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	Matador Recordings, LLC (Organization)
Decision number (file number)	P2017-ND-112 (File #003525)
Date notice received by OIPC	July 18, 2016
Date Organization last provided information	July 18, 2016
Date of decision	August 8, 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, • telephone number, • email address, • credit card number, expiry date, security code (CVV), and • website account password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected through the Organization's e-commerce websites.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 4, 2016, the Organization was advised by its third-party website developer that suspicious files had been identified and removed from the e-commerce websites of the record labels for which the Organization is the distributor. • The affected e-commerce websites are as follows: www.4ad.com , www.matadorrecords.com, www.roughtraderecords.com, www.truepanther.com, www.xlrecordings.com, www.theyoungturks.co.uk, or www.archive.beggars.com. • Online orders placed between April 28, 2015 and May 4, 2016, may have been obtained by an unauthorized third-party.
Affected individuals	The incident affected 56 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• The malicious software was removed from the sites. • An investigation into the incident was initiated by the Organization and a third party cybersecurity firm was contracted to conduct the investigation. • Customers' account passwords for the affected sites were reset. • Customers were advised to avoid using the same username and passwords for multiple websites. • A toll-free line was established to address questions and concerns that customers may have had about the matter. • Additional steps were taken to strengthen the security of the sites. • The Organization advised its customers to review account statements and report any unauthorized transactions to their financial institutions.
Steps taken to notify individuals of the incident	The Organization began notifying affected individuals in writing on July 15, 2016.
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 "Stolen payment card information is generally used to make fraudulent charges." I agree with the Organization. The contact and financial information at issue could be used to cause the harms of identity theft and fraud. Credentials (passwords) could be used to compromise other online accounts. 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.	The Organization reported that "…generally, card network regulations provide that cardholders are not responsible for fraudulent charges that are timely reported to the issuer of the card." In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from malicious intent (deliberate intrusion and installation of suspicious files) and the information was exposed for approximately a year. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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. Credentials (passwords) could be used to compromise other online accounts. 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 incident resulted from malicious intent (deliberate intrusion and installation of suspicious files) and the information was exposed for approximately a year. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 affected individuals were notified in writing beginning on July 15, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner