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	Outdoor Network LLC. (Organization)
Decision number (file number)	P2015-ND-08 (File #P2451)
Date notice received by OIPC	September 5, 2013
Date Organization last provided information	September 17, 2013
Date of decision	February 25, 2015
Summary of decision	There is a 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 incorporated in Lake Placid, Florida. I have jurisdiction because the Organization is an "organization" as defined in section 1(1) (i) (i) of PIPA and the personal information was collected from Alberta, via the internet.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following personal information: • client names, • mailing address, • credit card number, • credit card expiration date, • credit card CVV or CVC code. 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	• On July 16, 2013 there was an unauthorized intrusion into the Organization's websites. A third party installed malware on the Organization's server, allowing access to the shopping cart portion of the Organization's website. • The breach was discovered on July 16, 2013. It was found that the breach affected purchases from the company between December 2012 and July 2013. • The personal information stored in the applicable database included the following fields: name, address, credit card number, credit card expiration date and credit card security code (CVV or CVC code).
Affected individuals	400 affected individuals were residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization notified all the affected credit card companies of the breach. • The Organization undertook an independent forensic investigation to ensure the malware was removed from its data systems. • The Organization arranged to provide credit information and call center-related services to affected individuals.
Steps taken to notify individuals of the incident	Notifications were sent to affected individuals by mail on September 12, 2013.
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 recognized the sensitivity of the information at issue and that unauthorized access may pose a risk for harm, specifically identity theft and fraud. In my view, the personal information involved is highly sensitive. The types of harm that could result from unauthorized access to the personal information in this instance are identity theft and fraud. 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, it considered there to be a real risk of significant harm to the affected individuals. In my view, there is a real risk of harm resulting from this incident given the breach was the result of an unauthorized intrusion and installation of malware, and considering the number of individuals affected.

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 includes sensitive financial information, the breach was the result of an unauthorized intrusion and installation of malware, and a significant number of individuals were affected. The Organization notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* on September 13, 2013. The Organization is therefore not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner