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	Lightspeed Technologies, Inc. (Organization)
Decision number (file number)	P2020-ND-056 (File #014960)
Date notice received by OIPC	February 6, 2020
Date Organization last provided information	May 7, 2020
Date of decision	May 28, 2020
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 whose personal 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 located in Newburg, Oregon, USA and 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, and • financial account number. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta from a former employee via email.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 14, 2020, customers of the Organization reported receiving spoofed emails attempting to change the account information used for remitting payment to the Organization.

	• An investigation found that an unauthorized party accessed email accounts at different periods between August 19 and August 22, 2019, and between September 20, 2019 and September 23, 2019. The investigation was not able to conclusively determine which emails or attachments were viewed by the unauthorized party. • On January 14, 2020, the Organization determined that a compromised email or attachment contained the personal information of one Alberta resident, including the individual's name and financial account number.
Affected individuals	The incident affected 33 individuals including one (1) individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Reminded the individual to be vigilant in monitoring credit history. • Implemented additional safeguards and technical security measures to help further protect personal information.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter on February 5, 2020.
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 "There is no indication based on available log data that the information about the Alberta resident was viewed, but we are notifying the individual out of an abundance of caution. If the threat actor did view the information about the Alberta resident it could be used to commit fraud." In my view, a reasonable person would consider that the contact and financial information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. 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 that "The likelihood that harm will result to the Alberta resident is low. The attack was focused on attempting to divert payments owed to [the Organization] by sending fraudulent emails to customers requesting that … payment remittance information be changed. We cannot tell if the information of the Alberta resident was viewed, but out of an abundance of caution, have notified the individual and provided information to mitigate any potential damages that may result from this incident." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (spoofing email) by an unknown third

	party and it appears the personal information may have been used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized party viewed, read, copied, or downloaded the affected individual's personal information.

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.

A reasonable person would consider that the contact and financial information at issue in this case could be used to cause the harms of identity theft, fraud and/or financial loss. These are all significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (spoofing email) by an unknown third party and it appears the personal information may have been used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized party viewed, read, copied, or downloaded the affected individual's personal information.

I require the Organization to notify the affected individual whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual in a letter on February 5, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner