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	Stuart Olson Inc., and its subsidiary Canem Systems Ltd. (Organization)
Decision number (file number)	P2019-ND-165 (File #013324)
Date notice received by OIPC	May 31, 2019
Date Organization last provided information	May 31, 2019
Date of decision	November 20, 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 all or some of the following information: • name, • home address, • compensation information, • Social Insurance Number, • date of birth, • banking information, • driver's license information, • employment contract, • disciplinary documentation, and • short/long-term disability information. 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 March 10, 2019, the Organization experienced an encrypted ransomware attack that affected access to a majority of the Organization's IT systems and internal servers. The attacker demanded payment of a ransom in exchange for restored access to these systems. • The incident was discovered the same day by staff investigating a help desk ticket related to email performance. • The Organization's investigation has not found any evidence to indicate there was any exfiltration of personal information, however this possibility cannot be conclusively ruled out. • For a brief period of time while the system was being restored, files containing employee personal information did not have the proper access restrictions in place. This vulnerability was corrected within an hour of the issue being discovered. • The systems were restored from March 11, 2019 - March 27, 2019.
Affected individuals	The incident affected approximately 2,725 employees.
Steps taken to reduce risk of harm to individuals	• Immediately disabled all systems, which were shut down within 4 hours of the initial report. • Re-building the entire IT architecture in a new environment and restoring from backups. • Engaging third-party forensic IT consultants to complete vulnerability scans of the restored systems and identify corrective actions. • Undertaking a comprehensive internal investigation to determine the scope and impact of the incident. • Engaged external legal counsel and third-party forensic IT consultants. • Reviewing and updating security and cybersecurity measures. • Reviewing and assessing cybersecurity and privacy policies and procedures. • Purchasing credit monitoring and identity theft protection for the affected employees for a period of twelve months.
Steps taken to notify individuals of the incident	Affected individuals were initially notified by email on March 13, 2019. Two additional notifications were provided to the affected individuals by email on May 14, 2019 and through regular mail during the week of May 20, 2019.
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	The Organization reported: *… if the personal information were to have been ex-filtrated (which appears unlikely at this time), there is a risk of identity theft, fraud and financial loss to the employees in*

also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	*question in addition to a risk of humiliation and embarrassment by having employment compensation information, disciplinary documentation, and disability information potentially disclosed.* *The potential harms of identity theft/fraud, embarrassment, humiliation and embarrassment; assuming they occur, are significant.* In my view, a reasonable person would consider the contact, identity, employment, financial and health information potentially at risk 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 likelihood that harm could result to … employees affected by the Incident is moderate to low. An extensive forensic review has not identified any evidence that personal information was ex-filtrated from [the Organization's] systems as a result of the Incident and thus not accessed, disclosed or disseminated.* *However, the personal information involved in the Incident is highly sensitive and, if ex-filtrated and/or accessed (which cannot be conclusively ruled out), could be used to conduct harm against affected individuals. The fact that the Incident was caused as a result of a ransomware attack gives some indication that the purpose of the attack was not to steal data, however, the fact that there was access means that harm could result to the affected individuals.* *Furthermore, when restoring … systems, certain personal information of employees was accessible to a limited number of other … employees for less than one hour.* I agree with the Organization's assessment. A reasonable person would consider that 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 action, ransom demand). Although the Organization reported it "has not identified any evidence that personal information was ex-filtrated", this cannot be ruled out.
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, employment, financial and health information potentially at risk could be used to cause the significant harms of identity theft, and fraud, as well as hurt, humiliation and embarrassment. 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 action, ransom demand). Although the Organization reported it "has not identified any evidence that personal information was ex-filtrated", this cannot be ruled out.

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 affected individuals were notified by email on March 13, 2019 and again on May 14, 2019, and through regular mail during the week of May 20, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner