



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Lake Kennedy McCulloch CPAs (Organization)
Decision number (file number)	P2018-ND-55 (File #005372)
Date notice received by OIPC	April 6, 2017
Date Organization last provided information	January 29, 2018
Date of decision	May 7, 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 the affected individual in Alberta pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (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”	<p>The incident involved all or some of the following information:</p> <ul style="list-style-type: none">• name,• address,• social security number,• direct deposit banking information,• date of birth, and• telephone number. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p> <p>The Organization did not respond to correspondence requesting information about how the Alberta resident’s personal information was collected by the Organization. To the extent the personal information was collected in Alberta, I have jurisdiction in this matter.</p>

DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none"> • On February 11, 2017, the Organization identified a potential data security incident and hired a forensic investigation firm. The firm discovered that the Organization’s information system was hacked on January 30, 2017. • The perpetrator(s) acquired 2015 tax return information for a number of the Organization’s clients. In a small percentage of cases, the information was used to fraudulently file 2016 returns for the purpose of obtaining tax refunds.
Affected individuals	The incident affected 1 Alberta resident.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Immediately contacted various law enforcement agencies including the Internal Revenue Service. • Changed system passwords, including for its accounting and tax software products. • Monitoring the situation and re-examining data privacy and security policies and procedures to find ways to reduce the risk of future data incidents.
Steps taken to notify individuals of the incident	Affected individuals were initially notified by email on February 22, 2017. An updated notice with information about the investigation was sent on April 7, 2017.
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.	<p>The Organization reported that it “... is aware of a small percentage of individuals who have had false tax returns filed in their names. However, the IRS is working with them, along with [the Organization] as needed, to help correct their tax records and ensure they have paid the proper amount of tax and receive the proper refund.”</p> <p>In my view, the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.</p>
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 “...is aware only of action by the hackers to file fraudulent tax returns. Their opportunity has largely been thwarted because [the Organization] acted quickly to coordinate with the IRS. These individuals still have sensitive personal information about these individuals, and there remains, therefore a significant risk that information could be used for other impermissible purposes.”

	<p>In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information has already been used for fraudulent purposes.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>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.</p> <p>The contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, the information has already been used for fraudulent purposes.</p> <p>I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organization initially notified the affected individuals by email on February 22, 2017 and provided an updated notice on April 7, 2017 and in accordance with the Regulation. The Organization is not required to notify the affected individual again.</p>	

Jill Clayton
Information and Privacy Commissioner