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** | Combat Network Inc. (Organization) |
| **Decision number (file number)** | P2020-ND-151 (File #015888) |
| **Date notice received by OIPC** | May 15, 2020 |
| **Date Organization last provided information** | May 15, 2020 |
| **Date of decision** | November 20, 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 those 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 an "organization" as defined in section 1(1)(i) of PIPA. |
| **Section 1(1)(k) of PIPA "personal information"** | The incident involved all or some of the following information:<br>• name,<br>• telephone number,<br>• address,<br>• email address,<br>• employer,<br>• job title,<br>• date of birth,<br>• birth certificate,<br>• social security number,<br>• banking and credit card information,<br>• employee ID,<br>• passport and/or driver's license information,<br>• employee security clearance status,<br>• salary,<br>• biometric identifiers,<br>• username and passwords,<br>• car make, model or license plate, and<br>• immigration services information. |

| | |
|---|---|
| | This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.<br><br>To the extent the personal information was collected in Alberta, PIPA applies. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |
| **Description of incident** | • Between approximately October 23, 2019 and October 30, 2019, the Organization was targeted by threat actors who gained unauthorized access to its network systems, and more particularly to some of its employees' mailboxes.<br>• The breach was discovered on October 31, 2019 when the Organization was informed by the Canadian Security Intelligence Service (CSIS) and the Canadian Centre for Cyber Security (CCCS) of potentially malicious activity on its systems linked to a suspect IP address.<br>• During its investigation, access to mailboxes and outbound transfers of data from its email server were noted and the identity of the threat actors was confirmed.<br>• Evidence was not available to determine which email was accessed or exfiltrated so the Organization conducted an eDiscovery process on mailboxes to determine the personal information that may have been breached. |
| **Affected individuals** | The incident affected 643 individuals of which 29 are Alberta residents. |
| **Steps taken to reduce risk of harm to individuals** | • Offered credit monitoring services to affected individuals.<br>• Took steps to secure infrastructure by adding additional security measures.<br>• Worked in close cooperation with CSIS and CCCS and external forensic experts.<br>• Implementing additional security measures to strengthen system security. |
| **Steps taken to notify individuals of the incident** | Affected individuals were notified by email and/or letter between March 20, 2020 and April 7, 2020.<br><br>The Organization reported that one (1) individual was not directly notified by the Organization, which had received the information from the individual's employer. The Organization notified the individual's employer of the incident. |

| | |
|---|---|
| | The Organization also reported that one (1) individual was not notified. The information pertaining to that individual was limited to name and telephone number. |
| **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 "identity theft and/or scam" may occur as a result of the breach. The Organization also reported:<br><br>*According to external forensic experts, the threat actors were not motivated by the collection of personal information, but rather to access to some [sic] of [the Organization's] clients [sic] confidential data considering the nature of threat actors activities [sic]...To this day, there is no evidence that a third party other than the threat actors accessed to the [sic] personal information in question.*<br><br>In my view, a reasonable person would consider the comprehensive contact, financial, credential, and identity information at issue could be used to cause the harms of identity theft, fraud, and financial loss. 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,<br><br>*According to external forensic experts, the threat actors were not motivated by the collection of personal information. Nonetheless, considering the nature of the attack and the sensitivity of the information potentially accessed the likelihood of harm is medium.*<br><br>In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of unauthorized threat actors (deliberate intrusion). Although the Organization reported that "According to external forensic experts, the threat actors were not motivated by the collection of personal information", I do not find this to be reassuring. The Organization can only speculate as to the motives of the threat actors. Further, the information may have been exposed for approximately one (1) week. |
| **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 comprehensive contact, financial, credential, and identity information at issue could be used to cause the harms of identity theft, fraud, and financial loss. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of unauthorized threat actors (deliberate intrusion). Although the Organization reported that "According to external forensic experts, the threat actors were not motivated by the collection of personal information", I do not find this to be reassuring. The Organization can only speculate as to the motives of the threat actors. Further, the information may have been exposed for approximately one (1) week.

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).

Section 19.1(1) of the Regulation states that the notification must "… be given directly to the individual…" , although section 19.1(2) says "… the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that (2) of the affected individuals were not notified directly: for one individual, only name and address were compromised; the other individual's employer was notified, as the information originally came from the employer.

Given the Organization's submissions, I accept that indirect or substitute notice as described by the Organization is reasonable where the Organization was unable to contact the affected individual directly. I accept that name and address alone are unlikely to be used to cause significant harm to the other affected individual.

I understand the Organization notified all other affected individuals by email or mail between March 20, 2020 and April 7, 2020 in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

Jill Clayton
Information and Privacy Commissioner