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** | VTech Holdings Ltd. (Organization) |
| **Decision number (file number)** | P2016-ND-30 (File #001927) |
| **Date notice received by OIPC** | December 07, 2015 |
| **Date Organization last provided information** | February 25, 2016 |
| **Date of decision** | May 30, 2016 |
| **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 registered in British Columbia and 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:<br><br><u>Learning Lodge app store</u><br><u>Parents' account information</u><br>• name,<br>• email address,<br>• mailing address,<br>• secret question and answer (for password retrieval),<br>• internet protocol (IP) address,<br>• download history of device purchases, and<br>• password.<br><br><u>Childs' profile information</u><br>• child name,<br>• child gender,<br>• child birthdate,<br>• child progress log (for parent's reference). |

| | |
|---|---|
| | Kid Connect<br>• user email address,<br>• profile photo,<br>• password,<br>• chat, voice messages and photos (send by child or parents).<br>• bulletin board posting (made by parents, child).<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • On November 23, 2015, a reporter from the online publication Motherboard (www.motherboard.vice.com) contacted the Organization's public relations firm in Canada to inform it of a potential breach.<br>• On November 24, 2015, the Organization's Hong Kong internal investigation detected that there had been anomalous activity on its network on or about November 14. This information was forwarded to the Organization's parent company.<br>• On November 26, 2015, the Organization confirmed that there had been a breach of its network on or about November 14, 2015.<br>• Data involved in the breach included customer data on the Learning Lodge app store customer database and Kid Connect servers, in Hong Kong and the United States.<br>• On December 15, 2015, UK police announced the arrest of a suspect in the hack. |
| **Affected individuals** | Approximate numbers of affected individuals.<br><br>Canadians<br>• Parents: 238,035<br>• Children: 317,608<br><br>Albertans<br>• Parents: 32,503<br>• Children: 45,553 |

| | |
|---|---|
| **Steps taken to reduce risk of harm to individuals** | • The Learning Lodge app store and Kid Connect network, as well as a number of websites, were suspended temporarily while a security assessment was conducted.<br>• The Organization advised customers to change secret questions and answers for password retrieval on other sites where they use the same questions/answers they used on Learning Lodge.<br>• The Organization cooperated with law enforcement in the UK, United States, and Hong Kong.<br>• The Organization is investigating the incident and reviewing its plans, policies and procedures to determine what changes or additions are necessary to prevent the recurrence of the hack and to provide adequate security to customer data.<br><br>**The Organization also reported it:**<br>• Hashes user passwords and encrypts stored voice messages and photos sent via Kid Connect.<br>• Does not collect or store customer credit card numbers or other financial account information, but uses a secure, third-party payment gateway to handle customer payments. |
| **Steps taken to notify individuals of the incident** | • On November 27, 2015 the Organization published a statement on its global website outlining the details of the data breach, and notified the affected customers via email.<br>• The Organization published 5 press releases regarding the incident on its global website in November and December 2015. |
| **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 there was no indication that the information was misused by the hacker or disseminated to anyone but the Motherboard reporter. As a result, the Organization does not believe there is any significant harm or the likelihood of harm.<br><br>I disagree with the Organization. Parents' names, email and home addresses could be used for phishing. Although passwords were hashed and a third party is used for credit card information, password retrieval questions and answers are often reused and could be used to compromise other online accounts. The childrens' information involved in this incident includes identity information, which could be used for identity theft and fraud. Further, children represent a potentially vulnerable population. Phishing, identity theft and fraud 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 it does not think there is any likelihood of harm resulting from this incident.<br><br>The Organization's current information is that the hacker intended to steal the Organization's customer information solely to embarrass the company, and did not intend to use the information or disseminate it to anyone other than the Motherboard reporter.<br><br>I disagree with the Organization. The incident involved a deliberate intrusion by an unauthorized individual who was in control of the information of a significant number of individuals for a month prior to an arrest on December 15, 2015. The Organization can only speculate about the hacker's true intent and any further disclosure of the information. |

**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 parents' information at issue could be used for phishing and to compromise other online accounts. The childrens' information could be used for identity theft and fraud. Phishing, identity theft and fraud are all significant harms. The incident involved a deliberate intrusion by an unauthorized individual who was in control of the information of a significant number of individuals for a month prior to an arrest on December 15, 2015. The Organization can only speculate about the hacker's true intent and any further disclosure of the information.

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

I understand the Organization sent an email to all affected individuals on November 27, 2015. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner