UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): March 23, 2026

Stryker Corporation
(Exact name of Registrant as Specified in Its Charter)

Michigan	001-13149	38-1239739
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(IRS Employer Identification No.)

1941 Stryker Way Portage, Michigan	49002
(Address of Principal Executive Offices)	(Zip Code)

Registrant's Telephone Number, Including Area Code: (269) 385-2600

(Former Name or Former Address, if Changed Since Last Report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common Stock, $.10 Par Value	SYK	New York Stock Exchange
2.125% Notes due 2027	SYK27	New York Stock Exchange
3.375% Notes due 2028	SYK28	New York Stock Exchange
0.750% Notes due 2029	SYK29	New York Stock Exchange
2.625% Notes due 2030	SYK30	New York Stock Exchange
1.000% Notes due 2031	SYK31	New York Stock Exchange
3.375% Notes due 2032	SYK32	New York Stock Exchange
3.625% Notes due 2036	SYK36	New York Stock Exchange

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§ 230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§ 240.12b-2 of this chapter).

Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Item 7.01 Regulation FD Disclosure.

As previously reported in two separate Current Reports on Form 8-K, filed with and furnished to (as the case may be) the U.S. Securities and Exchange Commission (the "SEC") on March 11, 2026, and March 12, 2026, respectively, Stryker Corporation (the "Company") disclosed that the Company had identified a cybersecurity incident. Since then, the Company has worked around the clock, together with third-party experts and law enforcement to contain and neutralize the impact of the cyber incident and restore operations. Since then, the Company has been providing updates to its customers, suppliers, vendors and partners on its ongoing investigation through the Company's website and its social media channels. The information included in this report is a further update on the status of its ongoing investigation, which is also being communicated to its customers, suppliers, vendors, and partners through its website.

Early in the Company's investigation and based on the information it had at that time, management believed that the incident did not involve ransomware or malware. Further into the course of its investigation alongside Palo Alto Networks' Unit 42 and other experts, the Company was able to identify that while the threat actor used a malicious file to run commands which allowed it to hide its activity while in its systems, this file was not capable of spreading — either inside or outside of the Company's environment. As of the date of this report, the Company's investigation has not identified malicious activity directed towards its customers, suppliers, vendors or partners. The Company has continued to learn more alongside its third-party advisors, including those at Palo Alto Networks Unit 42. Their latest findings are included in a General Assurance letter, which is attached hereto as Exhibit 99.1 and can also be found on the Company's website at Stryker.com. This letter reaffirms the Company's belief that this incident is contained and that the current analysis has not identified any evidence of the threat actor accessing customer, supplier, vendor and partner systems as a result of this incident. The Company has also posted a statement on its website at Stryker.com which is attached hereto as Exhibit 99.2.

As its investigation is ongoing, the Company will continue to update its customers, suppliers, vendors and partners through its website disclosures, which updates will supersede previously made website reports. For example, the Company's website reports have been updated to reflect that the cybersecurity incident caused disruption to the Company's corporate network environment, including but not limited to the Microsoft environment. The Company's investigation of the cybersecurity incident is ongoing, and the scope, nature and impact, including, but not limited to operational and financial impact, of the incident continue to be assessed and re-evaluated. Accordingly, the Company has not yet determined whether the incident is reasonably likely to have a material impact on the Company.

The information furnished in this report, including Exhibits 99.1 and 99.2, shall not be deemed "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), or incorporated by reference in any filing under the Securities Act of 1933, as amended, or the Exchange Act, except as shall be expressly set forth by specific reference in such filing.

Caution Concerning Forward-Looking Statements

This Current Report on Form 8-K contains forward-looking statements subject to the safe harbor protection provided by Section 27A of the Securities Act of 1933, Section 21E of the Securities Exchange Act of 1934, and the Private Securities Litigation Reform Act of 1995. All statements other than statements of historical fact are forward-looking statements, including statements regarding the Company's current beliefs regarding the extent of the cybersecurity incident and the results or findings of the Company's investigation thereof; the Company's ability to contain and/or mitigate the incident; the disruption to our business or operations; and the potential impact on the Company's reputation, financial condition and results of operations. These forward-looking statements involve known and unknown risks, uncertainties and other important factors that may cause actual results to differ materially from expectations as of the date of this filing. Factors that could cause actual results to differ materially from those indicated in the forward-looking statements include, but are not limited to, any impairment of the integrity of the Company's systems or data; delays or difficulties in restoring the Company's systems and data; the Company's continued ability to use alternatives to its systems, to the extent needed; the Company's ability to process information it collected while using alternatives to its systems and the integrity of that information; the adequacy of processes during the period of disruption of the Company's systems; the results of the Company's analysis of the scope and details of the

cybersecurity incident; the unauthorized release of any of the Company's data, including third party data held by the Company, or the use of any such data for any fraudulent purposes; potential adverse impact of the incident on the Company's results of operations, including revenue, operating income and cash flows from operations, and on its financial condition, including liquidity; diversion of management's attention from operations of the Company to address the cybersecurity incident; potential litigation related to the cybersecurity incident; potential adverse effects on relationships with customers, suppliers, patients and other third parties as a result of the cybersecurity incident; reputational risk related to the cybersecurity incident; regulatory scrutiny as a result of the cybersecurity incident; and other risks listed or described from time to time in our filings with the SEC, including our Annual Report on Form 10-K and Quarterly Reports on Form 10-Q that we have filed or will file hereafter. Except as required by applicable law, we disclaim any intention or obligation to publicly update or revise any forward-looking statement to reflect any change in our expectations or in events, conditions or circumstances on which those expectations may be based, or that affect the likelihood that actual results will differ from those contained in the forward-looking statements.

Item 9.01 Financial Statements and Exhibits.

(d) Exhibits

99.1 General Assurance Letter

99.2 Company Statement

104 Cover Page Interactive Data File (the cover page XBRL tags are embedded within the Inline XBRL document)

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

STRYKER CORPORATION
(Registrant)

Dated: March 23, 2026

By: /s/ Tina S. French
Name: Tina S. French
Title: Corporate Secretary

Exhibit 99.1

March 20, 2026

Stryker Corporation

Att: David Nathans, Vice President, Chief Information Security Officer

Subject: Stryker Corporation Partner and Customer Connections to the Stryker Environment

Mr. Nathans,

Per your request, **Palo Alto Networks Unit 42** hereby issues this letter as a status update on Unit 42's services assisting **Stryker Corporation (Stryker)** to provide, at your direction, Digital Forensics and Incident Response (DFIR) services in relation to a security compromise involving **impacts to Stryker's Entra ID environment, servers, and workstations** ("Security Incident").

Scope of Work

As part of the completed activities for this engagement, Unit 42 has worked with **Stryker**'s technical teams to perform the following:

- **Threat Hunting & Forensic Analysis:** Conducted deep-dive analysis of endpoint forensic images, network logs, and identity infrastructure (including **Entra ID/Active Directory**) to identify indicators of compromise (IOCs) and evidence of unauthorized access.
- **Containment & Eradication:** Identified and neutralized suspected malicious binaries and unauthorized persistence mechanisms.
- **Infrastructure Review:** Reviewed available forensic evidence from, and the security of critical business process flows within, the **Stryker** corporate environment.

Current Findings and Assurance

As of 2026-03-20, 15:20 UTC, based on the forensic evidence reviewed and the threat hunting activities performed across the environment:

1. **No Persistent Activity Identified:** Unit 42 has found no current evidence of active, uncontained, persistent unauthorized access within the **Stryker** environment.
2. **Eradication of Identified IOCs:** All known indicators of compromise associated with this specific incident have been successfully identified and addressed.
3. **Remediation Validation: Stryker** has engaged Microsoft to assist with recovery of the identity infrastructure and has reported that existing accounts have been secured. Unit 42 is supporting Stryker and Microsoft in these efforts. Additionally, with guidance from

Unit 42, **Stryker** is rebuilding impacted systems or restoring from backups predating the known window of compromise to further prevent threat actor re-entry. Those impacted systems not yet rebuilt/restored, have been isolated from the network.

Conclusion

As of the date of this letter, within the scope of our services, Unit 42 has not identified evidence of unauthorized activity related to the Security Incident since 2026-03-11. Currently available evidence indicates that the identified unauthorized activity has been contained and the immediate risk to **Stryker**'s operational environment has been mitigated. At your direction, Unit 42 will continue to monitor the environment as part of its analysis and threat hunting phases.

The information provided in this status update letter may be subject to change based on the continued performance of Unit 42's services. Unit 42 shall not be responsible or liable for any reliance on the contents of this letter by any third party.

Sincerely,

Troy Bettencourt

VP, Digital Forensics and Incident Response Palo Alto Networks | Unit 42 | 941.447.1030

Exhibit 99.2

Customer Update: Stryker Network Disruption

03/23/2026

Our internal teams continue to work around the clock with external partners to make meaningful progress on our restoration efforts. We are grateful for the partnership and collaboration with government agencies and industry partners.

We believe the incident is contained, and we are prioritizing restoration of systems that directly support customers, ordering and shipping. 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.

Early in our investigation, we believed there was no indication of ransomware or malware. Further into the course of our investigation, alongside Palo Alto Networks Unit42 and other experts, we identified that the threat actor used a malicious file to run commands which allowed them to hide their activity while in our systems. To be clear, this file was not capable of spreading — either inside or outside of our environment. Most importantly, at no point has our investigation identified malicious activity directed towards our customers, suppliers, vendors or partners. Unit42's latest findings are included in a General Assurance Letter we received, which can be found here. This letter reaffirms our belief that this incident is contained and that analysis has not identified any evidence of the threat actor accessing customer, supplier, vendor and partner systems as a result of this incident.

There is nothing more important to us than the customers and patients we serve, and we recognize the criticality of every procedure to every patient. We are working closely with our global manufacturing sites as operations continue to stabilize. Manufacturing capability is ramping quickly as critical lines and plants are brought back online, prioritizing patient needs. This is a 24/7 effort and the first priority of our entire organization.