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	Repsol Oil & Gas Canada Inc. (Organization)
Decision number (file number)	P2019-ND-116 (File #011122)
Date notice received by OIPC	December 7, 2018
Date Organization last provided information	December 7, 2018
Date of decision	July 31, 2019
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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved information in a number of documents and pieces of correspondence, including a Canada Revenue Agency (CRA) Certificate of Coverage, paystubs, correspondence from Sun Life Financial, interoffice mail destined for expatriate employees, and employee benefit claim forms. Some or all of the following information elements were included: • name • home address • social insurance number • citizenship • date of birth • gender • date of hire • signature • employee ID number • name of bank and last 4 digits of account number • pay information • Sun Life account number • pension and/or savings plan information (balance and funds) • name of beneficiary

	• personal bank statements • information related to dental, medical or health claims, including Sun Life member ID number, and information about spouses/dependents, treatment providers and expenses. 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 October 25, 2018 an unknown male gained access to the Organization's Calgary office. The trespasser accessed the mailroom for approximately 2 hours, leaving with a number of envelopes and miscellaneous items. • The incident was discovered the next morning and reported to law enforcement.
Affected individuals	The incident affected 10 individuals.
Steps taken to reduce risk of harm to individuals	• Reported to law enforcement and security. • Interviewed staff to identify any personal information that was in the mailroom and affected individuals. • Modified public office hours. • Enhanced security, including CCTV camera positioning and foot patrol. • Developed a corrective action plan to prevent future breaches. • Communicated an office security awareness bulletin to all employees and will provide training. • Modified mail delivery protocols. • Offered to pay for one (1) year of credit monitoring with a credit agency.
Steps taken to notify individuals of the incident	Affected individuals were notified by email or letter on December 6, 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 that some of the information at issue could be used to cause the harms of "financial fraud or identity theft", and, "…if there was personal identifying information in those documents, or possibly personal embarassment [sic] or humiliation depending on the nature of the document." In my view, a reasonable person would consider that the contact, identity, employment, financial and health/medical information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment.
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 fact that the loss was due to a criminal act (break and enter and theft) means there was a malicious intent. That said, it does not appear that the individuals were targeted, nor is there evidence to suggest that the perpetrator had any relationship with the individuals whose information was, or may have been, compromised. In other words, it appears this was a crime of opportunity/random incident. Further, there were no vulnerable individuals involved.* *CRA Certificates: If the information was copied, the likelihood of harm is high, given that this was a malicious criminal act, contained highly sensitive identifying information which could be used to commit financial fraud or identity theft.* *Pay Stubs: The likelihood of harm is low, despite being a malicious criminal act. There is no sensitive identifiers such as date of birth, SIN, etc. The employee number is specific to [the Organization] and is not useful outside the organization.* *Sun Life Statements: The likelihood of harm is medium, given this was a malicious criminal act. While the documents do not contain a SIN or bank account information, they do contain date of birth, information about beneficiaries and employment information (date of hire), which could be used to try and commit identity theft or financial fraud.* *Sun Life benefit claims: The likelihood of harm is low, despite being a malicious criminal act. This is because the information is not financial in nature, butr [sic] rather health related, so there is no real advantage to a third party in having this information and it is unlikely it would be disclosed/used by the perpetrator.*

	Personal Mail: Likelihood of harm is difficult to assess as thereis [sic] no way to know for certain what type of information may have been compromised. In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because the breach resulted from malicious action (theft). The Organization did not report recovering the information. The likelihood of hurt, humiliation and embarrassment are decreased as it is unlikely there is any personal or professional relationship between the thief and the affected 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 the affected individuals.

A reasonable person would consider that the contact, identity, employment, financial and health/medical information at issue could be used to cause the significant harms of identity theft and fraud, as well as hurt, humiliation and embarrassment.

The likelihood of identity theft and fraud resulting from this incident is increased because the breach resulted from malicious action (theft). The Organization did not report recovering the information. The likelihood of hurt, humiliation and embarrassment are decreased as it is unlikely there is any personal or professional relationship between the thief and the affected individuals.

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 that individuals were notified by email or letter on December 6, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner