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** | Financeit Canada (Organization) |
| **Decision number (file number)** | P2019-ND-155 (File #013122) |
| **Date notice received by OIPC** | September 5, 2019 |
| **Date Organization last provided information** | September 18, 2019 |
| **Date of decision** | October 23, 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 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 the following information:<br>• name,<br>• address,<br>• postal code,<br>• telephone number,<br>• email address,<br>• date of birth, and<br>• monthly income.<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 personal information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss | ☒ unauthorized access ❑ unauthorized disclosure |
| **Description of incident** | • On August 26 and 27, 2019, an unauthorized third party accessed the Organization's systems. |

| | |
|---|---|
| | • The Organization investigated and determined a hacker logged into a merchant account on the Organization's platform using valid login credentials.<br>• The hacker was able to exploit a vulnerability allowing them to gain access to personal information relating to loan applications for other merchants. The hacker did this by creating a script to export the personal information from the platform through a non-public application programming interface (API). This API was the source of the vulnerability.<br>• It is not known how the hacker came to be in possession of valid credentials.<br>• While all data is encrypted at rest in the Organization's database, the affected API decrypts data in order to display it to merchants. |
| **Affected individuals** | The incident affected approximately 102,720 loan applicants, including 18,824 individuals in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Launched an investigation.<br>• Notified law enforcement.<br>• Patched and deployed into production the vulnerability in the software.<br>• Scanned similar attack vectors and fixed all identified vulnerabilities.<br>• Hired an external information security firm to do a vulnerability assessment which confirmed the number of loan applications affected, the root cause of the incident, and that the vulnerability was addressed.<br>• Added additional automated controls to its platform to assist with automatic detection and remediation of vulnerabilities.<br>• Implemented procedures e.g. updating authentication procedures, adding preventative warnings on new applications to detect the use of information from compromised accounts, adding an additional layer of review of changes to payment instructions and addresses.<br>• Provided additional training and education to front-line staff to heighten awareness of specific malicious behaviour and promote best practices to prevent the introduction of new vulnerabilities.<br>• Offered free credit and identity protection to affected individuals for at least one year. |
| **Steps taken to notify individuals of the incident** | The Organization reported that affected individuals would be notified by letter starting the week of September 23, 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 non-trivial consequences or effects. | The Organization reported that "Improper use of this information could put affected individuals at risk of identity theft or financial fraud."<br><br>I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the significant harms of identity theft and fraud. In addition, email addresses (particularly in conjunction with other information) could be used for phishing purposes, increasing vulnerability to identity theft and fraud. This is also a significant harm. |
| **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 provide an assessment of the likelihood that significant harm would result from this incident.<br><br>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of a deliberate, unauthorized intrusion and it appears the personal information was exported and therefore at risk for further distribution and unauthorized use. |

**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 significant harms of identity theft and fraud. In addition, email addresses (particularly in conjunction with other information) could be used for phishing purposes, increasing vulnerability to identity theft and fraud. This is also a significant harm. The likelihood of harm resulting from this incident is increased as the breach was the result of a deliberate, unauthorized intrusion and it appears the personal information was exported and therefore at risk for further distribution and unauthorized use.

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 will be notifying the affected individuals by letter starting September 23, 2019 in accordance with the *Regulation*. **I require the Organization to confirm to my Office in writing, within 10 days from the date of this decision, that affected individuals have been notified.**

Jill Clayton
Information and Privacy Commissioner