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	H & R Block Canada, Inc.
Decision number (file number)	P2018-ND-016 (File #006501)
Date notice received by OIPC	September 7, 2017
Date Organization last provided information	December 4, 2017
Date of decision	January 26, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	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 was involved in this incident: • name, • address, • social insurance number, and • financial information (tax summary). This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• In February 2017, an employee of the Organization gave a tax summary to a client and inadvertently included another client's tax summary. • The Organization discovered the error on April 24, 2017 when the unintended recipient visited the Organization's office and returned the documents.

Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization's Chief Privacy Officer and Regional Director were informed of the incident on April 24, 2017. • The employee responsible for the error had completed privacy and security training prior to the incident. The employee was a pre-season employee who has since left the Organization and will not be rehired. • Staff members at the location of the incident were retrained on privacy practices and precautions. • Privacy training will continue to be a requirement for all employees and conducted each time a seasonal employee is hired/rehired for a tax season.
Steps taken to notify individuals of the incident	The Organization notified the affected individual by telephone and email on April 26, 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.	The Organization reported that "The type of harm that could potentially result from this breach would be fraud, identity theft and possible embarrassment." I agree with the Organization. The identity and financial information at issue could be used to cause the harms of identity theft and fraud. 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 "The risk of harm is unlikely since one paper copy was inadvertantly [sic] given to one individual who returned it once he discovered it in his possession. There was no malicious intent asssociated [sic] with the breach. The breach was attributed to human error not theft and the information has been recovered. The client is aware of the situation and is comfortable that the information has been returned and not used." I agree with the Organization that the risk of harm resulting in this case is mitigated to an extent as the incident did not result from malicious intent, but rather human error, and the unintended recipient returned the information to the Organization. However, the information was out of the Organization's control for approximately 2 months and the Organization did not report steps taken to confirm the information was not used or further disclosed during this time.

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 individual in this case. The identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. The risk of harm is mitigated to an extent as the incident did not result from malicious intent, but rather human error, and the unintended recipient returned the information to the Organization. However, the information was out of the Organization's control for approximately 2 months and the Organization did not report steps taken to confirm the information was not used or further disclosed during this time. The Organization is required to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individual by telephone and email on April 26, 2017.

Jill Clayton
Information and Privacy Commissioner