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** | OnePlus Technology (Shenzhen) Co., Ltd. (Organization) |
| **Decision number (file number)** | P2020-ND-123 (File #014050) |
| **Date notice received by OIPC** | December 3, 2019 |
| **Date Organization last provided information** | December 3, 2019 |
| **Date of decision** | October 27, 2020 |
| **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 whose personal information was collected in Alberta, pursuant to section 37.1 of *the Personal Information Protection Act* (PIPA). |
| **JURISDICTION** | |
| **Section 1(1)(i) of PIPA "organization"** | The Organization is a smartphone manufacturing company incorporated in China and is an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved the following information:<br>• first and last name,<br>• telephone number,<br>• email address,<br>• address,<br>• IMEI number,<br>• user name and ID,<br>• order number, total amount, time,<br>• delivery time (to send the products from the warehouse),<br>• sign in time (for the customers to accept the delivery).<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| **Description of incident** | • On November 13, 2019, the Organization received a monitoring alarm system warning, which showed abnormal behavior in its after-sales service API portal.<br>• The Organization investigated and discovered that between October 30 and November 13, 2019, an unauthorized individual registered for an account and used it to access the after-sales pickup and dropoff services IMEI lookup page. Through the lookup page, registered users may find order information using the IMEI number (i.e., the International Mobile Equipment Identity number found on smartphones). The unauthorized individual was able to access data relating to other users and their orders. |
| **Affected individuals** | The incident affected 255,061 individuals, including 3,173 in Alberta. |
| **Steps taken to reduce risk of harm to individuals** | • Blocked the intruder's IP and analyzed the API's security posture.<br>• Disabled the API and assessed the impact.<br>• Fixed the vulnerability, deployed an emergency patch, and restored the API function.<br>• Confirmed the scope of impacted order and user data.<br>• Conducted a post-mortem and laid out plans to prevent it from happening again.<br>• Notified all affected customers directly by email and posted a security notification on the community forum.<br>• Checking all ecommerce website APIs to ensure there are no more security vulnerabilities.<br>• Will continue to provide professional semi-annual data protection training and security developing training for all staff.<br>• Implementing a systematic personal data protection reinforcement project. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by email on November 23, 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 "Affected individuals may receive marketing or other communications from other organisations. Their details may also be used to conduct phishing attempts."<br><br>In my view, a reasonable person would consider the contact and transaction information, particularly in conjunction with email address, could be used to cause the harms of phishing, increasing vulnerability to identity theft and fraud. |
| **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 difficult to assess the likelihood of significant harm resulting to individuals. On one level the data accessed is limited in nature as it concerns only customer order details and their contact details. The information does not include financial details or user account passwords. As a result, it is unlikely that the information can be immediately and directly used to the material detriment of affected customers. However, [the Organization] recognises that there is the risk that some customers could face the risk of phishing attempts using the contact details obtained. The risk of those attempts occurring and, if they do, being successful is difficult to assess.*<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because it resulted from malicious action (deliberate intrusion). The information was potentially exposed over the course of 2 weeks. |

**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 the contact and transaction information, particularly in conjunction with email address, could be used to cause the harms of phishing, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because it resulted from malicious action (deliberate intrusion). The information was potentially exposed over the course of 2 weeks.

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

I understand affected individuals were notified by email on November 23, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner