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	Talisman Energy Inc. (Organization)
Decision number (file number)	P2015-ND-47 (File #P2610)
Date notice received by OIPC	March 11, 2014
Date Organization last provided information	October 6, 2014
Date of decision	July 24, 2015
Summary of decision	There is a real risk of significant harm to 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 registered to carry on business in Alberta. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information for 9 individuals: • name, • bank account number, and • bank address. The following information was at issue for 11 individuals: • name, bank account number and bank address, and • partial credit card number and expiry date, • home address or home telephone number and, • in one case, a partial passport number on a flight boarding pass.

	The following information was at issue for 6 individuals: • name, bank account number and bank address, and • full credit card number and expiry date. This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• Employees of the Organization are required to submit information and provide supporting documentation to request reimbursement of employment-related expenses by way of wire transfer to an overseas bank account. Employees scan the information into the Organization's SAP system as confidential, which restricts access to a limited number of employees with designated access. • In July 2013, the Organization's Privacy Coordinator was notified that the information at issue was scanned into the system without required access controls. • The Organization conducted an audit and investigation and found that, between January 2012 and July 2013, information for 26 individuals had been uploaded without the proper access controls. • The information at issue may have been accessible to 1,100 of the Organization's employees. The Organization does not have the ability to audit if any of its employees accessed the personal information.
Affected individuals	Twenty six employees were affected.
Steps taken to reduce risk of harm to individuals	• A full review of all wire transfers was undertaken. Documents were re-scanned and properly secured within the SAP system with appropriate coding to ensure limited access to designated individuals. • Affected individuals were offered reimbursement for the cost of a credit protection plan. • The Organization developed and implemented a written procedure for all wire transfer transactions involving personal information to ensure they are properly coded and secured when entered into the accounting system. The Organization will also conduct training for new employees regarding this procedure.

Steps taken to notify individuals of the incident	Individuals identified as having a moderate and real risk of harm as a result of the incident were notified by telephone, email and face-to-face conversation.
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 most of the information at issue was of low to moderate sensitivity and the only information of high sensitivity was the full credit card numbers and expiry date. This information could be used to cause financial loss. The Organization also recognized the information could be used for identity theft purposes. In my view, and consistent with previous decisions issued (P2010-ND-006), name, bank account number, and bank address alone or in combination with additional personal information, is information that could be used to cause identity theft and fraud. Credit card numbers and expiry dates in particular are highly sensitive and could be used for these purposes. In my view, 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 submitted that the likelihood of harm resulting from this incident was low for the following reasons: • There is no evidence the information was accessed for improper purposes. • There is no evidence of malicious intent or theft. • The information was stored in an internal accounting system that is complex and difficult to navigate. • There was no external access to the system. Only employees of the Organization with access to the system could potentially access the information. The Organization's employees are expected to review and understand the Organization's Privacy Policy and are bound by the policy on Business Conduct and Ethics. I agree with the Organization that the above factors reduce the likelihood of harm resulting from this incident. In addition, I note that the likelihood of bank account number being used to commit financial fraud or identity theft is remote, considering that financial institutions have additional controls and processes in place to prevent these harms from occurring. In my view, it would be easier and more likely that credit card numbers and expiry dates would be used for identity theft and fraud purposes. In addition, this sensitive information was exposed for up to 19 months and may have been accessible to

	1,100 of the Organization's employees. The Organization is not able to confirm that the information was not accessed by unauthorized individuals.

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 those affected individuals whose credit card numbers and expiry dates were exposed as a result of this incident.

Name, bank account number, and bank address alone or in combination with additional personal information, is information that could be used to cause identity theft and fraud. Credit card numbers and expiry dates in particular are highly sensitive and could be used for these purposes. In my view, these are significant harms. While it is unlikely that bank account information alone will be used to cause significant harm, there is a real risk that this information in combination with credit card numbers and expiry dates would be used to cause identity theft and fraud. In addition, the information was exposed for up to 19 months and may have been accessible to 1,100 of the Organization's employees. The Organization is not able to confirm that the information was not accessed by unauthorized individuals.

I require the Organization to notify those affected individuals whose credit card numbers and expiry dates were exposed as a result of this incident, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by telephone, email, letter and through face to face conversations. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner