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	Shutterstock Music Canada ULC dba PremiumBeat (Organization)
Decision number (file number)	P2017-ND-40 (File #004143)
Date notice received by OIPC	October 25, 2016
Date Organization last provided information	October 25, 2016
Date of decision	March 6, 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 following information was involved in this incident: • name, • address, • telephone number, • email address, and • encrypted passwords for website users. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 29, 2016 the Organization became aware of unauthorized access to its database through a vulnerability in a third party plugin to software used on its website. • Through malware infecting software on the server, the perpetrator was able to download user information.

Affected individuals	A total of 150,000 individuals were affected, including 1,613 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Shut down affected systems, patched vulnerabilities and re-architected the affected systems for security. • Installed monitoring and logging software to monitor malicious files and block further attacks. • The compromised software was updated, patched, and isolated in an environment separate from personal information within approximately 24 hours.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on October 4, 2016.
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 reported "This breach could lead to phishing and unauthorized access to other on line accounts. The large number of email addresses makes it possible to engage in phishing attacks against those users. If the passwords are decrypted, individuals could suffer from unauthorized access to other online accounts using the same compromised credentials." The Organization also reported that it "stores no other identification information, which minimizes the risk of using this information for identity theft or fraud." I agree with the Organization's assessment. Email addresses could be used for phishing purposes. Decrypted passwords could be used to obtain unauthorized access to other online accounts. 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.	As noted above, the Organization reported that "The large number of email addresses makes it possible to engage in phishing attacks against those users." Further, "The passwords were stored encrypted. Analysis of the logs shows that the information was accessed once, as a result of malware infecting software on the … server." I agree with the Organization's assessment. The likelihood of phishing is increased as the incident resulted from malicious intent (deliberate intrusion and installation of malware); however, unauthorized access to online accounts is less likely as the credentials would need to be decrypted. The information was downloaded and has not been recovered.

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. Email addresses could be used for phishing purposes. Decrypted passwords could be used to obtain unauthorized access to other online accounts. These are significant harms. The likelihood of phishing is increased as the incident resulted from malicious intent (deliberate intrusion and installation of malware); however, unauthorized access to online accounts is less likely as the credentials would need to be decrypted. The information was downloaded and has not been recovered. 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 affected individuals by email on October 4, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner