Super Micro Computer, Inc.
980 Rock Avenue
San Jose, CA 95131

October 18, 2018

Dear Valued Customer,

We are confident that a recent article, alleging a malicious hardware chip was implanted during the manufacturing process of our motherboards, is wrong. From everything we know and have seen, no malicious hardware chip has been implanted during the manufacturing of our motherboards.

We trust you appreciate the difficulty of proving that something did not happen, even though the reporters have produced no affected motherboard or any such malicious hardware chip. As we have said firmly, no one has shown us a motherboard containing any unauthorized hardware chip, we are not aware of any such unauthorized chip, and no government agency has alerted us to the existence of any unauthorized chip. Despite the lack of any proof that a malicious hardware chip exists, we are undertaking a complicated and time-consuming review to further address the article. In the meantime, I want to assure you that Supermicro's design, manufacturing and quality processes are designed to ensure we provide high-performing, safe, reliable, and secure hardware to all our customers.

Regular Testing

We are a customer-focused, engineering-led culture, so we test our products at every step along the way. We check every board, we check every layer of every board, and we check the board's design visually and functionally, throughout the entire manufacturing process. Every board we manufacture has Supermicro oversight, including multiple layers of testing, from design to delivery.

Specifically, our process requires the inspection of the layout and components of every product at the beginning and end of each stage of manufacturing and assembly. Our employees are on site with our assembly contractors throughout the process. These inspections include several automated optical inspections, visual inspections, and other functional inspections. We also periodically employ spot checks and x-ray scans of our motherboards along with regular audits of our contract manufacturers. Our test processes at every step are not only designed to check functionality, but also to check for the integrity and composition of our designs and to alert us to any discrepancies in the base design.

Technical Implausibility

Our motherboard designs are extremely complex. This complexity makes it practically impossible to insert a functional, unauthorized component onto a motherboard without it being caught by any one, or all, of the checks in our manufacturing and assembly process. The complex design of the underlying layers of the board also makes it highly unlikely that an unauthorized hardware component, or an altered board, would function properly.

Our motherboard technology involves multiple layers of circuitry. It would be virtually impossible for a third party, during the manufacturing process, to install and power a hardware device that could communicate effectively with our Baseboard Management Controller because such a third party would lack complete knowledge (known as "pin-to-pin knowledge") of the design. These designs are trade

secrets protected by Supermicro. The system is designed so that no single Supermicro employee, single team, or contractor has unrestricted access to the complete motherboard design (including hardware, software, and firmware).

Supply Chain Management

We employ stringent due diligence and qualification processes to select our contract manufacturers, which we regularly audit for process, quality, and control.

Our manufacturing process is designed to prevent unauthorized physical alterations of our motherboards by either our contract manufacturers or anyone at Supermicro. Motherboard design is systematically compartmentalized along the supply chain and within Supermicro in order to maintain security and product integrity. No party in the manufacturing process—other than Supermicro—has full information about the design of our motherboards during our multi-step production process. Even at Supermicro, the system is designed so that no single employee or team has unrestricted access to the entire design.

Each of our contractors has only the portion of the total engineering design of the motherboard that it needs to carry out its part in the manufacturing process. Modifications to the design plan must be confirmed with Supermicro, which then passes those modifications on to those downstream in the manufacturing process. If any single contractor attempts to modify the designs, the manufacturing process is structured so that those alterations would not match the other design elements in the manufacturing process. This makes it practically impossible for anyone to add an unauthorized hardware component that could both escape detection and function properly. This also ensures there are multiple quality checks built into each step of our manufacturing process.

For these reasons, we are confident that these allegations are wrong. In addition, experts across the ecosystem, including FBI Director Christopher Wray, NSA Senior Cybersecurity Advisor Rob Joyce, Director of National Intelligence Dan Coats, the Department of Homeland Security, the UK's GCHQ and even an expert quoted in the article itself, have questioned these allegations. Finally, Apple and Amazon have issued strong statements denying the claims.

Thank you very much for your business and continued support.

Charles Liang
President and CEO

David Weigand
SVP and Chief Compliance Officer

Raju Penumatcha
SVP and Chief Product Officer