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	Goldenvoice, LLC (Organization)
Decision number (file number)	P2017-ND-136 (File #005305)
Date notice received by OIPC	March 30, 2017
Date Organization last provided information	October 3, 2017
Date of decision	October 3, 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 based in the state of California 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: • first and last name, • email address, • mailing address, • telephone number, • date of birth, • website username, • driver's license number (or barcode), and • passport number or other ID information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via the Organization's website, Coachella.com, and/or at the Coachella or Stagecoach music festivals.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• Sometime between September 2016 and early March 2017, hackers obtained unauthorized access through the Coachella.com website to certain databases connected to it (including data collected at the Coachella festival, Stagecoach festival and the Coachella.com website forum). • On February 21, 2017, the Organization discovered the incident when the attackers sent an email demanding ransom for the information.
Affected individuals	The incident affected 600,000 individuals, including 30 to 40 Alberta residents with names and emails compromised and approximately 14 Albertans whose identification documents were compromised.
Steps taken to reduce risk of harm to individuals	• Patched the vulnerability and mitigated the known risks to ongoing operations. • Took steps to recover the information and eliminate any distribution of the data by the hackers. • Engaged service providers to monitor the distribution of known lists.
Steps taken to notify individuals of the incident	An initial group of affected individuals were notified by email on February 28, 2017. A second group was notified via mail and email on March 24, 2017.
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 the possible harm that might result from this incident include "phishing scams as a result of the breach of email addresses, especially in combination with other information (such as name and evidence of interest in musical festivals)." The Organization also identified telephone scams and tailored scams as possible harms. The Organization reported that those individuals "whose ID number (e.g. driver's license or passport number) was breached may be at risk for identity theft and other forms of impersonation." I agree with the Organization. The contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. Credentials (username) could be used to compromise other online accounts. 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 "The risk of harm may be significant… however, the majority of individuals did not have all applicable data fields present within the database, which may limit the possibility of successful identity theft or impersonation." In my view, 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 and installation of malware). Further, the information may have been exposed for approximately seven 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.

The contact and identity information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. Credentials (username) could be used to compromise other online accounts. These are all significant harms. The likelihood of harm is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and installation of malware). Further, the information may have been exposed for approximately seven months.

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 an initial group of affected individuals by email on February 28, 2017. A second group was notified via mail and email on March 24, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner