



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	H&R Block Canada, Inc. (Organization)
Decision number (file number)	P2017-ND-132 (File #005139)
Date notice received by OIPC	March 6, 2017
Date Organization last provided information	July 20, 2017
Date of decision	September 15, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify these individuals 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,• date of birth,• Social Insurance Number,• account numbers (e.g. student loan),• banking information, and• T4 tax information. <p>This information is about an identifiable individual and her partner, and is "personal information" as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• In April 2016, a client inquired about her 2014 tax file at a local branch office of the Organization.

	<ul style="list-style-type: none"> • The local branch office informed the client that her file could not be located. • The Organization reviewed the office’s storage boxes, but the file was still not located. The Organization is not sure whether the client’s file was lost, inadvertently shredded, destroyed as part of an office clean-up, or misfiled. • The Organization has concluded that the file is not in the local branch office and confirmed the file was not located in any of its subsequent searches of its storage facility and other branch offices. • The Organization informed the client of its search efforts and offered the client credit monitoring services.
Affected individuals	The incident affected 2 Alberta residents (the client and her partner).
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Retrained office staff and managers on privacy procedures. • Offered one year credit monitoring services to the affected individual. • Offered to recreate the file for the affected individual from the Organization’s electronic records.
Steps taken to notify individuals of the incident	In April 2016, the affected individual brought the issue to the Organization and was advised of its search efforts to locate the missing file in February 2017 by email.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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>	<p>The Organization reported that there is “no indication of any actual harm but there is a risk of fraud and identity theft if the file was lost rather than shredded or misfiled.”</p> <p>In my view, the financial and identity information at issue could be used to cause the harms of fraud, identity theft and financial loss. These are significant harms.</p>

<p>Real Risk</p> <p>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.</p>	<p>The Organization reported that “given it was a full individual file from a prior tax year, the file was likely misfiled or shredded as part of the annual document destruction although this file was not yet scheduled for destruction. However, we do not have confirmation of this so the file could have potentially been taken or lost any time after February 2016....We are unaware of any malicious intent....”.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the Organization has not been able to determine what happened to the file. Although the Organization does not believe the information was the target of theft or any malicious intent, and has no knowledge of the information being used or disclosed, it is impossible to know this for sure.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>Based on the information provided by the Organization and given the circumstances, I have decided that there is a real risk of significant harm resulting from this incident.</p> <p>The financial and identity information at issue could be used to cause the harms of fraud, identity theft and financial loss. These are significant harms. The likelihood of harm resulting from this incident is increased because the Organization has not been able to determine what happened to the file. Although the Organization does not believe the information was the target of the theft or any malicious intent, and has no knowledge of the information being used or disclosed, it is impossible to know this for sure.</p> <p>I require the Organization to notify the affected individual and her partner (to the extent the financial and identity information concerns them both) in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the affected individual brought the issue to the Organization’s attention in April 2016 and the Organization followed up with the individual by email in February 1, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individual again; however, I require the Organization to confirm to my office, within 10 days of the date of this decision, that the affected individual’s partner has been notified, if the partner’s financial and identity information is also at issue in this incident.</p>	

Jill Clayton
Information and Privacy Commissioner