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	1209652 Alberta Limited (Organization)
Decision number (file number)	P2015-ND-03 (File #P2632)
Date notice received by OIPC	March 26, 2014
Date Organization last provided information	May 13, 2014
Date of decision	January 12, 2015
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 incorporated in Alberta. 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 following information is at issue: • names of all individuals, • social insurance numbers of 6 employees and 6 clients, • phone numbers of all individuals, • addresses of all individuals, • email addresses of all individuals, and • employee time sheets of 6 employees This information is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	Emails containing confidential client and employee information were emailed to two contracted staff's personal email accounts. This was an unauthorised disclosure not related to the staff's work related duties and appears to have been intentional. The two staff members are no longer employed by the Organization.
Affected individuals	900 Albertans were affected.
Steps taken to reduce risk of harm to individuals	• User accounts used to email the information were immediately disabled. • Protocols were established to reduce the size of emails that can be transmitted outside of the Organization.
Steps taken to notify individuals of the incident	The six employees were notified on April 24, 2014 in person. The clients whose SIN numbers were disclosed were notified via letter the week of May 13, 2014.
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 six employees and the six clients whose SIN numbers were disclosed may be at a risk of identity theft and fraud. In my view, the personal information of the 6 employees and the 6 clients whose social insurance numbers were disclosed is highly sensitive. The types of harm that could result from unauthorized access to the personal and employee information in this instance are identity theft and fraud. In my view, these are significant harms. For the remaining individuals, the personal information disclosed consists of contact information such as email addresses and phone numbers. The types of harm that could be caused as a result of the disclosure of this personal information include unsolicited emails, phone calls or mail and phishing. In my view, 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 it considered there to be a real risk of significant harm to the six employees and the six clients whose SIN numbers were disclosed. However it felt the risk to the remaining individuals was low. In my view, the likelihood of harm resulting from this incident (identity theft and or fraud, phishing) is increased because the personal information was intentionally disclosed and has not been recovered, and the number of affected individuals.

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 involves sensitive identity information, such as social insurance numbers, as well as contact information such as email addresses. This information could be used to cause harm in the form of identity theft and or fraud, and phishing. The likelihood of harm resulting from this incident is increased because the personal information was intentionally disclosed and has not been recovered, and the number of affected individuals. 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 has already notified the employees in person on April 24, 2014 and the clients were notified via letter the week of May 13, 2014 in accordance with the Regulation.

Jill Clayton
Information and Privacy Commissioner