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** | Financial Literacy Counsel Inc. (Organization) |
| **Decision number (file number)** | P2018-ND-051 (File #008536) |
| **Date notice received by OIPC** | April 30, 2018 |
| **Date Organization last provided information** | April 30, 2018 |
| **Date of decision** | May 7, 2018 |
| **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)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The following information was involved in this incident, in various combinations:<br><br>• name (first and last),<br>• address,<br>• email address,<br>• telephone number,<br>• insurance information (policy number, insurance provider, eligibility to increase insurance coverage, type of coverage, investment company, investment type, investment account number, history and balance of investments, and bank account information and signature).<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.<br><br>The Organization reported the majority of the affected individuals in Alberta (6 of a total of 11) "… only had their first name, last name, email and phone number affected". |

| DESCRIPTION OF INCIDENT | |
|---|---|
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • Between March 26, 2018, and April 6, 2018, inbound emails sent to an employee of the Organization were forwarded to unauthorized email addresses.<br>• The Organization discovered the incident on April 6, 2018, when an employee noticed she was not receiving emails on her desktop or Office 365 account.<br>• The Organization's investigation found malware on the computer's Google Chrome browser, which was removed by an external IT company on April 10, 2018.<br>• The cause of the incident is not known, but is suspected to be the staff member clicking either on a phishing email with a malicious link or attachment, or on a malicious link within a Google Chrome browser window. |
| **Affected individuals** | The incident affected a total of 137 individuals, including 11 from Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Removed the unknown email address from the staff member's account and disconnected the affected computer.<br>• Retained an external IT company to investigate, and found and removed malware.<br>• Scanned and monitored the affected computer and staff Outlook accounts. Confirmed no other incoming emails were being forwarded to unknown email addresses.<br>• Changed workstation log-in credentials and passwords and installed two-factor authentication.<br>• Placed flags with insurance and investment companies for affected accounts, working to change investment account numbers and flag accounts.<br>• Offered to reimburse individuals whose sensitive data was affected for credit monitoring or for any fees incurred in trying to change banking account information. |
| **Steps taken to notify individuals of the incident** | The Organization notified 5 of the 11 affected individuals whose sensitive personal and financial information was affected by telephone, and is in the process of notifying all 11 individuals by email/mail during the week of April 30, 2018. |

| REAL RISK OF SIGNIFICANT HARM ANALYSIS | |
|---|---|
| **Harm**<br>Some damage or detriment or injury that could be caused to the 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 "For the 5 people whose personal information included a combination of banking information, signature, history and balance of investments and/or investment account number there is a potential risk of fraud and/or identity theft. For all 11 affected individuals, there is a potential risk of phishing".<br><br>The Organization also said "The harm resulting from fraud or identity theft is significant because it can cause financial loss and other legal consequences for the victim. The harm resulting from phishing is significant because the individuals that have email information could be emailed by the attacker and tricked into clicking on malicious links, or if they are contacted by phone they may be tricked into providing sensitive information."<br><br>I agree with the Organization's assessment of the types of harm that might result from this incident. The contact and insurance information could be used to cause the significant harms of identity theft and fraud. Email addresses could be used to cause the significant harm of phishing. |
| **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 determined that there is a reasonable basis to conclude that harm could occur to the 11 individuals. The incident involved a malicious attack by an unknown person who caused emails to be forwarded, possibly for criminal purposes, which could likely cause harm to the affected individuals."<br><br>I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email). |

**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 as a result of this incident. The contact and insurance information could be used to cause the significant harms of identity theft and fraud. Email addresses could be used to cause the significant harm of phishing. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email).

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand 5 of the 11 affected individuals were contacted by telephone, and all 11 individuals were notified by email/mail during the week of April 30, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner