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	Dalmac Oilfield Services Inc. (Organization)
Decision number (file number)	P2017-ND-114 (File #005145)
Date notice received by OIPC	March 10, 2017
Date Organization last provided information	March 10, 2017
Date of decision	August 8, 2017
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 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, • social insurance number (SIN), • address, • date of birth, • telephone number, • pay rate, • direct deposit banking information, and • dates of employment. 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 February 22, 2017, the Organization discovered that key-logger software had been installed on an employee's computer, when the employee signed into the Organization's bank account and noticed unauthorized transactions on the account. • The Organization investigated the incident and found that personal information manually entered on the compromised computer between December 22, 2016 and February 22, 2017 was potentially captured by the malware. • The Organization said that it has no evidence that any personal information was compromised or misused in any manner, but is taking measures to ensure security of the information.
Affected individuals	The incident affected 10 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Wiped and re-imaged all the computers that are high users of sensitive information. • Scanned all computers on system to ensure that there is no malware remaining. • Instructed employees to change their personal and corporate passwords. • Contacted affected employees to alert them of possible information loss. • Offered affected employees free credit monitoring for a year.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 9, 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 the possible harm that might result from this incident include identity theft that "could lead to financial loss and a negative effect on credit." I agree with the Organization. The identity, financial and employment information at issue 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 "the harm is not significant until they (the third party) decide to use the information…As we have taken steps to mitigate the risk of harm to the employees I believe the harm to employees is not significant." However, the Organization also reported that the likelihood of harm is "medium to high" as the "hackers that installed the software on our systems did have the malicious intent to steal information and has already shown that they are trying to use this information for theft."

	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 intrusion and installation of malware), who has already tried to use the information gathered for theft purposes. Further, the information may have been exposed for approximately two 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.

The comprehensive contact, identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud, and financial loss. These are 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 intrusion and installation of malware), who has already tried to use the information gathered for theft purposes. Further, the information may have been exposed for approximately two months.

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 dated March 9, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner