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	Nodor International Limited (trading as Red Dragon Darts) (Organization)
Decision number (file number)	P2021-ND-110 (File #013497)
Date notice received by OIPC	July 8, 2019
Date Organization last provided information	July 8, 2019
Date of decision	April 7, 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 those 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved all or some of the following information: • name, • address, • telephone number, • email address, and • payment card information (name, card number, CVV and expiry date). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On March 20, 2019, the Organization was contacted by its card payment merchant acquirer, Worldpay, regarding irregularities experienced by customers after purchasing goods on the Organization's website, www.reddragondarts.com. • The Organization's investigation at the time of reporting indicated that the website was compromised by malicious code that collected data from the payment page, sending it to a remote server under the attacker's control. • The Organization reported there were two windows of compromise: September 9, 2018 to January 24, 2019 and March 4, 2019 to March 6, 2019, although the latter window may have begun as early as February 15, 2019.
Affected individuals	The incident affected up to 15,732 customers, including 19 based in Alberta.
Steps taken to reduce risk of harm to individuals **".**	• Engaged third party forensic investigators. • Removed malicious scripts, secured systems and closed vulnerabilities. • Arranged and passed a PCI compliance check. • Changed the way online payments are processed. • Moving to a new developer and platform. • Followed up with current developer to ensure all recommendations made by the forensic vendors have been implemented. • Incorporating new monitoring and security procedures.
Steps taken to notify individuals of the incident	The Organization reported that it was intending to notify all affected individuals "without undue delay".
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 its notification to affected individuals would identify "...steps they can take to protect themselves" and would offer a 12 month membership to a darkweb monitoring service to "...help them to monitor their personal data for certain signs of potential identity theft". In my view, a reasonable person would consider 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, increasing vulnerability to identity theft and fraud.

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 it is "...aware that the risk of unauthorised access to payment card details is likely to result in a "real risk of significant harm"". In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action on more than one occasion. The information was exposed for over 4 months.

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 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, increasing vulnerability to identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action on more than one occasion. The information was exposed for over 4 months.

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

The Organization reported that it was intending to notify all affected individuals "without undue delay". I require the Organization to confirm to my office in writing, within 10 days of the date of this decision, that it has done so.

Jill Clayton
Information and Privacy Commissioner