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	Joyent, Inc. (Organization)
Decision number (file number)	P2018-ND-012 (File #004570)
Date notice received by OIPC	December 15, 2016
Date Organization last provided information	December 5, 2017
Date of decision	January 11, 2018
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 Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • country of residence, • telephone number, and • hashed password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that it provides services to businesses and individual users. As such, some of the information appears to qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information."

	Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that PIPA applies to the personal information about the thirty-four (34) residents of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization provides cloud-hosting services for businesses and individual users. • The Organization recently learned that on December 4, 2014, an unauthorized party obtained certain data maintained on the Organization's user management database. • The relevant system is a backend database used by the Organization to manage information pertaining to user accounts.
Affected individuals	The incident affected 34 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Took steps to secure its systems and protect its users. • Remediated the Organization's network. • Has no indication that the issue involved payment card data. • Continues to review its systems and protocols in its ongoing effort to enhance security. • Implemented administrative and technical safeguards to help prevent a similar issue from occurring in the future.
Steps taken to notify individuals of the incident	The Organization did not notify the affected individuals.

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 a low likelihood of harm to affected users, however, because (1) the affected data listed above is not sensitive in nature and (2) this data alone would not provide an unauthorized party with access to a user's account." In my view, email addresses could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing 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 "there is a low likelihood of harm to affected users, however, because (1) the affected data listed above is not sensitive in nature and (2) this data alone would not provide an unauthorized party with access to a user's account." In my view, the likelihood of harm resulting in this case is increased because the incident appears to be the result of malicious intent (unauthorized access). Further, the information may have been exposed for approximately 2 years.

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.

Email addresses could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing is a significant harm. The likelihood of harm resulting in this case is increased because the incident appears to be the result of malicious intent (unauthorized access). Further, the information may have been exposed for approximately 2 years.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). The Organization is required to confirm to my Office, within ten (10) days of the date of this decision, that it has done so.

Jill Clayton
Information and Privacy Commissioner