UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, DC 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): July 25, 2024

CRIMSON WINE GROUP, LTD.

(Exact Name of Registrant as Specified in Charter)

Delaware	000-54866	13-3607383
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(IRS Employer Identification No.)

5901 Silverado Trail, Napa, California	94558
(Address of Principal Executive Offices)	(Zip Code)

(800) 486-0503

(Registrant's telephone number, including area code)

N/A

(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: None.

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 1.05. Material Cybersecurity Incidents.

As previously disclosed on the Current Report on Form 8-K filed by Crimson Wine Group, Ltd. (the "Company") on July 5, 2024 (the "Initial Report"), on June 30, 2024, the Company detected a cybersecurity incident in which an unauthorized third party gained access to certain information systems of the Company. Upon detection, the Company promptly initiated response protocols and began taking steps to contain, assess and remediate the cybersecurity incident, including launching an investigation with external cybersecurity experts. As the Company was in early stages of its investigation and assessment of the incident, it was unable to determine at the time of the Initial Report whether the incident had or will have a material impact on the Company.

On July 25, 2024, the Company determined that the cybersecurity incident has likely had a material impact on the Company's business operations. The incident consisted of the third party's unauthorized access to a portion of the Company's internal information systems and the exfiltration of certain files, including files potentially containing sensitive personal information. The Company is still investigating the extent of any personal or otherwise sensitive information contained in the files acquired by the unauthorized third party, including if any personal information of customers was impacted. The Company intends to provide required notifications to affected and potentially affected parties and to applicable regulatory agencies. As part of its process to contain, assess and remediate the incident, the Company took measures, including shutting down certain of its systems, to isolate its operations from the Internet, which resulted in disruption to the Company's business operations, despite the implementation of workarounds for certain offline operations, and limitation of access to portions of the Company's business applications supporting aspects of the Company's operations and corporate functions, including financial and operating reporting systems. Although the Company has substantially restored its information systems and data that were impacted by the cybersecurity incident and has resumed normal business operations, it continues to assess operational impacts and evaluate additional measures to strengthen its surveillance of cybersecurity threats and to prevent unauthorized cybersecurity incidents on or conducted through its information systems and to strengthen its information backup protocols.

Although the Company has determined that the cybersecurity incident has likely had a material impact on the Company's business operations, as of the date of this Current Report on Form 8-K, the Company believes that the cybersecurity incident has not had a material impact on the Company's overall financial condition or results of operations. and the Company does not believe the cybersecurity incident is reasonably likely to materially impact the Company's overall financial condition or results of operations. The Company believes it holds adequate cybersecurity insurance to offset a substantial portion of the costs of the cybersecurity incident; however, the Company may incur expenses and losses related to this incident that are not covered by insurance. To the extent the Company incurs future, material direct expenses or other losses as result of this cybersecurity incident, and those costs are not covered by insurance, the Company will report such material losses in the appropriate period.

The Company remains subject to various risks due to the cybersecurity incident, including potential litigation, changes in customer behavior, additional regulatory scrutiny, and the

subsequent availability of, or increase in cost to the Company of, its insurance policy covering cybersecurity incidents.

Forward-Looking Statements

This Current Report on Form 8-K contains forward-looking statements, including, but not limited to, statements regarding the Company's current beliefs, understanding and expectations regarding the cybersecurity incident and its impact or anticipated impact on the Company's business, operations and financial results. Factors that could cause actual results to differ from those expressed in these forward-looking statements include the ongoing assessment of the cybersecurity incident; legal, reputational and financial risks resulting from the cybersecurity incident or additional cybersecurity incidents; and the risks described in the Company's Annual Report on Form 10-K for the year ended December 31, 2023 and subsequent Quarterly Reports on Form 10-Q. Unless required by law, the Company expressly disclaims any obligation to update publicly any forward-looking statements, whether as result of new information, future events or otherwise.

SIGNATURES

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.

Dated: July 25, 2024

CRIMSON WINE GROUP, LTD.

By: /s/ Jennifer L. Locke
Name: Jennifer L. Locke
Title: Chief Executive Officer