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	Global Knowledge Network (Canada) Inc. (Organization)
Decision number (file number)	P2019-ND-113 (File #012549)
Date notice received by OIPC	March 20, 2019
Date Organization last provided information	March 20, 2019
Date of decision	July 26, 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 the individuals whose information was collected in Alberta 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 the following information: • first and last name, • physical address, • fees for services (fees paid to the individual by the Organization during 2018), and • social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On or about February 20, 2019, an employee printed and mailed out T4A forms to course instructors for tax purposes.

	• Each printed page included one individual's T4A form on half of the document and the T4A form of another individual on the other half. Two copies of each printed page were mistakenly mailed to one of the individuals identified within the document. As a result, recipients may have received one or two copies of a document, which included not only their own T4A form, but also the T4A form of one other individual. • The breach was discovered on or about March 1, 2019, when the Organization received several calls from individuals who had received the forms.
Affected individuals	The incident affected 92 individuals, 10 of whom are in Alberta.
Steps taken to reduce risk of harm to individuals	• Offering 12 months credit monitoring services to affected individuals. • Informing all potential unintended recipients to destroy and not circulate the information in question. • Recommending individuals carefully review and monitor their bank accounts, credit cards, and other financial transaction statements and to report any concerns to their financial institutions. • Recommending individuals obtain a free credit report and providing information regarding how to do so. • Informing individuals to contact local police force if they believe they are a victim of identity theft or fraud. • Providing information regarding the Canadian Anti-Fraud Centre. • Identifying a contact person to provide additional information and to answer any potential questions the affected individuals may have. • Implementing additional safeguards to prevent a similar event from occurring in the future. • Provided additional training to staff involved in the T4 process.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 19, 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 possible harms that could result from this incident include "Potential identity theft or fraud". In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the harms of identity theft and fraud. The financial information could be used to cause the harms of hurt, humiliation and embarrassment. These are all 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 "Since the personal information includes Social Insurance Numbers there is a real risk of harm. However, since the information was sent to other instructors of our company (all bound by written confidentiality obligations) we believe the likelihood that the harm will result and that personal information involved will be misused as a result of the incident is low." In my view, a reasonable person would consider that the likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error. Further, given all the unauthorized recipients are other instructors, the likelihood of identity theft and fraud may be reduced. However, for the same reason, the likelihood of hurt, humiliation and embarrassment is increased, due to possible professional/personal relationships. The Organization also reported that it would be informing all potential unintended recipients to destroy and not circulate the information in question, but did not report on whether or not confirmation was received from the unintended recipients.

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 contact and identity information at issue could be used to cause the harms of identity theft and fraud. The financial information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms.

The likelihood of harm is decreased because the breach did not result from malicious intent, but rather human error. Further, given all the unauthorized recipients are other instructors, the likelihood of identity theft and fraud may be reduced. However, for the same reason, the likelihood of hurt, humiliation and embarrassment is increased, due to possible professional/personal relationships. The Organization also reported that it would be informing all potential unintended recipients to destroy and not circulate the information in question, but did not report on whether or not confirmation was received from the unintended recipients.

The Organization is required to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

I understand that affected individuals were notified by letter on March 19, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner