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** | Brookfield Residential Properties Inc. (Organization) |
| **Decision number (file number)** | P2021-ND-040 (File #017171) |
| **Date notice received by OIPC** | September 2, 2020 |
| **Date Organization last provided information** | February 22, 2021 |
| **Date of decision** | March 2, 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 *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:<br><u>Employee cohort:</u><br>• name,<br>• mailing address,<br>• email address,<br>• date of birth,<br>• gender,<br>• marital status,<br>• social insurance number,<br>• driver's licence,<br>• passport,<br>• bank account numbers,<br>• doctor's notes,<br>• requests for medical leave,<br>• WCB information,<br>• personal health numbers,<br>• benefits and insurance information,<br>• beneficiary names,<br>• beneficiary date of birth,<br>• dependent names, |

| | |
|---|---|
| | • dependent date of birth,<br>• job title,<br>• employee ID number,<br>• compensation,<br>• performance reviews, and<br>• trade union information.<br><br><u>Former employee cohort:</u><br>• name,<br>• mailing address,<br>• email address,<br>• date of birth,<br>• marital status,<br>• social insurance number,<br>• driver’s licence,<br>• bank account numbers,<br>• health information,<br>• job title,<br>• employee ID number,<br>• compensation,<br>• performance reviews, and<br>• trade union information.<br><br>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. Some of the personal information was collected in Alberta. |
| **DESCRIPTION OF INCIDENT** | |
| □ loss ☒ unauthorized access □ unauthorized disclosure | |
| **Description of incident** | • On or about July 1, 2020, an email phishing attack was carried out against a former employee who was working for the Organization in a consulting capacity. As a result of the attack, a threat actor gained unauthorized access to the Organization’s network(s).<br>• On or about July 31, 2020, the threat actor gained access to the Organization’s servers and domain controller.<br>• The incident was discovered on August 9, 2020 when IT staff found malicious text files with links to a website demanding ransom payment, in exchange for a decryption key and deletion of affected files.<br>• Between discovery of the incident on August 9, 2020 and September 9, 2020, the Organization investigated the credibility and claims of the threat actor.<br>• Amid the Organization’s investigation, the attacker threatened to disclose a portion of the records. Between August 16, 2020 |

| | |
|---|---|
| | and August 19, 2020, the threat actor proceeded to publish blocks of exfiltrated data to the dark web.<br>• The Organization downloaded the records on August 20, 2020 and began analyzing the dataset to determine what data elements were impacted. Their analysis concluded on September 9, 2020, approximately 70 days after the suspected date of initial breach on July 1, 2020.<br>• On February 22, 2021, the Organization reported that the personal information remains on the dark web despite efforts, with law enforcement, to remove them from public availability. |
| **Affected individuals** | The incident affected 391 individuals, including 355 whose information was collected in Alberta.<br>The number of affected beneficiaries and dependents was not reported by the Organization. |
| **Steps taken to reduce risk of harm to individuals** | • Shut down servers and disabled network ports to prevent unauthorized users from accessing the network.<br>• Terminated all user access and reset credentials.<br>• Verified user identity prior to restoring access.<br>• Strengthened password requirements.<br>• Engaged internal and external forensic and cybersecurity experts to assist in breach investigation, response, and remediation.<br>• Deployed additional security and threat detection products, services, and countermeasures, to analyze breach and decrease future likelihood of unauthorized access.<br>• Removed malicious code, blocked malicious IP addresses, disabled unauthorized remote access tools.<br>• Removed admin privileges from all computers, and requiring IT approval prior to software installation.<br>• Deployed an educational program to prevent fraud and phishing attacks in the future, including communicating privacy and cyber hygiene ‘best practices’ to all employees.<br>• Reviewing, updating, and creating new security protocols to mitigate future threats.<br>• Creating backup and redundancy protocols to enable timely restoration of data in a secure manner.<br>• Deployed multi-factor authentication for remote connections.<br>• Reviewing and considering additional steps and initiatives to further reduce risk of reoccurrence in the future.<br>• Engaged credit bureaus for identity theft protection and credit monitoring services for affected individuals.<br>• Notified law enforcement.<br>• Notified Union whose members were impacted. |

| | |
|---|---|
| | - Ongoing dark web monitoring. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by email and / or letter on August 28, 2020, September 1, 2020, and October 1, 2020.<br>Beneficiaries and dependents whose personal information was affected were not notified. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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:<br>*The contact, identity and bank information accessed and disclosed as a result of the breach may be used for fraud and/or identity theft and/or financial loss.*<br>Regarding beneficiaries and dependents, when prompted, the Organization reported:<br>*[The] limited beneficiary/dependent information that was exfiltrated (name and, in some cases, date of birth), did not alone create a "real risk of significant harm" to the employees. The harm of identity theft to the affected employees, which is the likely harm that could result, is low with this category of information.*<br>*The beneficiary/dependent information is limited to only the name of the beneficiary and, in some (but not all cases) their date of birth … the risk is potential identity theft.*<br>In my view, a reasonable person would consider that the contact, identity (including date of birth of beneficiaries and dependents), financial, health and employment information at issue could be used for the purposes of identity theft, and fraud. Health information at issue could also be used for the purposes of embarrassment, hurt or humiliation. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms. |
| **Real Risk**<br>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:<br>*Based on the method used to access [the Organization's] system, the type of information that was obtained and disclosed, and the disclosure of the data on the dark web, there is a likelihood that fraud, identity theft or financial loss could result.* |

Regarding beneficiaries, when prompted, the Organization reported:

> *"The "beneficiary/dependent name and date of birth" were not included as types of information affected in the August 28, 2020 notification letters to current employees, as this data category was not known to [the Organization] at the time the notification letter was sent."*
>
> *"[The] limited beneficiary/dependent information that was exfiltrated (name and, in some cases, date of birth), did not alone create a "real risk of significant harm" to the employees. The harm of identity theft to the affected employees, which is the likely harm that could result, is low with this category of information."*
>
> *"The beneficiary/dependent information is limited to only the name of the beneficiary and, in some (but not all cases) their date of birth. [The Organization] did not notify the beneficiaries/dependants that their personal information was impacted because, in its view, the very limited information that was exfiltrated does not carry a "real risk of significant harm" to those individuals. This type of data alone, without more, is unlikely to pose a "real risk of significant harm" to those individuals. Again, the risk is potential identity theft."*

The Organization also stated:

> *"Unfortunately, the exfiltrated records remain available on the [threat actor's dedicated leak site]"*
>
> *"[It] is very difficult to locate this information at all, and even more difficult within the larger data set. The records are not publicly indexed by any search engines and are not easily accessible by the public or by any conventional means, and requires specialized knowledge and tools to locate, access, and download"*
>
> *"To date, [the Organization] is not aware of any harm to affected individuals linked to this cybersecurity breach."*

In my view, a reasonable person would consider that 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, who made a ransom demand and intentionally released personal information.

| | |
|---|---|
| | The information remains exposed on the dark web. A lack of reported harm, and the requirement of “specialized knowledge and tools to locate, access, and download” the affected personal information from the dark web, does not effectively mitigate against the possibility of harms occurring in the future. |

## 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 (including date of birth of beneficiaries and dependents), financial, health and employment information at issue could be used for the purposes of identity theft, and fraud. Health information at issue could also be used for the purposes of embarrassment, hurt or humiliation. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

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, who made a ransom demand and intentionally released personal information.

The information remains exposed on the dark web. A lack of reported harm, and the requirement of “specialized knowledge and tools to locate, access, and download” the affected personal information from the dark web, does not effectively mitigate against the possibility of harms occurring in the future.

I understand the Organization notified affected individuals by email and / or letter on August 28, 2020, September 1, 2020, and October 1, 2020. However, I also understand that notification letters did not indicate beneficiary/dependent names and dates of birth as types of information affected. Further, beneficiaries were not notified, as the Organization assessed there to be no real risk of significant harm to those individuals, nor does the Organization have the means “to contact these individuals directly."

**To the extent notifications to affected individuals did not indicate beneficiary and dependent names and dates of birth were impacted, I require the Organization to notify those affected individuals again in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation), and to confirm to my Office within ten (10) days of the date of this decision, that affected individuals have been notified.**

Jill Clayton
Information and Privacy Commissioner