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	Sexauer Ltd. (Organization)
Decision number (file number)	P2016-ND-54 (File #002665)
Date notice received by OIPC	April 1, 2016
Date Organization last provided information	May 30, 2016
Date of decision	August 26, 2016
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 a corporation operating in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • social insurance number, • amount of income earned, • tax withholdings for 2015. This information is about identifiable individuals, and qualifies as "personal information" as defined in section 1(1)(k) of PIPA. Some information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On March 22, 2016, an employee of the Organization received an email that appeared to be from a member of the Organization's senior leadership team. The email requested copies of all 2015 employee T4 forms.

	• The employee responded to the email, including copies of Canada Revenue Agency 2015 T4 forms. The employee's response, however, was sent to an unidentified third party.
Affected individuals	A total of 58 individuals across Canada were affected (49 current employees and 9 former employees). Four (4) of the affected individuals are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified the Vice President, General Counsel & Secretary and Chief Information Office. • Launched an internal investigation and notified law enforcement (via the Canadian Anti-Fraud Centre). • Provided affected individuals with information about how to activate monitoring and/or additional protections available through Canada Revenue Agency, Service Canada, and consumer protection agencies. • Offered identity protection services for one year, at no cost, to the affected individuals. • Conducting a thorough review of its security measures, internal controls, and safeguards and making changes to existing policies and procedures, including training and awareness programs, to help prevent a similar incident in the future.
Steps taken to notify individuals of the incident	Current employees with a valid email address were notified of the incident by email on March 23, 2016. Current employees without an email address and former associates were provided written notification via overnight mail.
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 personal information contained on the 2015 T-4 Forms can be considered sensitive. The types of harms that may result from the criminal misuse of this type of information are financial loss, fraud and possible identity theft." I agree with the Organization's assessment. The personal information involved is sensitive identity and financial information. This information could be used to cause the harms of identity theft, fraud and financial loss. 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 it "believes the notification threshold has been met; however, it also believes that the likelihood of these harms actually occurring has been greatly reduced by the prompt action of the Company…". In my view, there is a real risk of significant harm resulting from this incident. The likelihood of harm is increased because the incident resulted from deliberate action (perpetrator impersonated a senior

	member of the Organization), indicating malicious intent, and the circumstances suggest the information at issue was the target. The Organization acted quickly to notify affected individuals, which will likely help to prevent and detect some types of harm; however, this cannot entirely mitigate the risk that significant harm will result from this incident.

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.

The personal information involved is sensitive identity and financial information. This information could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the incident resulted from deliberate action (perpetrator impersonated a senior member of the Organization), indicating malicious intent, and the circumstances suggest the information at issue was the target. The Organization acted quickly to notify affected individuals, which will likely help to prevent and detect some types of harm; however, this cannot entirely mitigate the risk that significant harm will result from this incident.

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 the Organization notified the affected individuals by email on March 23, 2016 and by overnight mail. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner