[redacted]

MAXAVA
MAXIMUM AVAILABILITY

*Strictly Private and Confidential* *10 December 2024 (NZT)*

Maximum Availability Limited (NZBN: 9429037548995) has been impacted by a cyber incident. As we operate as a tight group of companies globally, this incident also potentially impacts Maximum Availability Limited (SC298941), Maxava LLC, Maxava KK and other group and related companies. This notice is provided on behalf of all of these companies, which are together referred to as "Maximum Availability".

We are writing to you as a former employee of, or Independent Contractor to, Maximum Availability.

We became aware that some of our x86 business systems were impacted by an event last week.

We now know that we were the target of a ransomware attack.

We have engaged professional IT and forensic support to help us, and we are working as quickly as possible to understand how this happened and what we need to do to fix it.

We wanted to keep you updated on what has happened and how Maximum Availability has responded. We appreciate that you may have questions – if so please feel free to reach out to Desmond Venter (desmond.venter@maxava.com).

**What has happened?**

The hackers have accessed and encrypted at least some of the three x86 systems that were impacted by the attack.

These systems are currently isolated. Our primary business systems, which are cloud based, appear unaffected and we are able to carry on operating as usual. Maxava software products (IBM i products) are not developed on or released via the identified impacted business systems.

While the initial investigation conducted by our IT forensic investigators has not determined whether information has been removed from our network, it is possible that copies have been taken of password-protected backups of our payroll records, personnel files and emails. The investigation is ongoing. We have identified the organization that appears to be responsible for the ransomware attack.

## What has Maximum Availability done in response?

Upon discovering the suspicious activity, we took immediate steps to contain the situation and engage external experts.

At this stage it is not clear if the malware was the only malicious activity, or if the compromise may have been broader. Our IT forensic provider is currently reviewing the incident to determine how it has occurred and what may be affected. We are also conducting a full review of our IT security.

## What should you do?

As mentioned above, we have not determined whether information has been removed from our systems, although this is part of the ongoing investigation. We will keep you updated on any findings that may impact you.

As a precaution we would ask you to be alert for any suspicious email correspondence seeking payment or information in suspicious circumstances, or other unusual/dubious

emails (e.g. seeking to change bank account details). If you have received any suspicious correspondence, please let us know.

We are obviously incredibly frustrated that this has happened and sincerely apologise for any inconvenience or concern that this this may cause you.

We will keep you updated on any material developments. If you have any questions, please do not hesitate to contact Desmond or myself.

Kind regards,

Allan Campbell
Maximum Availability Limited (NZ company),
Maxava LLC,
Maxava KK,
Maximum Availability Limited (UK company)
allan.campbell@maxava.com
+64 21 577 000

Legal Notice – New Zealand Privacy Act

We have informed the Office of the Privacy Commissioner about the incident. You also have a right to make a complaint to the New Zealand Privacy Commissioner by calling 0800 803 909 (from within New Zealand) or visit: Office of the Privacy Commissioner | Complaining to the Privacy Commissioner. If you notify please use reference b1cc6100-48ec-4ca3-af0b-e6f332d99153 and direct your notification to the attention of Desmond Venter.

---