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	United Food and Commercial Workers Local 401 (Organization)
Decision number (file number)	P2020-ND-121 (File #012652)
Date notice received by OIPC	July 4, 2019
Date Organization last provided information	July 10, 2019
Date of decision	October 28, 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 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: • name, • address, • date of birth, • social insurance number, and • medical 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 June 7, 2019, a staff member's laptop was stolen from his vehicle. He reported it missing on June 8, 2019. • The laptop was a temporary replacement laptop and lacked the usual security protocols (full volume encryption) that are installed on laptops used by the Organization.

	• The laptop was protected by a strong password. • The Organization reported that no documents or personal information were locally stored on the device. Everything was accessed through email and a remote access drive. • Microsoft Outlook was installed on the laptop which provides access to six months' worth of staff members' email. • The Organization reported that the person who stole the laptop would have to log in using the staff member's credentials.
Affected individuals	The incident affected approximately 127 individuals.
Steps taken to reduce risk of harm to individuals	• Reported the theft to the police. • Changed the login passwords (password) as soon as IT personnel were informed. • Upgraded the operating system. • Installation of full volume encryption software to protect data stored locally. • Access by staff to a password-protected VPN connection, in order to prevent local storage of personal information on devices. • No longer allowed to remove temporary laptops from secure facilities at the Organization's offices. • Use of Webmail on temporary/replacement to prevent storing data locally on the device. • Reset all Organization-issued mobile devices passwords and increased the minimum password requirement. • Exploring the use of software on its mobile devices that allow remote locking and data wiping. • Increased security protocols in other areas unrelated to electronic access. • Incorporate privacy standard and appropriate handling of personal information into its next training session.
Steps taken to notify individuals of the incident	The Organization advised it planned to notify affected individuals and provided a draft notice for review.
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 the possible harm that may occur as a result of the breach is "possible identity theft and fraud." 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. Medical information could be use to cause the significant harms of embarrassment and humiliation.

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 that, "The personal information is sensitive. It is unknown who could have access to this information or how many persons the information was exposed to. The only security measure in place to prevent access to the laptop's contents is a windows log-in name and password. The information is potentially exposed for an unknown period of time. There is no evidence of malicious intent to purposely acquire the information. The information was not recovered…Given the nature of personal vehicles being broken into and that valuables such as laptops are commonly taken for their resale value, the [Organization] is of the opinion that there is a reasonable basis to believe that the electronic information is sufficiently secure to prevent personal information from being accessed by a person not authorized to access the information." In my view, the likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the laptop has not been recovered. The Organization can only speculate as to the intentions of the individual(s) who stole the laptop. Although there was a strong password used, encryption software was not installed on the laptop.

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. Medical information could be use to cause the significant harms of embarrassment and humiliation. The likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft) and the laptop has not been recovered. The Organization can only speculate as to the intentions of the individual(s) who stole the laptop. Although there was a strong password used, encryption software was not installed on the laptop.

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) **and confirm to my office in writing within ten (10) days of the date of this decision that it has done so.**

Jill Clayton
Information and Privacy Commissioner