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** | King Defence (Organization) |
| **Decision number (file number)** | P2020-ND-063 (File #015613) |
| **Date notice received by OIPC** | March 30, 2020 |
| **Date Organization last provided information** | July 8, 2020 |
| **Date of decision** | July 13, 2020 |
| **Summary of decision** | There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 information normally found on a cellular phone, such as photographs and text messages.<br><br>To the extent this information is about an identifiable individual, it is "personal information" as defined in section 1(1)(k) of PIPA. |
| **DESCRIPTION OF INCIDENT** | |
| ☒ loss ☐ unauthorized access ☐ unauthorized disclosure | |
| **Description of incident** | • On Monday March 23, an employee with the Organization went to the courthouse to meet with the friend of a client, who had the client's cellphone.<br>• Due to Covid-19 concerns, the employee placed the cellphone in a plastic bag and put the bag in the centre console of his vehicle.<br>• The employee did not return to the office to review the contents of the cellphone as staff were working from home during the coronavirus outbreak. |

| | |
|---|---|
| | • The Organization reported that the employee left the phone in the locked vehicle thinking it was a secure place given that he was in the process of moving and any virus on the phone would die before he reviewed the cellphone.<br>• On March 27, 2020, the employee noticed the vehicle was broken into, but did not notice the cellphone was missing until sometime later when the client called the Organization.<br>• The employee informed his supervisor of the incident.<br>• The Organization reported that the phone was locked and did not have a SIM card. |
| **Affected individuals** | The incident affected 1 individual. |
| **Steps taken to reduce risk of harm to individuals** | • Contacted Apple Inc. to change the passwords of the iCloud account associated with the phone.<br>• Created a policy that all client property will be delivered directly to the Organization's office and secured in the safe. The Organization will not be accepting property until the office reopens. |
| **Steps taken to notify individuals of the incident** | The affected individual was notified by telephone on March 27, 2020. |
| **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<br><br>*Photos and texts store [sic] on the client's phone could possibly be accessed of [sic] the person who has possession of it had the proper forensic tools to bypass the lock.*<br><br>In my view, a reasonable person would consider that personal information likely to be stored on a cellphone (e.g. photographs, text messages) could be used to cause significant harm; however, in this case, it is not clear what possible harms may exist. |
| **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,<br><br>*It is unlikely that the person who has access to the phone will be able to break through the encryption as the FBI requires Apple to supply special forensic tools to unlock phones of this nature. Calls and texts to the client's phone number will not be able to be accepted on the phone as the SIM card is not in the phone.*<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 malicious intent (theft) by an unknown third party. Although the Organization reported that the cellphone was |

| | |
|---|---|
| | encrypted, it does not know whether the cellphone had a robust passcode or password. The cellphone has not been recovered. |

**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 individual.

A reasonable person would consider that personal information likely to be stored on a cellphone (e.g. photographs, text messages) could be used to cause significant harm; however, in this case, it is not clear what possible harms may exist. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (theft) by an unknown third party. Although the Organization reported that the cellphone was encrypted, it does not know whether the cellphone had a robust passcode or password. The cellphone has not been recovered.

I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individual was notified by telephone on March 27, 2020 in accordance with the Regulation. The Organization is not required to notify the individual again.

Jill Clayton
Information and Privacy Commissioner