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	Leduc Mechanical Industries Inc. (Organization)
Decision number (file number)	P2021-ND-037 (File #016505)
Date notice received by OIPC	July 24, 2020
Date Organization last provided information	December 8, 2020
Date of decision	February 23, 2021
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 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 the following information: • name, • address, • date of birth, and • social insurance number. 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	• The Organization was switching its in-house accounting/bookkeeping products and needed to migrate data to the new platform. • The Organization engaged an individual to provide technical support, believing the individual was associated with the accounting software company.

	• The individual was granted remote computer access and uploaded an accounting file containing the information at issue. The individual was also given the account number for the online bookkeeping account, but was not given the password. • Immediately after the file was uploaded, the individual "demanded a large sum of money in exchange for "fixing" supposed errors with the data". • The Organization contacted the software company and confirmed the individual was not a legitimate employee. • No funds were paid to the imposter. However, the imposter is now in possession of the Organization's accounting information. • The breach occurred on July 22, 2020 and was discovered the same day.
Affected individuals	The incident affected fourteen (14) individuals.
Steps taken to reduce risk of harm to individuals	• Closed the online account and stopped any attempt to migrate the data from the desktop software to the online account. • Obtained legal services. • Engaged IT services to scan for possible malware. • Scanned the computer and adjusted firewall settings to prevent further or future damage. • Will not enter employee information other than name in the accounting software and will remove date of birth, SIN and address information. • Will make lists of secure, legitimate technical support staff and post in the office for quick and easy access. • Advised affected individuals to mitigate and monitor for possible fraudulent activity. • Offered one (1) year of credit monitoring to affected individuals.
Steps taken to notify individuals of the incident	The affected individuals were all notified by letter on or about August 12, 2020 with the exception of one individual.
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 the possible harm that may occur as a result of the breach is "Identity Theft" In my view, a reasonable person would consider that the contact and identity 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, *Of the 14 individuals compromised:* *2 had name and SIN compromised.* *4 had Name and birth date only compromised* *4 had name, SIN and birthdate compromised* *4 Had Name, SIN address and birthdate compromised* *We assume that the 4 individuals who had their names, SIN, address and birthdate compromised are the most at risk for identity theft.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate action, impersonation) and the information is still in the possession of the perpetrator.

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 and identity 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 appears to be the result of malicious intent (deliberate action, impersonation) and the information is still in the possession of the perpetrator.

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

The Organization reported that it notified all of the affected individuals on or around August 12, 2020; however, the Organization reported that for one affected individual, "we are unaware of his location status".

Section 37.1(1) of PIPA says "Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner *may* require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure" [emphasis added].

In this case, the Organization provided my Office with a submission as to why direct notice is not possible for one individual, and why indirect or substitute notice is not a reasonable option. I accept the Organization's submission and the Organization is not required to notify the one affected individual for whom the Organization is "unaware of his location status".

The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner