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	Raytheon Canada Limited (Organization)
Decision number (file number)	P2020-ND-117 (File #015886)
Date notice received by OIPC	May 5, 2020
Date Organization last provided information	August 31, 2020
Date of decision	October 26, 2020
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 whose personal information was collected 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 about current and former employees: • name, • home address, • date of birth, • Social Insurance Number, • salary and payroll data, • security clearance forms (e.g. criminal history), • residence and employment history, • names of immediate family members, • sort and/or long term disability information (may include health information). In addition, the incident involved the following information about visitors: • name and country of residence, • visit details and existence of a security clearance (if relevant to the visit).

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies to this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 13, 2020, the Organization was notified by a U.S. law enforcement agency of suspicious internet activity. • The Organization confirmed an unauthorized party exploited a vulnerability in a third-party technology it uses for web application delivery control and accessed a server containing personal information between January 11, 2020 to on or about March 27, 2020. • The Organization reported that it cannot conclusively determine whether any data was accessed or exfiltrated, but, out of an abundance of caution, notified impacted individuals and recommended that they act as if their personal data was compromised.
Affected individuals	The incident affected 1,236 individuals of which 439 are residents of Alberta
Steps taken to reduce risk of harm to individuals	• Commenced an investigation. • Taking steps to enhance the security of the impacted systems. • Remediating a vulnerability in the third-party web application technology. • Rebuilding the impacted server. • Changing access permissions. • Resetting user and administrator passwords. • Provided two (2) years of credit monitoring services as well as information about steps individuals can take to protect themselves.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and/or letter on May 20, 2020. The Organization reported that despite contacting services for address updates, there are few people for whom it cannot locate an address.

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: *While [the Organization] has no evidence of actual harm to affected individuals, identity theft is a possible harm that may occur as a result of the breach.* In my view, a reasonable person would consider the contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. Medical/health information could be used to cause the harms of hurt, humiliation, and embarrassment. 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, *While [the Organization] has no evidence of actual harm to affected individuals, it is possible that the personal information of current and former employees could be misused for identity theft purposes. It is less likely that impacted visitors … will suffer harm as a result of this incident, given that the impacted personal information is less sensitive.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unauthorized third party (deliberate intrusion). The Organization reported that it cannot conclusively determine whether any data was accessed or exfiltrated. Further, the information may have been exposed for approximately two and a half (2 ½) 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.

A reasonable person would consider the contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. Medical/health information could be used to cause the harms of hurt, humiliation, and embarrassment. 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 unauthorized third party (deliberate intrusion). The Organization reported that it cannot conclusively determine whether any data was accessed or exfiltrated. Further, the information may have been exposed for approximately two and a half (2 ½) months.

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

It appears from the Organization's report of this incident that most of the affected individuals were notified of the incident on or around May 5, 2020; however, the Organization reported, "Despite contacting services for address updates, there are a few people for whom we cannot locate an address."

Section 19.1(1) of the Regulation states "Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must …be given directly to the individual". However, pursuant to section 19.1 (2), "…where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

Given this, and pursuant to section 37.1(2) of PIPA which states "… the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate…", **I require the Organization to report to my office within ten (10) days of the date of this decision, with a submission considering indirect or substitute notice, and why the Organization believes this would or would not be a reasonable option in this case.**

Jill Clayton
Information and Privacy Commissioner