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	G.P Performing Arts Guild (Organization)
Decision number (file number)	P2013-ND-38 (File #P2356)
Date notice received by OIPC	June 5, 2013
Date Organization last provided information	November 8, 2013
Date of decision	November 25, 2013
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 56(1) of PIPA "non-profit organization"	The Organization is non-profit private company incorporated in Alberta. The Organization was incorporated in 2009 under the Alberta *Companies Act* and is registered as a private non-profit organization. A "non-profit organization" as defined by section 56(1)(b)(i) of PIPA includes an organization that is registered under Part 9 of the *Companies Act*. According to section 2.1(a)(i) of the *Companies Act*, as of February 1, 1982, no company could be incorporated under the *Companies Act* except under Part 9. The Organization was incorporated in 2009 and, therefore, fits the definition of a "non-profit organization" in section 56(1)(b)(i) of PIPA. Section 56(3) of PIPA states that the Act applies to a non-profit organization only in the case of personal information that is collected, used or disclosed by the non-profit organization in connection with any commercial activity carried out by the

	non-profit organization. "Commercial activity" is defined in section 56(1)(a) of PIPA. The Organization reported that the personal information involved in the incident was collected in connection with the purchasing of tickets to Organization art functions or dinner theatre. In my view, the selling of tickets for these events is a commercial activity carried out by the Organization. The personal information involved with this incident and collected by the Organization during the course of this commercial activity is subject to the application of the Act.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • email address, • phone number, and • credit card number and expiry date. This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	

Description of incident	• The Organization uses a third party service provider web application to facilitate online ticket purchasing, marketing and customer relations.
	• The service provider experienced an unauthorized intrusion into the web application server system on April 25, 2013, that involved the above personal information of Organization patrons.
	• The Organization patrons purchased tickets online to art functions or dinner theatre using the service provider web application system.
	• The service provider provided the following details about the intrusion:
	  o The compromised server was located in San Francisco, California.
	  o The intrusion appeared criminally motivated and involved installation of malware on the server.
	  o The credit card information was encrypted.

	However, this information may be accessible based on the nature of the intrusion.
Affected individuals	• The incident involved Organization patrons in addition to other members of the service provider in the United States and Canada. • 61,559 Canadians were involved. • Approximately 8,770 individuals provided Alberta addresses to the service provider at the time of the ticket purchase. • The Organization was unable to determine how many of its patrons were included in the 8,770 Alberta addresses.
Steps taken to reduce risk of harm to individuals	The service provider engaged a third party to investigate the incident, implemented enhanced security measures, and reported the incident to U.S. law enforcement and affected members that use the web application server system, including the Organization.
Steps taken to notify individuals of the incident	The service provider notified affected individuals in Canada by letter on May 21, 2013, including the patrons of the Organization.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 recognized the affected individuals may be at risk for identity theft and fraud due to the credit card information involved in the incident. In my view, the personal information involved is highly sensitive. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft or fraud. Since a significant number of email addresses, addresses and phone numbers were involved, the affected individuals may also be at risk for phishing. In my view, 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.	The Organization reported that due to the sensitivity of the personal information involved and the fact that the incident involved an unknown intruder, it considered there to be a real risk of significant harm to the affected individuals. I agree with the Organization that there is a real risk of significant harm to the affected individuals as a result of this incident. The credit card information may be accessible based on the nature of the intrusion. A significant number of email addresses and phone numbers are involved which places the

	affected individuals at risk for targeted phishing. These factors, in combination with the service provider's report that the intrusion appeared criminally motivated, in my view, increases the likelihood of significant harm resulting from this incident.

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 credit card information may be accessible based on the nature of the intrusion, the incident was caused by the installation of malware by an unauthorized intruder with alleged criminal intent, and a significant number of affected individuals' email addresses and contact information was involved. These factors contributed to my decision.

I require the Organization to notify its affected patrons in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the service provider notified all affected individuals, including the patrons of the Organization, in a letter dated May 21, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify its patrons again.

Jill Clayton
Information and Privacy Commissioner