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	SNC-Lavalin Inc. (Organization)
Decision number (file number)	P2019-ND-197 (File #013223)
Date notice received by OIPC	September 16, 2019
Date Organization last provided information	September 16, 2019
Date of decision	December 16, 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 the 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 information at issue includes: • name, • date of birth, • employment information such as department, business sector, office worked in, etc. • address, • personal contact details, • emergency contacts, • substance misuse assessment applications, • bank account information, • government identification including passports, drivers licence, national ID cards, settlement documentation and social insurance numbers. The Organization said "This information is stored securely within our HR systems however some of this information has appeared as attachments within the mailbox as part of the employees HR role. For a proportion of the individuals affected there is information that is much more limited and less likely to pose a real risk of significant harm".

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 3, 2019, the Organization discovered that an unknown and unauthorized third party had tried accessing user accounts on August 19, August 27 and September 3, and had gained access to the mailbox of one employee, which contained personal information. • The Organization reported "Although we cannot be completely certain that the content of the mailbox has been duplicated or exfiltrated, the attacker had the time and the means to do it". • The breach was discovered on September 3, 2019 when staff detected an unknown threat actor.
Affected individuals	The incident affected approximately 5,000 individuals, including approximately 250 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Conducted an investigation, including manually reviewing the compromised mailbox. • Required employees to change passwords. • Immediately blocked the IP addresses of the attacker and commenced forensic analysis to ascertain the impact. • Advised staff to take extra measures to protect their accounts. Strengthened MFA protocols. • Expedited in-flight security projects. • Conducted a full audit of all user passwords. • Reviewed response to the incident and established future plans to ensure continually improving security measures. • Planned review to assess how users classify, protect and exchange information, incident management and reporting. • Will undertake a full review of data protection controls and incorporate automated checks on the quality of passwords. • Reviewing policies and processes around mailboxes. • Posted a notice on website. • Offered identity theft insurance and credit monitoring services to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and email on September 18, 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 also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported "For individuals who have had background check, onboarding or other more detailed HR information compromised there is a possible risk of significant harm. This could be in the form of potential embarrassment, identify theft, fraud and email phishing attacks". In my view, a reasonable person would consider that the contact, identity, employment and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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: *Analysis of the affected mailbox and file cannot conclusively state that the information including any personal inforamtion [sic] was definitively compromised. Although we cannot be completely certain that the content of the mailbox has been duplicated or exfiltrated, the attacker had the time and the means to do it. We are working on the basis that it is likely this information is compromised…* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action) and the Organization cannot be certain that the personal information was not exfiltrated.

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 and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action) and the Organization cannot be certain that the personal information was not exfiltrated.

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).

I understand individuals were notified by letter and email on September 18, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner