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	Internap Inc. (Organization)
Decision number (file number)	P2014-ND- 56 (File #P2313)
Date notice received by OIPC	April 19, 2013
Date Organization last provided information	December 17, 2013
Date of decision	May 20, 2014
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 Delaware, USA. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and the information of Albertans was collected in Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • mailing address, • email address, • phone number, and • encrypted credit card number. The information listed above is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that, in some cases, the email address involved may have been a business email address. Section 4(3)(d) of PIPA states that the Act does not apply to the

	collection, use or disclosure of an individual's business contact information (defined in section 1(1)(a) to include a business email address) if the collection, use or disclosure is to contact the individual in relation to his/her business responsibilities and for no other purpose. As this is not the case in this incident, business email addresses are not excluded under section 4(3)(d).
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Sometime between March 4, 2013 and March 9, 2013, an unknown individual(s) gained access to the Organization's computer systems located in New York, NY USA. The systems held a database which stored customer information. • The breach was discovered on March 9, 2013, during a routine check of the Organization's systems by the technology team. • The personal information stored in the database included the following fields: name, mailing address, email address, phone number and encrypted credit card number. The number of completed fields varied by customer. • Within the database, the credit card information was stored in an encrypted format. All other personal information was stored in clear text. • The Organization could not confirm if the personal information was in fact accessed as a result of the intrusion; instead, the Organization reported there may have been unauthorized access to personal information on the server. There is no evidence to confirm whether or not actual customer profiles were accessed. The only evidence the company has is that the perimeter was hacked.
Affected individuals	The total number of affected customers worldwide was 5,883, including 2,258 with encrypted credit card information. The number of affected customers in Alberta was 14, all of whom had encrypted credit card information in their profile.
Steps taken to reduce risk of harm to individuals	The server and email function were shut down and were restored from known backup data. Entry point vulnerabilities were closed and updated as needed.
Steps taken to notify individuals of the incident	The Organization notified all affected individuals on April 16, 2013 by letter.

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.	In my view, the personal information involved is generally of low sensitivity. However, due to the nature of the intrusion and the significant number of email addresses, mailing addresses and phone numbers involved, I agree with the Organization that the affected individuals may be at risk for phishing. In my view, this is a significant harm.
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 since the intrusion used the server to send spam email to email addresses unrelated to the Organization, the possibility that the malware collected personal information from the compromised web server as a secondary objective to use for another similar event could not be ruled out. In my view, the likelihood of harm resulting from this incident is increased because of the nature of the malware and the unauthorized access. The Organization could not rule out the possiblilty of the malware collecting personal information. A significant number of email addresses and contact information are involved in this incident. In my view, these factors increase the likelihood of phishing as a result of 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 incident involved the installation of malware on the server. The malware sent spam email to unrelated email addresses using the Organization's server. The Organization submitted that due to the nature of the malware, the possibility could not be ruled out that the malware collected personal information during the incident that could be used for phishing.

The Organization notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) on April 16, 2013. The Orgainization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner