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	Tapestry Music Ltd. (Organization)
Decision number (file number)	P2019-ND-048 (File #011619)
Date notice received by OIPC	January 11, 2019
Date Organization last provided information	January 11, 2019
Date of decision	May 1, 2019
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 involved all or some of the following information of the Organization's customers, who both rent and purchase music equipment from the Organization. Other individuals created online accounts, but did not complete any transactions. • name, • telephone number, • email address, • address, • driver's license number, • spousal information (name, name of spouse employer, telephone number), • student information (name, name of school), • employment information (name of employer, work telephone number), • transaction details, • login information, and • credit card information (only customers who paid by Converge may have had their credit card information affected).

	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 website, www.tapestrymusic.com. To the extent the personal information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In early and mid-December 2018, the Organization was notified by a few of its customers that their information had been accessed. • On December 17, 2018, the Organization's IT Consultant confirmed that it had discovered backdoors on the Organization's website, www.tapestrymusic.com. • The threat actors first gained access on September 15, 2017 by attacking plugins, which allowed access to the website and customer database.
Affected individuals	The incident affected 5,112 individuals, including 213 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Shut down the ecommerce site on December 17, 2018 and hired a third party company to re-build the site. • Fully audited the email hosting platform. • Reset all passwords for staff email accounts, admin accounts on the ecommerce system, and operating system accounts on the virtual machine hosting its website. • Enforcing stronger passwords on all staff email accounts and all admin and system accounts. • Arranged for complimentary credit monitoring for customers whose credit card information may have been compromised. • Reported breach to the Information and Privacy Commissioner of British Columbia and the Federal Privacy Commissioner.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 24, 2018 or by mail on December 27, 2018 and January 10, 2019.
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	The Organization reported "The possible harms could include financial fraud where credit card information is affected, identity theft where employment and driver's license information is affected, and phishing campaigns where email addresses and login information is affected". I agree with the Organization's assessment. In my view, a reasonable

non-trivial consequences or effects.	person would consider that the contact, identity, financial, education and employment information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, resulting in an increased vulnerability to identity theft and fraud. Login information 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 "There is a reasonable likelihood that harm may result because this was an intentional and malicious attack on [the Organization's] website perpetrated by threat actors who were looking to appropriate valuable information. A few … customers have also reached out … to advise that their information had been accessed and that fraudulent charges to their credit cards had been attempted". In my view, a reasonable person would consider that 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). The information was exposed for over a year. Some affected individuals reported attempted 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.

A reasonable person would consider that the contact, identity, financial, education and employment information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, resulting in an increased vulnerability to identity theft and fraud. Login information could be used to compromise other online accounts. These are all significant harms.

The likelihood of harm resulting is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). The information was exposed for over a year. Some affected individuals reported attempted fraud.

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).

I understand affected individuals were notified by email on December 24, 2018 or by mail on December 27, 2018 and January 10, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner