UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

SECURITIES AND EXCHANGE COMMISSION, 100 F Street, NE Washington, DC 20549 Applicant, vs. **COVINGTON & BURLING LLP**, 850 10th St, NW Washington, DC 20268 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.*

3(a), satisfies all requirements for subpoena enforcement. Further, the Subpoena does not infringe on any privilege, compliance with the Subpoena would not violate the D.C. Rules of Professional Conduct, and the Subpoena is not unduly burdensome.

A. Jurisdiction and Venue are Proper

This Court has subject matter jurisdiction to enforce the Subpoena in aid of the Commission's investigation. Congress has explicitly authorized the Commission to seek, and the federal courts to issue, an order compelling compliance with a Commission subpoena if a person refuses to comply. Exchange Act Section 21(c) [15 U.S.C. §§ 78u(c)] and Securities Act Section 22(b) [15 U.S.C. § 77v(b)].[7]

This Court also has personal jurisdiction over Covington. Congress has authorized nationwide service of process for Commission investigative subpoenas. Exchange Act Section 21(b) [15 U.S.C. § 78u(b)]. "When the personal jurisdiction of a federal court is invoked based upon a federal statute providing for nationwide or worldwide service, the relevant inquiry is whether the respondent has had sufficient minimum contacts with the United States...." *SEC v. LovesLines Overseas Mgmt., Ltd.*, No. MISC. 04-302RWRAK, 2007 WL 581909, at *3 (D.D.C. Feb. 21, 2007) (internal citations omitted). In this case, venue for the enforcement of the Subpoena appropriately lies in this district since Respondent's headquarters are located in the District of Columbia and it conducts business here.

B. The Subpoena Satisfies All Requirements for Enforcement

An administrative agency's investigative subpoenas should be judicially enforced if the

[7] The Commission may seek an order requiring compliance with a subpoena upon application because subpoena enforcement proceedings are generally summary in nature, and, under exceptions contained in Rule 81(a)(5) of the Federal Rules of Civil Procedure, can be heard without strict adherence to the Federal Rules. *See e.g., SEC v. Sprecher,* 594 F.2d 317, 320 (2d Cir. 1979); *SEC v. First Security Bank of Utah,* 447 F.2d 166, 168 (10th Cir. 1971).

following criteria are met: (1) its "investigation will be conducted pursuant to a legitimate purpose," (2) the subpoena seeks information that "may be relevant to the purpose," (3) "the information sought is not already within the [SEC's] possession," and (4) all "administrative steps required … have been followed." *United States v. Powell*, 379 U.S. 48, 57-58 (1964) (enforcing IRS subpoena). A court must enforce an administrative subpoena if "the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant." *U.S. Int'l Trade Comm'n v. ASAT, Inc.*, 411 F.3d 245, 253 (D.C. Cir. 2005) (quoting *U.S. v. Morton Salt, Co.*, 338 U.S. 632, 652-53 (1950)). Once these threshold criteria are met, the burden shifts to the opposing party to establish that the subpoena is unreasonable. *SEC v. Brigadoon Scotch Distrib. Co*., 480 F.2d 1047, 1056 (2d Cir. 1973). The burden of showing unreasonableness "is not easily met." *Id*.

1. The SEC's Inquiry Has a Legitimate Purpose

The Commission's Subpoena in this case readily satisfies the standard articulated in *ASAT*, 411 F.3d at 253. First, the Commission's investigation is being conducted pursuant to authority vested in the Commission by Congress. *See* Securities Act Section 20(a) [15 U.S.C. § 77t(a)]; Exchange Act Section 21(a) [15 U.S.C. § 78u(a)]. Congress created the Commission as an independent regulatory agency having the primary responsibility to enforce the federal securities laws and thus primary responsibility to protect the integrity of the nation's capital markets. To that end, Congress gave the Commission broad authority to conduct such investigations as it deems necessary to determine whether any person "has violated, is violating or is about to violate" any provisions of the federal securities laws. Exchange Act Section 21(a) [15 U.S.C. § 78u(a)]. *See also* Securities Act Section 20(a) [15 U.S.C. § 77t(a)] (corresponding provision of the Securities Act granting similarly broad authority); *SEC v. Jerry T. O'Brien, Inc*., 467 U.S. 735, 741 (1984). Further, Congress gave the Commission authority to investigate "any facts,

conditions, practices or matters" that, in its discretion, the Commission deems necessary or proper to aid in the enforcement of the federal securities laws. Exchange Act Section 21(a)(1) [15 U.S.C. § 78u(a)(l)]. Congress specifically authorized the Commission to subpoena witnesses, take evidence, and require the production of books, papers, correspondence, memoranda, or other records that the Commission deems relevant or material to the inquiry. Securities Act Section 19(c) [15 U.S.C. § 77s(c)]. *See also* Exchange Act Section 21(b) [15 U.S.C. § 78u(b)].

The Commission seeks documents to investigate the impact of the Cyberattack on publicly-traded issuers and regulated entities, including those who are Covington's clients. The Commission seeks to understand whether the Hafnium threat actors viewed or exfiltrated MNPI related to any of Covington's public company clients and, if so, for which clients. This information, which is solely in Covington's possession, is critical to advancing the Commission's goal of protecting investors. For example, if the Commission knows which of Covington's public company clients had MNPI accessed, it can use its investigatory tools to identify any suspicious trading in those companies' securities, and investigate whether such trading was part of an illegal trading scheme based on MNPI viewed or exfiltrated as part of the Cyberattack. Similarly, the Commission can investigate whether illegal insider trading occurred based on the knowledge of the Cyberattack on publicly traded issuers.[8] In addition, and to promote its mission of protecting investors, the Commission has a legitimate interest in knowing whether any publicly-traded issuers that had MNPI accessed by the threat actors made all required disclosures to the investing public about any material cybersecurity events in connection with the Cyberattack..

[8] *Former Equifax Executive Charged with Insider Trading* (Mar. 14, 2018) available at https://www.sec.gov/news/press-release/2018-40; *SEC Charges Three Chicago-Area Residents with Insider Trading Around Equifax Data Breach Announcement* (Aug. 16, 2022) available at https://www/sec/gov/litigation/litreleases/2022/lr25470.htm.

To date, Covington has identified 298 clients whose information, while in Covington's possession, was viewed, copied, modified, or exfiltrated by the threat actor. Yet, Covington has consistently refused to provide the names of those clients.[9] In short, the Commission's investigation—and the Subpoena issued to Covington in connection therewith—is within the scope of the Commission's Congressionally-authorized law enforcement powers, and thus has a legitimate purpose.

2. The Information Sought Is Relevant to the Investigation

The Subpoena seeks relevant information. Information is reasonably relevant to an administrative investigation when it is "not plainly incompetent or irrelevant to any lawful purpose of the [agency]." *FTC v. Church & Dwight Co.*, 665 F.3d 1312, 1315 (D.C. Cir. 2011) (quoting *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1992)). When assessing the relevancy of information sought in an administrative subpoena, courts defer to the agency's determination of the scope of their investigative authority. *Id.* at 1316 (citing *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001), and *EEOC v. Lutheran Social Servs.*, 186 F.3d 959, 965 (D.C. Cir 1999)).

As the D.C. Circuit has recognized, the Commission's subpoena power is "co-extensive" with its investigative power, and thus, a conclusion that the subpoena is too indefinite or seeks irrelevant information is essentially "foredoomed by [the Circuit's] holding that the scope of the investigation itself is adequately bounded." *Arthur Young*, 584 F.2d at 1025. That is, "[t]he breadth of an investigation is for the investigators to determine. The breadth of a subpoena … may be excessive, but the test is relevance to the specific purpose, and the purpose is determined by the investigators." *Id*. at 1031 (quotation omitted); *see also Blinder, Robinson,* 681 F. Supp. at 4 (holding that prima facie determination that evidence sought has potential importance in terms of

[9] Again, excepting the two clients who voluntarily agreed to share their names with the Commission.

investigative objectives is sufficient to validate the scope of the request).

The low bar for establishing the relevance required to enforce the investigative Subpoena, and specifically Request No. 3(a), in this matter is easily satisfied here. The Commission is investigating whether there have been violations of the federal securities laws in connection with the Cyberattack. Request No. 3(a) seeks the limited, basic information necessary for the Commission to investigate whether federal securities laws have been violated in connection with the Cyberattack, including (1) whether the threat actors or their affiliates engaged in illegal trading based on MNPI accessed as part of the Cyberattack in violation of Section 10(b) of the Exchange Act, (2) whether others engaged in insider trading based on material, nonpublic knowledge of the Cyberattack, and (3) whether any publicly-traded issuers have failed to disclose any material cybersecurity events in connection with the Cyberattack in violation of, among other things, Section 10(b) of the Exchange Act or Section 17(a) of the Securities Act. The Commission has previously brought enforcement actions for those types of violations of the federal securities laws. *See, e.g.*, *supra* n.1.

3. The Information Sought Is Not Already within the Commission's Possession

The documents sought are not in the Commission's possession. Covington has refused to produce information responsive to Subpoena Request No. 3(a). Additionally, Covington alone is in possession of the names of its clients whose information was accessed or potentially accessed in connection with the breach—information that could be used by a threat actor or others to engage in potential illegal trading. The Commission has no way to obtain this information other than by Subpoena to Covington, as the information regarding which entities' information was accessed by the threat actors is solely in Covington's possession.

While the Commission has proprietary tools to survey the market for potential illicit trading

in the stock of all publicly traded companies, without knowing which companies are Covington's clients, the Commission would be unable to analyze trading patterns that might reveal illegal trading by the threat actors involved in the Cyberattack or others unless it knows which companies had their information accessed. For example, sophisticated threat actors, such as those associated with the Cyberattack, are likely well versed in avoiding routine surveillance. By contrast, knowing the identities of entities whose information was accessed would allow the Commission to conduct targeted analyses on trading in those entities' securities around the time of the unlawful access, vastly increasing the likelihood that the Commission would identify any potential illegal trading by the threat actors or others. Continued delay in the Commission's ability to access this information is damaging to this investigation and investors, as the threat actors may feel emboldened to engage in repeated wrongdoing. Further, without knowing which clients' information was accessed, the Commission will be unable to determine whether those entities made proper disclosures to the public about the Cyberattack. In short, without access to the names of the Covington clients whose information was accessed in the Cyberattack, the Commission will be severely hampered in its ability to investigate violations of the federal securities laws connected to the Cyberattack.

4. All Administrative Requirements Have Been Satisfied

Section 21(b) of the Exchange Act, 15 U.S.C. § 78u(b), provides that the Commission may, in the course of conducting investigations, designate officers and empower them to subpoena witnesses. 15 U.S.C. § 78u(b). Pursuant to Rule 8 of the Commission's Rules Relating to Investigations, investigative subpoenas may be served by several methods, including by any method conveying actual notice. 17 C.F.R. §§ 203.8 and 201.14(b)(3). The federal securities laws authorize the Commission to require the production of any books, papers, or other documents that the Commission deems relevant or material to its investigation. *See* 15 U.S.C. § 77s(c), 15 U.S.C. § 78u(b). Each of those steps was followed here. *See supra* at pp. 2-3. Accordingly, all

administrative requirements have been followed, and the Subpoena is valid and proper.

C. Request No. 3(a) Does Not Call for Protected Information

The Subpoena, including the very narrow Request No. 3(a), does not infringe on any privilege or the D.C. Rules of Professional Conduct. The Subpoena does not call for protected information, and the Commission is not seeking privileged communications between Covington and its clients. Moreover, the Commission has agreed to limit Covington's response to Request No. 3 to only the names of impacted regulated clients, thus eliminating the risk that any attorney-client communications would be responsive to the Subpoena. *See* Ney Decl., Exh. A, ¶ C.3.

1. The Identity of Clients Impacted by the Cyberattack Is Not Privileged

Covington has prepared a list of 298 clients impacted by the Cyberattack, and that list is not protected work product prepared in anticipation of litigation.[10] Initially, documents should only be deemed prepared "in anticipation of litigation," and thus within the scope of the work product doctrine, if "in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation." *United States v. Adlman*, 134 F.3d 1194 (2d Cir. 1998). Documents are not considered work product if they "would have been created in essentially similar form irrespective of the litigation." *Id*. In this case, Covington's list of 298 impacted clients would have been created in essentially similar form irrespective of litigation. Covington compiled the list with the business intention of reaching out to inform clients that their information had been accessed, as Covington informed the Commission it has done. *See* Ney Decl., Exh. B.

Moreover, even to the extent the identity of impacted clients could be considered work

[10] Covington's June 10, 2022 white paper made reference to the attorney-client privilege as well, but only in response to Request No. 3(c), which is no longer at issue as a result of the parties' negotiations. Ney Decl., Exh. B.

product, the information would be factual work-product over which the doctrine is not absolute. Rather, the work product privilege can be overcome upon a showing that the party seeking the information: (1) has substantial need for the materials; and (2) cannot, without undue hardship, obtain their substantial equivalent by other means. *See, e.g.*, Fed. R. Civ. P. 26(b)(3)(A). In this case, Covington indicated that 298 clients had their legal files accessed by the Hafnium threat actors. The Commission is charged with protecting investors from the threat arising from that activity, *e.g.*, potential illegal trading based on information gathered during the attack or based on the occurrence of the attack itself, as well as relevant disclosure obligations for public companies impacted by the attack—hence the Commission's substantial need for the information. In addition, and as previously stated, there is no other place for the Commission to obtain the relevant information as to which regulated companies were impacted. That information is uniquely in Covington's possession as the party whose network was accessed.

2. The D.C. Rules of Professional Conduct Specifically Permit Law Firms to Produce Client Confidential Information in Response to a Valid Subpoena

D.C. Rule of Professional Conduct 1.6 ("D.C. Rule 1.6") subpart (a)(1) generally prevents an attorney from "knowingly . . . reveal[ing] a confidence or secret of the lawyer's client." However, if issued a subpoena, the recipient must comply notwithstanding Rule 1.6, absent some other valid objection. This is because Rule 1.6(e)(2)(a) provides an exception to the general rule, and permits the lawyer to "reveal client confidences or secrets" when "required by law or court order." This court has specifically considered the relationship between Rule 1.6(a) and 1.6(e) in the context of a subpoena seeking communications between a law firm and its clients in a civil action, and determined that a subpoena is a court order subject to exception under the Rule. *See In Re: Motion To Compel Compliance With Subpoena Directed To Cooke Legal Group*, PLLC, 333 F.R.D. 291, 296 (D.D.C. 2019) (granting plaintiff's motion to compel production of the subpoenaed

documents). Specifically, the court in that case held that Rule 1.6 did "not bar [the law firm] from complying with the instant subpoena, but instead specifically permits the firm to do so" because of the application of the Rule 1.6(e) exception. *Id*.

Multiple courts have interpreted similar provisions in state ethics rules to allow the production of documents in response to subpoenas from executive agencies, including subpoenas issued by the Commission. *See, e.g.*, *Selevan v. SEC*, 482 F.Supp.3d 90, 95 (S.D.N.Y. 2020) (citing *Cooke Legal Group* in denying a law firm's motion to quash a Commission subpoena based on "well-established" law that administrative subpoenas qualify as "other law" for purposes of N.J. R. Prof. Conduct 1.6 exception"); *FTC v. Trudeau*, 2013 WL 842599 at *4 (N.D. Ill. March 6, 2013); *SEC v. Sassano*, 274 F.R.D. 495 (S.D.N.Y. 2011) (granting the Commission's motion to compel production of client financial information from law firm because the subpoena constituted law permitting disclosure "absent a valid basis for objection, such as privilege or lack of relevance"). In each of these instances, the courts held that a validly issued subpoena from an executive agency was sufficient to overcome the party's objection under the Rule 1.6(e) exception. The Subpoena's requested information falls squarely within the Rule 1.6(e) exception and requires Covington to produce responsive information.

D. Request No. 3(a) Is Not Unduly Burdensome

The Commission's Subpoena, especially in its narrowed form focusing exclusively on the names of those clients who might have had MNPI viewed or exfiltrated by the threat actors, is extremely limited and seeks information already in Covington's possession. Covington has told the Commission that the number of impacted public company clients is only 298. Covington has already identified—prior to receipt of the Subpoena—the 298 impacted public company clients and the scope of the impact on those clients. Indeed, Covington has already reached out to the clients on multiple occasions and, according to Covington, had substantive communications with the

majority of them regarding the implications of the Cyberattack. Ney Decl., Exh. B. Providing a list of the names of those impacted clients to the Commission is not burdensome.

CONCLUSION

As a result of Covington's refusal to fully comply with the Subpoena, the Commission is unable to gain access to relevant information and documents in an investigation that has been authorized for the protection of public investors, notwithstanding the fact that it has properly served an administrative subpoena. Covington has also not asserted a valid objection for its failure to comply with the Subpoena. Accordingly, the Commission requests that the Court grant this application and issue: (i) an order, in the form submitted, requiring Covington to show cause why it should not be ordered to comply with the Subpoena; (ii) if Covington fails to show adequate cause for its refusal to comply with the Subpoena, an order requiring Covington to comply with Subpoena Request No. 3(a) by providing the names of clients whose information was viewed, copied, modified or exfiltrated by the threat actors; and (iii) such other and further relief as may be necessary and appropriate to achieve compliance with the Subpoena.

Dated: January 10, 2023

Respectfully submitted,

/s/ Dean M. Conway

Dean M. Conway (DC Bar No. 457433)
Securities and Exchange Commission
100 F. Street N.E.
Washington, D.C. 20549
Tel. 202.551.4412
Email: conwayd@sec.gov

Of Counsel:

Lory Stone
W. Bradley Ney