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	Longbow Capital Inc. (Organization)
Decision number (file number)	P2019-ND-121 (File #011225)
Date notice received by OIPC	December 14, 2018
Date Organization last provided information	December 14, 2018
Date of decision	August 1, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify the affected individuals.
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: • name, • mailing address, • email address, • telephone number, and • social insurance numbers, passport number, banking information (in some cases). 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	• On September 11, 2018, an employee completed a fraudulent web-form based on an email which appeared to be from a trusted party. The information provided by the employee allowed a malicious actor to change the email account settings for that employee to activate forwarding of all incoming email.

	• The incident was discovered on December 3, 2018, when an IT consultant identified the unauthorized forwarding email address during a routine review of spam reports.
Affected individuals	The incident affected 9 individuals, including 5 in Alberta.
Steps taken to reduce risk of harm to individuals	• Consulted with an IT security firm to assess the cause and extent of the problem and determine steps to fix the problem. • Will retain an IT firm to review IT security procedures. • Employees will receive updated training regarding phishing and other online scams. • Changed the global email setting to prevent any future email forwarding. • Implementing two factor authentication for changes on all email accounts. • Notified data protection authorities. • Offered credit monitoring services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and email on December 11, 2018
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 the potential harms that might result from this breach include "Identity theft or fraudulent access to investors [sic] bank accounts." I agree with the Organization's assessment. A reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to fraud and identity theft.
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 the likelihood of harm resulting in this case is "Low, because of other safeguards in place." In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (installed email forwarding rule). The email forwarding rule appears to have been in place for almost 3 months.
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 significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to fraud and identity theft. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (installed email forwarding rule). The email forwarding rule appears to have been in place for almost 3 months.

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 individuals were notified by telephone and email on December 11, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner