**UNITED STATES DISTRICT COURT**
**DISTRICT OF COLUMBIA**

| | |
|---|---|
| **SECURITIES AND EXCHANGE COMMISSION**,<br>100 F Street, NE<br>Washington, DC 20549<br><br>Applicant,<br><br>vs.<br><br>**COVINGTON & BURLING LLP**,<br>850 10th St, NW<br>Washington, DC 20268<br><br>Respondent. | Case No. _____ |

**SECURITIES AND EXCHANGE COMMISSION'S MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF APPLICATION FOR AN ORDER TO SHOW CAUSE AND FOR AN ORDER COMPELLING COMPLIANCE WITH INVESTIGATIVE SUBPOENA**

The Securities and Exchange Commission (the "Commission") requests, pursuant to Section 21(c) of the Securities Exchange Act of 1934 ("Exchange Act") [15 U.S.C. § 78u(c)] and Section 22(b) of the Securities Act of 1933 ("Securities Act") [15 U.S.C. § 77v(b)], that the Court enforce an administrative subpoena issued to Covington & Burling LLP ("Covington" or "Respondent") as part of an investigation into possible violations of the federal securities laws. Covington has failed to comply with the subpoena's directive to produce certain documents. For the reasons set forth below, this Court should order Covington to comply with the subpoena.

## STATEMENT OF FACTS

### A. The Cyberattack

Covington & Burling LLP is an American multinational law firm headquartered in Washington, D.C., with 13 total offices, eight of which are located abroad. Declaration of W. Bradley Ney ("Ney Decl.") ¶ 6. The firm advises clients on transactional, litigation, regulatory, and public policy matters. *Id*.

In or around November 2020, threat actors associated with the Microsoft Hafnium cyberattack (the "Cyberattack") gained unauthorized access to Covington's computer network and certain individual devices. *See* Ney Decl., Exh. B. In connection with the Cyberattack, the threat actors were able to access non-public information of certain Covington clients, including 298 companies regulated by the Commission. *Id*. After Covington learned of the unauthorized access, it compiled a list of potentially affected clients and "contacted those potentially affected clients simply to notify them of that fact and invited each client to discuss the matter." *Id*. Covington has admitted that a foreign actor intentionally and maliciously accessed the files of Covington's clients, including companies regulated by the Commission. *Id*. In light of this reported breach, the Commission is seeking to determine whether the malicious activity resulted in violations of the federal securities laws to the detriment of investors. *Id.* at ¶¶ 4, 5.

### B. The Investigative Subpoena

On March 16, 2021, the Commission issued a formal order of private investigation and examination ("Formal Order"). Ney Decl., ¶ 4. Pursuant to the Formal Order, the Commission is investigating, among other things, whether any persons or entities involved in or impacted by the Cyberattack have been or are engaging in violations of the federal securities laws. *Id.* at ¶ 4. Information about potential violations related to improper access to material, nonpublic information

regarding Covington's public company clients is within the scope of the Formal Order. *See id.* at ¶¶ 4, 5.

The Commission regularly seeks information from companies that were victims of cyberattacks for a number of reasons, including to (1) understand the nature and scope of the attack, (2) assess and identify potential illegal trading based on information gathered during the attack; (3) assess and identify potential illegal trading based on the fact of the attack itself; and (4) determine relevant disclosure obligations of public companies impacted by the attack. Ney Decl., ¶ 18. The Commission has previously brought cases against threat actors who traded on information obtained through cyberattacks, including cyberattacks on law firms, as well as against companies that failed to disclose the material impact of cyberattacks to investors. *Id*. at ¶ 19.[1]

On March 21, 2022, after learning that the Cyberattack had impacted Covington, the Commission served a subpoena (the "Subpoena") by encrypted electronic mail on Anne Scott, a Covington attorney. Ney Decl. ¶ 7, Exh. A. Ms. Scott acknowledged service of the Subpoena on March 24, 2022. *Id.* at ¶ 7. The Subpoena called for Covington to produce limited information related to the Cyberattack. In response, Covington produced all of the documents called for in the Subpoena with the exception of documents related to Request No. 3.[2] Covington's refusal to

[1] *See, e.g.*, *SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases* (Aug. 11, 2015) available at https://www.sec.gov/news/press-release/2015-163; *Chinese Traders Charged with Trading on Hacked Nonpublic Information Stolen From Two Law Firms* (Dec. 27, 2016) available at https://www.sec.gov/news/pressrelease/2016-280.html; *Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million* (April 14, 2018) available at https://www.sec.gov/news/press-release/2018-71.

[2] As related to the Cyberattack, Request No. 3 originally called for (a) the client or other impacted party name; (b) the nature of the suspected unauthorized activity concerning the client or other impacted party, including when the activity took place and the amount of information that was viewed, copied, modified, or exfiltrated, if known, and (c) any communications provided to the client or other impacted party concerning the suspected unauthorized activity. *Id.*, Exh. A, ¶ C.3.

comply with Request No. 3 was based on assertions of privilege and client confidentiality. *See id.*, Exh. B.

### C. The Narrowing of the Scope of the Subpoena

Covington first reached out to the Commission on April 4, 2022, the same date that the documents were due under the Subpoena, to relay that it would not meet the deadline and that there may be some challenges to complying with Request No. 3.[3] Ney Decl. ¶ 9. Following Covington's refusal to produce documents in compliance with Request No. 3 and at its request, the Commission entered into good faith negotiations with Covington to narrow the Request, ultimately offering to limit it to Request No. (3)(a) only, *i.e.*, the names of any clients regulated by the Commission[4] whose information had been viewed, copied, modified or exfiltrated during the attack on Covington, which Covington still refused to provide. *Id.* at ¶¶ 9, 12.

As part of the negotiations, Covington undertook a review to identify how many, if any, of the 298 public company clients had material non-public information ("MNPI") that was viewed, copied, modified, or exfiltrated by the threat actor. Ney Decl. ¶ 13. As a result of that review, Covington concluded that, in its view, only seven of the 298 impacted clients' files contained MNPI. *Id.* at ¶ 14. However, the Commission has been unable to verify that information and

---

[3] With respect to the other Requests made under the Subpoena, Covington has represented that it has completed production for those Requests. Covington made its first production on April 18, 2022, and its last production on August 12, 2022. The total number of Responsive documents made in response to the Subpoena, not including Request No. 3, is very small—totaling only nine documents.

[4] While the subpoena as written referenced public companies, during the course of negotiations, Covington and the Commission agreed that the phrase public companies would refer to both companies traded on a U.S. exchange, and any other entities regulated by the Commission, including investment advisers, brokers and dealers, collectively referred to herein as the "public company clients" or the" clients." Ney Decl. ¶ 8.

disagrees with Covington's methodology for determining what constitutes MNPI.[5] *Id*. Therefore, the Commission seeks the names of all 298 clients who had any information accessed as part of the Cyberattack.

Throughout the course of the negotiations, the Commission has made every effort to accommodate Covington in an attempt to avoid the need for this subpoena enforcement action, including limiting request No. 3 to only the names of the impacted clients. Ney Decl. at ¶ 16. Despite the Commission's willingness to negotiate the scope of its lawful Subpoena, the parties were unable to reach agreement. *Id*. at ¶ 16. Accordingly, the Commission seeks the aid of the court to compel Respondent to produce the very limited information requested in Subpoena Request No. 3(a).

## ARGUMENT

The significance and importance of cybersecurity issues to the Commission's mission has never been more apparent than in the last several years, during which threat actors have targeted public companies and regulated entities with large-scale cyberattacks, often seeking to profit at the expense of investors who the Commission is charged with protecting. *See, e.g., Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Securities Act Release No. 33-10459 (Feb. 26, 2018) available at https://www.sec.gov/rules/interp/2018/33-10459.pdf. As a large law firm with hundreds of public company clients, Covington is regularly in possession of MNPI, the theft of which puts investors at significant risk. Neither Covington's position as a victim of a cyberattack, nor the fact that it is a law firm, insulate it from the Commission's legitimate investigative responsibilities.[6] As shown below, the Subpoena, including specifically Request No.

[5] Covington has refused to provide the Commission with even the names of the clients who the firm admits had MNPI that was potentially accessed by the threat actor. *Id*.

[6] *See, e.g*., FN.1. *See also* Section B., *infra.*

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.