



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	New Arlington Realty Inc. (Organization)
Decision number (file number)	P2021-ND-231 (File #018301)
Date notice received by OIPC	November 20, 2020
Date Organization last provided information	August 18, 2021
Date of decision	November 15, 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 those individuals whose personal information was collected in Alberta pursuant to section 37.1 of <i>the Personal Information Protection Act</i> (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”	<p>The incident “included personal data elements included in T4, which include[s]”:</p> <ul style="list-style-type: none">• name,• address,• social insurance number,• employment information, including salary information. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On or about November 11, 2020, a workstation and user account was compromised by an unauthorized third party, enabling a threat actor to access the Organization’s network.

	<ul style="list-style-type: none"> On November 14, 2020, after ransomware had been deployed on the network, the Organization’s Information Technology (IT) provider discovered the breach. A ransom note was also found. Further investigation found that the compromised workstation and user account had authorizations and administrative access beyond what was necessary.
Affected individuals	The incident affected 20 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Recovered systems from backup. Improved processes governing backups to ensure they occur, and are secure. Implemented a backup restoration verification process. Transitioned some services to the cloud. Exploring the use of two-factor authentication. Adopted practice of encrypting private data. Adopted new policies pertaining to use and security of workstations. Adopted practice of periodically requiring password resets. Considering the adoption of stronger password requirements. Eliminated improper authorizations and administrative access of affected user account. Reviewing website and public platforms to ensure “email addresses and other personal information” are not visible. Implemented staff awareness training on how to prevent breaches. Encouraging staff to undergo IT training. Offered credit protection plans to affected individuals. Notified police.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on November 20, 2020.
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.	<p>The Organization reported that “Personal information could be used for identity theft and personal gain.”</p> <p>In my view, a reasonable person would consider that the contact, identity, and employment information at issue could be used to cause the significant harms of identity theft and fraud.</p>

<p>Real Risk</p> <p>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.</p>	<p>The Organization reported that the “Likelihood is low as their main objective is for ransomware payment.”</p> <p>However, the Organization also reported implementing new safeguards including “encrypt[ing] personnel data in word and excel.”</p> <p>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, deployment of ransomware, demand of ransom payment). The Organization’s report did not rule out the possibility that personal information was accessed or exfiltrated. Further, personal information may not have been stored in an encrypted manner, increasing the likelihood that personal information was accessed without authorization.</p>
---	--

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, and employment 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 because the personal information was compromised due to the malicious action of a third party (deliberate intrusion, deployment of ransomware, demand of ransom payment). The Organization’s report did not rule out the possibility that personal information was accessed or exfiltrated. Further, personal information may not have been stored in an encrypted manner, increasing the likelihood that personal information was accessed without authorization.

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 the Organization notified affected individuals by email on November 20, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner