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** | Universe Machine Corporation (Organization) |
| **Decision number (file number)** | P2022-ND-060 (File #022855) |
| **Date notice received by OIPC** | August 17, 2021 |
| **Date Organization last provided information** | October 14, 2022 |
| **Date of decision** | October 28, 2022 |
| **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 headquartered in Edmonton, Alberta, and 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><br>• name,<br>• mailing address,<br>• telephone number,<br>• email address,<br>• date of birth,<br>• social insurance number,<br>• banking information,<br>• benefits records, and<br>• familial / dependent information.<br><br>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta. |
| **DESCRIPTION OF INCIDENT** | |
| ❑ loss ☒ unauthorized access ❑ unauthorized disclosure | |

| | |
|---|---|
| **Description of incident** | • On August 12, 2021, the Organization was the subject of a ransomware attack. It is believed that the attacker gained access to the environment via brute force attack against public facing ports.<br>• The incident was discovered the following day, August 13, 2021, when one of the Organization's managers attempted to log in to their computer. A ransom demand was also found.<br>• In its January 25, 2022 update, the Organization confirmed that "the threat actor obtained approximately 1% to 3% of its data" and that the "possibility of data exfiltration cannot be ruled out…"<br>• In a recent update, the Organization again advised that "since [Organization] has such a low bandwidth Internet connection, the threat actor was able to download only a small percentage of the [Organization's] overall data, in the range of 1 to 3%."<br>• The Organization also reported that "the disclosed data has <u>not</u> been released into the public domain." |
| **Affected individuals** | The Organization reported that 473 individuals were "potentially affected."<br><br>This included current and former employees of the Organization and current and former employees of another organization to which the Organization provides services [Decision P2022-ND-061]. |
| **Steps taken to reduce risk of harm to individuals** | • Disconnected affected systems from the network.<br>• Changed all passwords.<br>• Retained legal counsel and cybersecurity advisors to assist with response to the attack.<br>• Considering the advice of cybersecurity advisors to better protect against future incidents.<br>• Reported the incident to law enforcement. |
| **Steps taken to notify individuals of the incident** | "All current employees of the [Organization]" were notified by letter beginning August 17, 2021.<br><br>In an August 26, 2021, update, the Organization reported that "the former employees of [the Organization] … potentially affected by this privacy breach have not, as of the date of this addendum … been notified."<br><br>In a January 25, 2022 update, the Organization reported that they "[do] not intend to notify former employees of UMC potentially affected by this breach."<br><br>The Organization did not clarify whether they notified the family members or dependents of current or former employees whose |

| | |
|---|---|
| | personal information may have been affected by the incident. |
| **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:<br><br>*The unauthorized use of any personal information collected as a result of the breach could result in (a) economic loss by impacted employees, (b) embarrassment and inconvenience, and (c) distress, humiliation or anguish.*<br><br>I accept the Organization's assessment. A reasonable person would consider that the contact, identity (social insurance number, date of birth), financial, and employment information, including familial and dependent information, could be used to cause the harms of fraud, identity theft, negative affects on a credit record, and possibly embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms.<br><br>The Organization did not specify in its report, or in subsequent requests for information, the data elements involved for the current and former employees' family members and dependents that were affected. Therefore, it is not clear what possible harms may exist to those individuals. |
| **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>*The threat actor has issued a ransom demand, and typically in such situations upon payment of the ransom demanded, the collected data will be returned or destroyed.*<br><br>*In the event that a negotiated agreement with the threat actor cannot be arrived at, there is a reasonable liklihood [sic] that harm will result as the threat actor may disclose the personal information widely on the Internet, or it may sell such personal information to other rogue actors.*<br><br>In a January 25, 2022 update, the Organization reported:<br><br>*[The Organization] ultimately determined that the threat actor had obtained approximately 1% to 3% of its data. … [The] personal information taken by the threat actor has not been exfiltrated.*<br><br>*The threat actor had threatened to publish the misappropriated personal information as threatened in its ransom demand (attached as Exhibit 1) on September 13th,* |

| | |
|---|---|
| | *2021. [Vendor] has been monitoring for signs of the treat [sic] actor having published the misappropriated personal information as threatened in its ransom demand and, as of the date of this response, [vendor] has uncovered no evidence of any such publication.*<br><br>***The possibility of data exfiltration cannot be ruled out** at this time, however the risk of the threat actor publishing the misappropriated personal information as set out in its ransom demand appears to be low.* [emphasis added]<br><br>…<br><br>*[The Organization] also expunges employment-related information from its systems, which further mitigates the risk that employment-related information of former employees has been exfiltrated.*<br><br>In a recent response to a request for information, the Organization also stated:<br><br>*[Organization] has had [Vendor] confirm to it that since [Organization] has such a low bandwidth Internet connection, the threat actor was able to download only a small percentage of the [Organization's] overall data, in the range of 1 to 3%. Also, [Vendor] confirmed (see the attached email) that the disclosed data has not been released into the public domain. This is the only evidence that [Organization] can provide and it believes that it is conclusive. …*<br><br>*[Organization] does not have any information that would infer or suggest that any personal information of its or [another organization that retained the Organization as a service provider] employees was disclosed as a result of the attack.*<br><br>The Organization submitted a report to our office stating that the above described personal information was affected by the incident.<br><br>The Organization confirmed a "download of the Organization's overall data, in the range of 1-3%." The amount of data involved is irrelevant. It is the type of data and the circumstances that determine if there is a real risk of significant harm to affected individuals. In this case, the Organization confirmed a download of data as a result of the incident.<br><br>The Organization states the disclosed data has not been released into the public domain. Consistent with the reasoning in many |

| | |
|---|---|
| | decisions posted on my office's website, lack of evidence of misuse of the data does not mitigate against future harm. Information obtained from a breach can be published or used months or years after the incident.<br><br>With respect to the former employee personal information, the practice of expunging information may mitigate risk of harm to those individuals. However, the risk is not negated. The Organization did not provide information when requested to explain the expunging process. The Organization did not respond to requests to confirm if information about former employees was affected in the incident. However, the Organization indicated that former employees were affected by the incident in an addendum to its report.<br><br>In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, deployment of ransomware, demand for ransom payment).<br><br>Overall, the Organization did not rule out the possibility that records of current and former employees, and their family members or dependents, were exfiltrated. It confirmed that 1-3% of its overall data was downloaded. |

**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.

The contact, identity (social insurance number, date of birth), financial, and employment information, including familial and dependent information, could be used to cause the harms of fraud, identity theft, negative affects on a credit record, and possibly embarrassment, hurt or humiliation. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are significant harms.

The Organization did not clarify what data elements about current and former employees' family members and dependents were affected. Therefore, it is not clear what possible harms may exist to those individuals.

The Organization states the disclosed data has not been released into the public domain. Consistent with the reasoning in many decisions posted on my office's website, lack of evidence of misuse of the data does not mitigate against future harm. Information obtained from a breach can be published or used months or years after the incident.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, deployment of ransomware, demand for ransom payment).

The practice of expunging information about former employees may mitigate risk of harm to those individuals. However, the risk is not negated.

Overall, the Organization did not rule out the possibility that records of current and former employees, and their family members or dependents, were exfiltrated. It confirmed that 1-3% of its overall data was downloaded.

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…", however 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."

I understand the Organization notified current employees by letter, beginning on August 17, 2021. However, the notification did not include a description of all personal information involved. The notification mentioned that "benefit records" were involved, but did not include a description of the familial / dependent information. I further understand that the Organization "does not intend to notify former employees … potentially affected by this breach" and did not respond to requests to clarify whether it could rule out, with certainty, the possibility that former employees were affected. It is also not clear whether family members and dependents whose personal information may have been affected by the breach were notified of the incident.

**To the extent notifications to affected individuals did not indicate what familial / dependent information was involved, I require the Organization to notify those affected individuals again in accordance with section 19.1(1) of the Regulation. The Organization is required to confirm to my office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.**

**The Organization is also required to notify affected former employees, and family members or dependents, in Alberta in accordance with section 19.1(1) of the Regulation. The Organization is required to confirm to my office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.**

If the Organization is unable to notify affected individuals under section 19.1(1), it may consider making a submission to my office pursuant to section 19.1(2) of the Regulation within seven (7) days of this decision. The submission must include reasons why direct notification is unreasonable in the circumstances and include a plan on how it intends to notify affected individuals indirectly.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance