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	Klohn Crippen Berger Ltd. and Pure Canadian Gaming Corp. (Organizations) as reported by Think Relocation Consulting (service provider to the Organizations)
Decision number (file number)	P2018-ND-006 (File #002233)
Date notice received by OIPC	January 27, 2016
Date Organization last provided information	September 28, 2017
Date of decision	January 3, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organizations are 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 Organizations are "organizations" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information involved in this incident included "…names, immigration documents, citizenship documents, immigration application forms, educational certificates, employment documents, bank/financial statements." This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from individuals who were resident in Alberta at the time of collection.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 22, 2015, the home of the Organizations' service provider (Think Relocation) was broken into and a laptop was stolen. • The information at issue was stored on the laptop, which was password protected but not encrypted.

	• The service provider reported there is no evidence indicating that the security of the laptop password has been compromised. The laptop has not been connected to the internet since the incident to enable the remote wipe function. • The laptop has not been recovered. • The incident occurred in British Columbia. It was discovered the same day.
Affected individuals	A total of 200 individuals were affected, including 12 residents of Alberta.
Steps taken to reduce risk of harm to individuals	The service provider: • reported the theft to the Organizations, the RCMP, Immigration Consultants of Canada Regulatory Council, and the BC OIPC. • offered 3 year credit monitoring to the employees of one client organization. • has taken steps to secure information on cloud based services and information sharing applications.
Steps taken to notify individuals of the incident	The service provider reported that affected individuals were notified in by email and in writing the week of January 21, 2016.
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 service provider reported "The most likely harm is identity theft." In my view, the identity documents and numbers, employment and education information, police background checks, and profile information (personal and travel history, family information) is sensitive information that could be used to cause the significant harms of identity theft, fraud, and financial loss.
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 service provider reported "It is unknown how much of the data was viewed, if at all. Given the lack of sophistication in the break-and-enter, it is likely that the time required to review the data and put it to use outweighed the ease of wiping the hard drive and re-selling the computer. The information has not been recovered and the remote wipe does not seem to have been initiated (meaning the computer was never re-connected to the internet). The laptop's serial number was provided to police but has not been recovered." In my view, the likelihood of harm resulting in this case is increased because the incident was the result of malicious intent (theft), the laptop was not encrypted, and has not been recovered. The service provider can only speculate that the perpetrators would wipe the hard drive and re-sell the computer, rather than use the personal information stored on it for identity theft or fraud purposes.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the service provider and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals in this case. The identity documents and numbers, employment and education information, police background checks, and profile information (personal and travel history, family information) is sensitive information that could be used to cause the significant harms of identity theft, fraud, financial loss. The likelihood of harm resulting in this case is increased because the incident was the result of malicious intent (theft), the laptop was not encrypted, and has not been recovered. The service provider can only speculate that the perpetrators would wipe the hard drive and re-sell the computer, rather than use the personal information stored on it for identity theft or fraud purposes. I require the Organizations to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand from the service provider that all affected Albertans were notified of the incident in writing and by email during the week of January 21, 2016. The Organizations are not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner