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	Intuit Canada ULC (Organization)
Decision number (file number)	P2019-ND-119 (File #011112)
Date notice received by OIPC	February 14, 2019
Date Organization last provided information	February 14, 2019
Date of decision	August 1, 2019
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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved T4 Statements which include the following information: • name, • address, • Social Insurance Number, and • financial information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	
Description of incident	• The Organization engaged a local accounting firm to prepare and mail out amended T4 statements. • The mail-out took place on January 4, 2019.

	• On January 10, 2019, the Organization learned that some of the amended T4 statements may have been sent to old mailing addresses. The concern was first identified by an employee who discovered that his amended statement was delivered to his old mailing address.
Affected individuals	The incident affected 106 individuals, including 28 in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified the individuals affected by the misdirected mailing. • Offered free credit monitoring and identity theft protection for 24 months. • Increased scrutiny of vendor and its processes, increased quality assurance efforts to include a manual review of subsequent mailings for this engagement and if sampling is used in the future, an increase in sample size.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on February 14, 2019.
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 "Due to the type of personal information involved, the affected individuals may result in identity theft and fraud." I agree with the Organization's assessment. A reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud.
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 "Each misdirected communication was sent to the correct named individual in a sealed envelope. As of this notice, 30 of the 106 misdirected communications have been returned to us unopened. Furhtermore [sic], the misdirected communication was a result of human error. Due to the afrementioned [sic] reasons, we believe the likelihood of harm to be low." In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is decreased because the breach did not result from malicious action. However, the Organization reported that it only recovered 30 of the 106 misdirected communications. There is a real risk of significant harm to those individuals whose personal information remains unaccounted for.

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. A reasonable person would consider that the financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of identity theft and fraud resulting from this incident is decreased because the breach did not result from malicious action. However, the Organization reported that it only recovered 30 of the 106 misdirected communications. There is a real risk of significant harm to those individuals whose personal information remains unaccounted for. 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 that affected individuals were notified by letter on February 14, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner