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	Gingerbread Shed Corporation (Organization)
Decision number (file number)	P2014-ND-12 (File #P2693)
Date notice received by OIPC	May 20, 2014
Date Organization last provided information	May 20, 2014
Date of decision	September 30, 2014
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 information at issue was collected in Alberta and stored on a server located in Phoenix, Arizona USA. 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, • address, • telephone number, • email address, • account user name and password, • credit card information (card number, card verification value or CVV, expiry date, account number) This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization was notified of a potential issue by a merchant, who had been contacted by their processor. A forensics firm was hired and conducted an investigation. The investigation determined that an unauthorized intrusion had occurred. The attack was conducted utilizing sophisticated malware enabling the attackers to capture and download data stored on the Organization's server. • The attack occurred between November 25, 2013 and February 17, 2014. It was discovered in April 2014.
Affected individuals	50,000 customers were affected; 1,265 of these customers are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• An independent forensic investigation was initiated to determine the extent of the security incident. • Law enforcement officials were informed. • Credit card companies were notified. • Affected servers were removed and replaced with newly built and secure ones. • Software patches were installed. • Administrative passwords were changed. • Firewall rules were updated to ensure suspicious IP (Internet Protocol) addresses are blocked. • Considerations have been made to implement advanced threat defence system and application whitelisting. • Customers were advised to monitor their credit records and financial accounts.
Steps taken to notify individuals of the incident	The Organization began notifying affected individuals on May 5, 2014.
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 recognized that the information at issue could be used to cause harm, and specifically financial loss/fraud in the form of fraudulent credit card charges. In my view, the personal and financial information involved is highly sensitive. The types of harm that could result from unauthorized access to or use of the information in this instance are identity theft, financial loss and/or fraud. 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 there is a risk of harm due to malicious intent, the fact the information was exposed for approximately 90 days, and the information has not been recovered. I agree with the Organization's assessment. In my view, these factors increase 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 personal information involved could be used to cause significant harm in the form of identity theft, financial loss and/or fraud. There is a real risk of harm due to malicious intent, the fact the information was exposed for approximately 90 days, and the information has not been recovered. These factors contributed significantly to my decision.

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 affected individuals, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner