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	Heyrock Chartered Accountants (Organization)
Decision number (file number)	P2014-ND-55 (File #P2549)
Date notice received by OIPC	December 24, 2013
Date Organization last provided information	April 2, 2014
Date of decision	April 15, 2014
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 a partnership as defined in the *Partnership Act* and is operating in Alberta. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(iv) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved electronic copies of the Organization's clients' personal tax returns and includes the following: • name, • social insurance number, • address, • date of birth, • marital status, • information about spouse or common-law partner and dependents, • residence information, • income information, • investments,

	• pension amounts, • child care, • moving expenses, and • optional banking information (branch number, institution number and account number). This information is "personal information" as defined in section 1(1)(k) of PIPA and the loss of this information occurred in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	
Description of incident	• On December 16, 2013, a back-up drive (USB drive) was stolen from the Organization's office. The USB drive was used to back-up computer data including clients' personal tax returns. • The loss was discovered on December 17, 2013, when the RCMP stopped a stolen vehicle and found the USB drive in the vehicle.
Affected individuals	• 300 clients of the Organization, including 285 Albertans.
Steps taken to reduce risk of harm to individuals	• The USB drive was recovered within 24 hours of the loss. • Canada Revenue Agency was notified about the incident. • Fraud alerts were made to Equifax and TransUnion. • Additional credit monitoring was offered to the clients through Equifax Complete Premier Plan. • Office locks were changed. • Computer passwords were changed.

Steps taken to notify individuals of the incident	• Notifications were sent by email, phone calls, and letters mailed on December 23, 24, and 29, 2013.
	• Written notifications sent in December included:
	  o a description of the circumstances of the loss,
	  o the time period when the loss occurred, and
	  o contact information for a person who can answer questions about the loss.
	• During phone calls clients were made aware that the USB drive contained an electronic back-up copy of their tax returns.
	• In a February 10, 2014 letter, the Organization notified clients that the USB drive "contained an electronic copy of your personal tax return."

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 that the type of harm that may result from the breach is identity theft. In my view, the personal information involved in this case is highly sensitive. It includes the personal tax returns of the Organization's clients which would include client's name, social insurance number, birthdate, address, income level, and in some cases, bank account information. 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 there is a real possibility the information may be used for identity theft. In my view, the likelihood of harm resulting from this incident is increased because the USB drive was not encrypted and was found in a stolen vehicle. The RCMP recovered the USB drive in a relatively short period of time (under 24 hours); however, the Organization could not determine whether the data on the USB drive had been accessed.

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 on personal tax returns, including name, date of birth, social insurance number, and financial information for all affected individuals. The information was not encrypted, stolen from the Organization's premises and recovered from a stolen vehicle, indicating criminal intent. These factors contributed significantly to my decision.

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 notified the clients by emails, phone calls and letters in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner