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	Indigo Books & Music Inc. (Organization)
Decision number (file number)	P2017-ND-07 (File #001075)
Date notice received by OIPC	July 3, 2015
Date Organization last provided information	October 8, 2015
Date of decision	January 5, 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"	I have jurisdiction because 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, • billing address, • shipping address, • transaction history, • loyalty program number and points balance, • loyalty program transaction history, • telephone number, • date of birth, • product areas of interest, and • future product purchase wish lists. The Organization also reported that "while certain customer accounts have stored credit card information linked to their accounts, this credit card information is masked and was not accessible. However, once credentialed access to the account is gained, purchases using the stored credit card data are possible at [the Organization's online shopping site] only."

	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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 8, 2015, the Organization received two separate reports from customers of unauthorized electronic gift card transactions made on June 5. • The Organization investigated and found that an unauthorized individual had gained access to 102 customer accounts using valid credentials. • The Organization reported that its own customer systems had not been compromised and so the authentication credentials used for accessing the accounts could not have originated from its systems. • The Organization reported that it believes the accounts were accessed using email address and password combinations obtained from a website that posts personal information from compromised applications. • The Organization reported that the authentication credentials used for accessing those accounts may have been obtained as a result of individuals using the same authentication credentials across multiple e-commerce applications. • Upon accessing an account, the unauthorized individual(s) changed the email address on the account and then made purchases using gift and credit cards on the account.
Affected individuals	A total of 102 Canadians were affected by this incident, including 12 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Suspected unauthorized purchases were placed on hold. • Account passwords were reset and customers were advised to change their account emails. • A password strength meter was implemented and customers were advised to select strong passwords. • Passwords are salted and hashed. • The Organization implements encryption (secure socket layer) on its e-commerce sites. • The Organization certifies its online environment to ensure compliance with Payment Card Industry Data Security Standard. • The incident was reported to the City of Ottawa Police. • The individual responsible for the incident was arrested and charged on June 24, 2015.

Steps taken to notify individuals of the incident	Affected individuals were notified of the incident by email sent June 23, 2015.
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 that there is no real risk of significant harm to the affected individuals because the email and password combinations used for accessing the accounts were not obtained from the Organization's systems and there is no evidence to indicate that the unauthorized individual had a desire to access and use personal information of the affected individuals. The Organization said "On the contrary, although the unauthorized individual has exhibited nefarious intent, it is very apparent that his nefarious intent is to unlawfully acquire goods through the fraudulent use of stolen email and password combinations and the misappropriation of electronic gift card balances." In my view, although the unauthorized individual did not obtain credentials from the Organization (but rather from some other source), the information was nonetheless used to obtain access to identity (i.e. date of birth) and comprehensive profile information in the Organization's systems. This information could be used to cause the significant harms of 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.	Despite reporting that the unauthorized individual's "nefarious intent is to unlawfully acquire goods through the fraudulent use of stolen email and password combinations…", the Organization reported that there is no real risk of significant harm to the affected individuals. The Organization reported it is "carefully reviewing every recent account charge transaction to ensure that accounts can be properly restored or replaced, thereby eliminating or minimizing any potential harm or inconvenience to the affected account holders." The Organization also "elected to advise the individuals that they will not be charged for any fraudulent purchases made in relation to this incident." In my view, the likelihood of harm resulting from this incident is increased because there was malicious intent involved (deliberate intrusion) and information in the Organization's control was in fact used to make fraudulent purchases. Although the Organization has committed to ensuring customers are not charged for fraudulent purchases, this will only apply where the Organization is aware of such transactions. Further, this does not necessarily mitigate the potential harm that may result if information from the Organization's systems is used for identity theft or other forms of fraud (at other e-commerce sites, for example). Finally, the personal information at issue was exposed for almost three weeks (from at least June 5 until the individual was arrested June 24).

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. Although the unauthorized individual did not obtain credentials from the Organization (but rather from some other source), the information was nonetheless used to obtain access to identity (i.e. date of birth) and comprehensive profile information in the Organization's systems. This information could be used to cause the significant harms of identity theft and fraud (and was in fact used to make fraudulent purchases). The likelihood of harm resulting from this incident is increased because there was malicious intent involved (deliberate intrusion) and information in the Organization's control was in fact used to make fraudulent purchases. Although the Organization has committed to ensuring customers are not charged for fraudulent purchases, this will only apply where the Organization is aware of such transactions. Further, this does not necessarily mitigate the potential harm that may result if information from the Organization's systems is used for identity theft or other forms of fraud (at other e-commerce sites, for example). Finally, the personal information at issue was exposed for almost three weeks (from at least June 5 until the individual was arrested June 24). I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the individuals by email sent June 23, 2015 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner