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 Nurses of Alberta (Organization)
Decision number (file number)	P2018-ND-103 (File #009338)
Date notice received by OIPC	July 30, 2018
Date Organization last provided information	July 30, 2018
Date of decision	August 7, 2018
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 Organization reported "The information involved was a mixture of personal information and business information of members." The desktop and the external drive contained documents with the following information: • TD1 forms (first name and initials, last name, date of birth, employee number, address, postal code, and social insurance number), • void cheques (name, address and bank account number), • seniority lists (names, employment sites/units, full time equivalency, status, seniority date), and • membership lists (employee number, name, home telephone number, work telephone number, and address of the member). 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 July 22, 2018, an unknown individual broke into the Organization's locked office in Red Deer and stole a desktop computer, back-up drive, and a password book. • The incident was discovered on July 22, 2018 after the building's security alarm went off and RCMP was dispatched. • The desktop computer was encrypted and password-protected and part of the Organization's disablement system. Once the desktop "pinged" on Sunday, July 22, 2018, the Organization was able to disable the computer, scrub the information on the computer, and render it useless. • There was no password protection on the external hard drive and it was not part of the Organization's disablement system. The Organization reported that the banking and SIN information and membership/seniority lists that were saved as a PDF to the desktop and backed up on the external drive would likely be available to the thief.
Affected individuals	The Organization reported approximately 1900 individuals may have been affected, including 17 individuals whose identity and/or banking information was compromised.
Steps taken to reduce risk of harm to individuals	• When the desktop computer was turned on, the Organization was unable to determine its location, but was able to disable the desktop remotely and scrub information from the desktop. The Organization cannot be sure this was the first time the desktop was turned on after it was stolen, however, and cannot be sure steps taken were sufficient to prevent a compromise of information on the desktop. • Reviewed records to determine the identity of the individuals whose personal information may have been stolen. • Prior to the theft, the Organization was in the process of updating its privacy policy and procedures and had anticipated providing training sessions for staff and locals. The Organization plans to take pro-active steps to mitigate risks in the future and will use this incident as a learning opportunity for staff.
Steps taken to notify individuals of the incident	The Organization reported that it was in the process of drafting notification letters to the 17 individuals whose identity and banking information was potentially compromised and would notify no later than July 30, 2018.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 information that was most likely compromised was the personal information found in the TD1 forms and void cheques that were saved as PDF files to the desktop itself and backed up on the external hard drive. The type of harm that could be caused by the compromise of this personal information includes fraud, identity theft, and negative effects on the person's credit record. There is a small chance of financial loss, but as there were no credit card numbers involved, we see this type of harm as less likely than identity theft." I agree with the Organization's assessment. Identity and financial information could be used to cause the significant harms of identity theft, fraud and negative effects on a credit record. Information included on seniority lists/membership lists could be used to make unwanted contact, but is less likely to be used to cause any significant harm.
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 "We are most concerned because the information was compromised by a break and enter and theft, so there is evidence of malicious intent." Further, "The risk of identity theft or fraud, using the compromised SIN numbers and bank account information would be much higher. The risk will depend on the sophistication of the criminal who stole the equipment, and whether they intend to perpetuate crimes such as identity theft and fraud, or whether this was a crime committed just to obtain some stolen hardware." The Organization also said that "Although [the Organization] had the desktop computer encrypted and password protected, and it was disabled on the same day as the theft, the external hard drive was not protected. The information on the hard drive remains exposed (not recovered) and could be used for criminal purposes." In my view, there is a real risk of harm resulting from this incident. The breach was the result of malicious intent (deliberate break-in and theft). It appears the information has not been recovered.

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 as a result of this incident.

Identity and financial information could be used to cause the significant harms of identity theft, fraud and negative effects on a credit record. Information included on seniority lists/membership lists could be used to make unwanted contact, but is less likely to be used to cause any significant harm. The breach was the result of malicious intent (deliberate break-in and theft). It appears the information has not been recovered.

I require the Organization to notify the affected individuals whose identity and banking information was potentially compromised, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation), and **confirm to my office in writing, within 10 days of the date of this decision, that this has been done.**

Jill Clayton
Information and Privacy Commissioner