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** | Servus Credit Union Ltd. (Organization) |
| **Decision number (file number)** | P2019-ND-174 (File #013447) |
| **Date notice received by OIPC** | June 21, 2019 |
| **Date Organization last provided information** | June 21, 2019 |
| **Date of decision** | November 26, 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 the 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"** | Information involved in the breach included:<br><br>• name,<br>• account number, types, balances, transaction history and patterns, bill payees and associated account numbers (excluding credit cards as only the last 4 digits are disclosed), e-transfer details (email addresses and phone numbers for both member and anyone who has received an e-transfer from member).<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On June 18, 2019, an impersonator was able to successfully access a member's account by successfully answering authentication questions from two (2) different call centre agents. |

| | |
|---|---|
| | • The breach was discovered the same day when the actual member contacted the Organization regarding an unauthorized e-transfer and spoke to the call centre agent who had just reset online access for the impersonator. |
| **Affected individuals** | The incident affected 2 individuals. |
| **Steps taken to reduce risk of harm to individuals** | • Reimbursed funds.<br>• Revoked online access to the account pending receipt of computer cleaning.<br>• Flagged account to require enhanced authentication.<br>• Offered 24 months of credit monitoring services.<br>• Due to similar impersonations, within the last year, conducted a series of training sessions with agents using successful phone calls to highlight "red flag" indicators of an impersonation attempt. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified verbally on June 19, and in writing on June 21, 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 "There is the risk for identity theft and fraudulent transactions as a result of the unauthorized access".<br><br>In my view, a reasonable person would consider that the 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 reported "In this case, harm has occurred as the member has lost funds."<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate impersonation) and actual harm resulted. |
| **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 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 the breach appears to be the result of malicious intent (deliberate impersonation) and actual harm resulted.

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 affected individuals were notified verbally on June 19, and in writing on June 21, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner