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	West Coast Reduction Ltd. (Organization)
Decision number (file number)	P2018-ND-091 (File #007014)
Date notice received by OIPC	November 3, 2017
Date Organization last provided information	June 18, 2018
Date of decision	July 27, 2018
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 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 all or some of the following information: • name, • email address, • bank account number, • social insurance number, • driver license number, and • copy of passport. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 23, 2017, a user at the Organization's Head Office received a malicious phishing email from a trading partner correspondent.

	• The Organization understands that the trading partner was tricked into disclosing his email credentials and many or all of his contacts were then sent a copy of a malicious email. • The user who received the email also disclosed their credentials to the sender of the phishing email. Subsequently, one more user with the Organization also entered their credentials. • On October 25, 2017, the Organization's IT department was notified when emails started being issued from the two impacted users to people in their contact lists. • On October 26, 2017, the Organization identified the recipients of the malicious email and sent them a warning.
Affected individuals	The incident affected 308 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Changed passwords for infected accounts. • Scanned for malware and reviewed all mailboxes (i.e. emails) for malicious tampering (i.e. forwarding rules to external mail recipients). • Mined the data to determine the impacted individuals. • Notified active employees, inactive employees and applicants. • Notified the Organization's sister company of the breach and provided the employee letter notification and Equifax subscription for distribution to their employees. • Provided *Identity Theft and Identity Fraud Victim Assistance Guide* to affected individuals. • Offered identity theft and credit monitoring. • Conducted a broad information security awareness program. • Held training across the Organization to provide email awareness training with a focus on protection of personal information and user credentials. • Implementing changes to how personal information is communicated internally and working to eliminate the use of email for personal information. • Working with HR service providers to implement more secure methods for the exchange of information. • Introducing a revised security policy.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and postings on November 3, 2017, November 10, 2017, November 15, 2017 and November 16, 2017.

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 "at a minimum identity theft and fraud are potential harms." I agree with the Organization. The contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. 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 it "believes the stolen credentials were used from outside the country to steal the data in question. With valid credentials, the contents of the email accounts could be accessed in clear text. The information is highy [sic] sensitive and one user's account was exposed from Oct 23 at 14:02 to Oct 25 at approximately 13:00. The information could be used for identity theft or fraud and is now unrecoverable. The number of individuals is under assessment, but is likely in the hundreds." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate action and misdirection of email). Further, the information may have been exposed for almost two days and a relatively large number of individuals were affected.

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 contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate action and misdirection of email). Further, the information may have been exposed for almost two days and a relatively large number of individuals were affected.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals in a letter and a posting on November 3, 2017, November 10, 2017, November 15, 2017 and November 16, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner