate initial reports, determine what happened, what information was affected and to implement additional procedures to protect security of information. • Removed malware. • Working with Federal Bureau of Investigation to investigate the incident. • Established a dedicated hotline for individuals to contact with questions or concerns.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on or about May 15, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 did not specifically identify any harm that might result from this incident, but reported that it is "providing potentially impacted individuals with helpful information on how to protect against identity theft and fraud". In my view, the financial information at issue 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 did not specifically assess the likelihood of harm resulting from this incident. In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for over two months.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for over two months. I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation.* I understand the Organization notified affected individuals by letter on or about May 15, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner