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. (Organization)
Decision number (file number)	P2017-ND-134 (File #005248)
Date notice received by OIPC	March 16, 2017
Date Organization last provided information	September 8, 2017
Date of decision	October 2, 2017
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • date of birth, • Social Insurance Number, • telephone number, • email address, and • financial information in the form of T4, T4 RIF,T4A and T5 tax slips. 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	• On March 3, 2017, a client filled out a drop off form and provided documents to a local branch office of the Organization.

	• There were multiple tax folders on the reception desk and the employee at the local branch office does not remember what happened to the client's documents. • The client came back to the local branch office with more documents that same day and was informed that the original documents could not be located. • The Organization has not located the client's original documents. • The Organization informed the client and offered the client credit monitoring services.
Affected individuals	The incident affected one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Notified associates that client documents must be kept in locked filing cabinets at all times and only one file should be worked on at any time to eliminate misplacement of documents. • Offered credit monitoring services and identity theft protection to the affected individual.
Steps taken to notify individuals of the incident	The affected individual was notified in person at the time of the incident on March 3, 2017. The Organization contacted the affected individual again by email and telephone on March 6, 2017 and March 10, 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 information could be used to cause "Possible fraud and identity theft". I agree with the Organization. The financial and identity information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. The contact information, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm.
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 "since we do not know what happened to the information we cannot provide an accurate assessment. There is no evidence of malicious intent....The information has never been recovered. There is only one individual affected by the breach and she is a senior." The Organization also said, "the harm could be significant should the information get into the wrong hands but this is speculative since we do not know what happened to the information, It is quite possible that the information went into a shredding bin."

	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 documents and the information has not been recovered. 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.

DECISION UNDER SECTION 37.1(1) OF PIPA

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.

The financial and identity information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. The contact information, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm.

The likelihood of harm resulting from this incident is increased because the Organization has not been able to determine what happened to the documents and the information has not been recovered. 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.

I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individual was notified in person at the time of the incident on March 3, 2017. The Organization contacted the affected individual again by email and telephone on March 6, 2017 and March 10, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner