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** | North American Title Company (Organization) |
| **Decision number (file number)** | P2019-ND-145 (File #005641) |
| **Date notice received by OIPC** | May 19, 2017 |
| **Date Organization last provided information** | November 8, 2017 |
| **Date of decision** | August 19, 2019 |
| **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:<br><br>• name,<br>• passport number,<br>• mortgage loan number,<br>• bank account number, and<br>• bank account routing number.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via the affected individuals' mortgage lender. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| **Description of incident** | • On May 5, 2017, the Organization's chief security officer received a spam email from another employee's email.<br>• The Organization investigated and determined that a phishing incident occurred and that there was potential unauthorized access to information contained within an employee's emails.<br>• The unauthorized third party may have had access to the employee's email account from February 9, 2017 to February 15, 2017 and used the account to send spam emails.<br>• Although the Organization did not find that the unauthorized third party actually obtained this information or used it for improper purposes, the third party did have access to the employee's email account during the time indicated above. |
| **Affected individuals** | The incident affected 2 Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Immediately disabled access to the mailbox.<br>• Enhancing existing security measures relating to protecting sensitive information.<br>• Providing additional training to employees related to phishing incidents. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by letter on May 19, 2017. |
| **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 did not identify any specific harm that might result from this incident but reported that it is "providing one year of credit monitoring and identity theft protection" to affected individuals.<br><br>In my view, a reasonable person would consider the identity and financial information at issue could be used for identity theft and fraud purposes. 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 that it "has no indication that any unauthorized individuals… accessed or acquired the information contained in the employee's email account."<br><br>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 an unknown third party (deliberate intrusion). Although the Organization reported it has no indication unauthorized individuals accessed or acquired information in the account, the Organization did report the account was exposed for approximately one (1) week and the Organization did not provide any evidence, such as |

| | |
|---|---|
| | audit logs, to suggest the unauthorized individual did not access or acquire information. |

**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 the identity and financial information at issue could be used for identity theft and fraud purposes. 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 an unknown third party (deliberate intrusion). Although the Organization reported it has no indication unauthorized individuals accessed or acquired information in the account, the Organization did report the account was exposed for approximately one (1) week and the Organization did not provide any evidence, such as audit logs, to suggest the unauthorized individual did not access or acquire information.

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 in a letter dated May 19, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner