



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Grimes Well Servicing Ltd. (Organization)
Decision number (file number)	P2015-ND-59 (File # 001485)
Date notice received by OIPC	August 26, 2015
Date Organization last provided information	September 22, 2015
Date of decision	October 19, 2015
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 <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	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”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• date of birth,• Social Insurance Number,• driver’s license number and abstract, and• T2200 forms (Canada Revenue Agency form – Declaration of Conditions of Employment, describing the employee’s employment-related expenses not reimbursed by the employer). <p>This information is “personal information” as defined in section 1(1)(k) of PIPA and was collected in Alberta.</p>

DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none"> • An employee of the Organization was the subject of a social engineering attack (phishing). • The employee’s email account was compromised. • Contact information from the employee’s email account was then used by the attacker to send unsolicited and malicious emails to other employees of the Organization in an attempt to gain access to more information. • The incident occurred between August 13 -17, 2015.
Affected individuals	A total of 91 individuals were affected. The majority of these individuals are residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • The password of the compromised account was changed. • The passwords of all administrative staff were also changed. • Employees were educated about the incident. • Each computer involved was monitored to ensure it was not compromised and malicious software was not installed.
Steps taken to notify individuals of the incident	The Organization confirmed on September 22, 2015 that affected individuals have been notified directly.
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.	<p>The Organization recognized that the affected individuals may be at risk of identity theft and fraud.</p> <p>In my view, the personal information involved is sensitive as it contains date of birth, Social Insurance Number, driver’s license number and driving abstract. This information could be used to cause the harms of identity theft and fraud. These are significant harms.</p>
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.	<p>The Organization reported that, due to the sensitivity of the personal information involved, there is a real risk of significant harm to the affected individuals.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because of malicious intent. The attacker used the compromised email account to send unsolicited and malicious emails to other employees.</p>

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 personal information involved sensitive information including date of birth, Social Insurance Number, driver's license number and driving abstract. The information was accessed in an unauthorized manner and with malicious intent.

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 the Organization notified the affected individuals in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner