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** | Kids Uncomplicated Ltd. (Organization) |
| **Decision number (file number)** | P2017-ND-93 (File #001150) |
| **Date notice received by OIPC** | July 9, 2015 |
| **Date Organization last provided information** | February 3, 2017 |
| **Date of decision** | July 14, 2017 |
| **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)(i) of PIPA. The incident took place in Alberta. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved all or some of the following information:<br>• name,<br>• address,<br>• telephone number,<br>• email address,<br>• individual service plan (including family goals, name, address, name of parent, diagnosis),<br>• intake form contact sheet.<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 28, 2015, sometime between 4:00 a.m. and 9:00 a.m., a vehicle belonging to an employee of the Organization was broken into.<br>• A client binder with one family's personal information was stolen from the trunk. A company assigned iPad was also taken. The iPad was password protected, but not encrypted.<br>• The incident was discovered the same day, at 9:00 a.m.<br>• The iPad was wiped remotely by 9:30 a.m.<br>• The binder was found on July 3, 2015 in a nearby park. All documents were accounted for.<br>• The iPad was recovered during the second week of July. It was dead and the individual who had it did not have a charger, and was unable to use it because of the password protection. |
| **Affected individuals** | The incident affected five (5) individuals who were members of the same family. |
| **Steps taken to reduce risk of harm to individuals** | • The incident was reported to law enforcement.<br>• The paper documents were recovered.<br>• The iPad was remotely erased and then recovered. |
| **Steps taken to notify individuals of the incident** | The family was notified of the incident by email and telephone. |
| **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 that "Harm that may result from this breach includes fraud, identity theft, and humiliation. The sensitivity of the information is highly personal and confidential." Further, the Organization said that "Harm is not significant. The binder was disposed of in a nearby park, and the iPad's information was remotely erased."<br><br>In my view, the contact and profile (health and care) information could be used to cause the harms of identity theft, fraud, hurt, humiliation and embarrassment. Email address could be used for phishing purposes. These are all 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 "There is a possibility that harm could occur. The paper documents have been retrieved, but there is potential that unauthorized individuals have viewed them. The paper documents were exposed for 5 days. The iPad …was password protected, and all information was erased as soon as the theft was discovered." The Organization also noted that if the iPad were hacked, additional individuals could be at risk of harm, including a vulnerable population (youth). |

| | |
|---|---|
| | In my view, there is a real risk of harm to those individuals whose information was in the paper records. The incident was the result of malicious intent (deliberate act to break in to a vehicle and theft of property), and the information was exposed for five days. However, there is very low risk that the iPad contents were accessed as the contents were almost immediately wiped remotely. |

**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 whose information was in the paper records.

The contact and profile (health and care) information could be used to cause the harms of identity theft, fraud, hurt, humiliation and embarrassment. Email address could be used for phishing purposes. These are all significant harms. The incident was the result of malicious intent (deliberate act to break in to a vehicle and theft of property), and the information was exposed for five days. However, there is very low risk that the iPad contents were accessed as the contents were almost immediately wiped remotely.

I require the Organization to notify the affected individuals whose information was in the paper records in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by email and telephone. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner