March 16, 2026

**Stryker cyber incident response certification letter**

**Incident and response**

On Wednesday, March 11, Stryker was targeted in a cyberattack which resulted in a global disruption to our internal Microsoft environment. The threat actor performed a wipe of our internal virtual infrastructure using a legitimate mobile device management (MDM) platform called Microsoft Intune. This rendered laptops, mobile devices and virtual servers inoperable.

Our internal teams, in partnership with third-party experts, reacted quickly to not only regain access but to remove the unauthorized party from our environment.

The event only affected Stryker's internal Microsoft corporate environment. This was not a ransomware attack, and no malware was deployed to our systems. The incident has been contained, and we are now in the restoration process, which is progressing steadily.

Importantly, our investigation continues to be ongoing.

**Product safety**

All Stryker products across our global portfolio, including connected, digital, and life-saving technologies, remain safe to use. This event was contained to Stryker's internal Microsoft environment, and as a result it did not affect any of our products—connected or otherwise. Stryker, much like any Fortune 300 company, has embedded policies and procedures for cybersecurity assurances for our products in the field. This process at Stryker provides additional assurances that no potential vulnerabilities or risk of exploitation related to our connected products exist. Per our standard protocols, we have leveraged this process to confirm that our connected products were not impacted by the incident and remain safe to use.

**Communication with Stryker Sales Representatives**

It is completely safe for Stryker sales representatives to be onsite in hospitals and facilities. It is also safe for you to communicate by phone or e-mail with Stryker personnel. The event only affected Stryker's internal Microsoft corporate environment. This was not a ransomware attack, and no malware was deployed to our systems.

**Supply, ordering and shipping**

We are working closely with our global manufacturing sites to manage operations and mitigate potential impacts, supported by our robust resiliency and business continuity plans. We are actively bringing our electronic ordering systems back online. In the meantime, your Stryker Sales Representatives will be working with you and your distributors directly in an effort to bring you replenishment product through manual ordering where that option exists. Orders placed prior to the disruption will be reconciled as systems are restored, and electronic orders placed during the disruption will process once systems are back online, and supply is flowing normally.

**Next steps**

We are prioritizing restoration of systems that directly support customers, ordering and shipping. Our core transactional systems are already on a clear path to recovery, and we will continue to provide updates as progress is made.

We are committed to transparency and will continue to provide additional updates as we have information to share. While the investigation is ongoing, Stryker confirms that the above information is accurate to the best of our knowledge as of the date of this document.

**Kevin Lobo**

Chair and Chief Executive Officer