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** | First National Financial LP (Organization) |
| **Decision number (file number)** | P2020-ND-014 (File #013723) |
| **Date notice received by OIPC** | October 9, 2019 |
| **Date Organization last provided information** | October 9, 2019 |
| **Date of decision** | February 13, 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 the 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 information at issue includes:<br><br>• name,<br>• address,<br>• date of birth,<br>• email address,<br>• telephone number,<br>• pre-authorized debit form (with banking information for mortgage payments),<br>• government issued identification provided to the individual's solicitor (i.e. passport, driver's license or citizenship documentation).<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| **Description of incident** | • The account credentials of an employee of the Organization were compromised during a credential harvesting phishing attack against the employee on August 26, 2019.<br>• These credentials were used by an unidentified party to gain unauthorized access to the employee's mailbox between August 30, 2019 and September 17, 2019.<br>• The unidentified third party had access to customer data contained within the email mailbox. There is no evidence the data was actually accessed or exfiltrated but this cannot be ruled out.<br>• The unauthorized access was first detected on September 17, 2019 when external contacts advised the employee about phishing emails sent by the unidentified third party from the employee's email account. |
| **Affected individuals** | The incident affected 224 individuals. |
| **Steps taken to reduce risk of harm to individuals** | • Disabled the affected account, reset password and investigated with assistance from third party information security expert.<br>• Sent two internal all-staff communications that included best practices and tips<br>• Flagged all potentially impacted accounts for escalated due diligence.<br>• Established a dedicated call centre line and email address to receive inquiries from affected individuals.<br>• Provided two years of credit monitoring and identity theft services, at no cost to affected individuals.<br>• Reviewing applicable policies and protocols and, where necessary, considering appropriate enhancements.<br>• Have or will be conducting an internal debrief of the incident.<br>• Will enhance policy and employee training for information technology and information security.<br>• Performed a self-assessment on additional security measures to mitigate similar risks. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on October 3 and 7, 2019. |
| **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 | The Organization did not specifically assess the likelihood of harm resulting from this incident but its notification to affected individuals said:<br><br>*We also encourage you to monitor your accounts with financial institutions and be alert to any requests for personal information, in particular financial information,* |

| | |
|---|---|
| non-trivial consequences or effects. | *account numbers or passwords. Always verify the identity of the requester. Generally, you can monitor for signs of fraud by requesting a free credit report from each of the two major credit reporting agencies.*<br><br>In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, 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 did not specifically assess the likelihood of harm resulting from this incident.<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (deliberate action, phishing attack). Information in the mailbox was exposed for more than 2 weeks. The Organization reported "There is no evidence the data was actually accessed or exfiltrated but this cannot be ruled out". |

**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 financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (deliberate action, phishing attack). Information in the mailbox was exposed for more than 2 weeks. The Organization reported "There is no evidence the data was actually accessed or exfiltrated but this cannot be ruled out".

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 individuals were notified by letter on October 3 and 7, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner