IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Securities and Exchange Commission, Applicant, v. Covington & Burling LLP, Respondent.	Misc. Case No. 1:23-mc-00002

OPPOSITION OF COVINGTON & BURLING LLP TO THE SEC'S APPLICATION FOR AN ORDER COMPELLING COMPLIANCE WITH INVESTIGATIVE SUBPOENA

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

REGULATIONS

RULES

OTHER AUTHORITIES

INTRODUCTION

The SEC asks this Court to compel Covington & Burling LLP ("Covington"), a large, multinational law firm, to produce the names of 296 clients affected by a malicious cyberattack on the firm's network. The SEC's effort to compel Covington to help the agency investigate the firm's clients, without any evidence whatsoever of wrongdoing by Covington or those clients, is an assault on the sanctity and confidentiality of the attorney-client relationship.

While lawyers are not immune from discovery, their clients' time-honored privacy and confidentiality interests should not yield to intrusive government fishing expeditions, especially where all evidence suggests that the cyberattack here was motivated by state espionage objectives unrelated to the securities markets. Before the SEC can force third parties like Covington to divulge private information, the Fourth Amendment demands that it show far more than the purely speculative interest the agency advances here. *See Carpenter v. United States*, 138 S. Ct. 2206, 2221–22 (2018). Accordingly, rather than bless the SEC's application to enforce its March 21, 2022 document subpoena against Covington—an application about which at least one SEC commissioner publicly voiced "concerns"—this Court should reject it in favor of the far more important constitutional protections, professional ethics principles, and societal values at stake.

More than two years ago, a threat actor associated with the Chinese government infiltrated Covington's network and gained access to emails or files associated with some of the firm's clients.[1] Covington promptly contained the threat and reported the breach to the FBI, which is the lead federal agency responsible for investigating cyberattacks. The FBI expressed appreciation

[1] The subpoena at issue asked Covington to identify and produce communications with "public companies" affected by the cyberattack. SEC Ex. A § C. The SEC later told Covington that it should construe "public company clients" to include all SEC-regulated entities, such as brokers, dealers, and exchanges. Meeks Decl. Ex. 1, at 1 n.2. Covington will use "public company" throughout this brief as a proxy for all SEC-regulated entities covered by the subpoena.

for Covington's assistance and conducted its investigation without ever demanding confidential information about, or the identity of, Covington's affected clients.

Fast forward a year, and enter the SEC. Dismissive of Covington's "position as a victim" and "the fact that it is a law firm" that owes fiduciary and ethical duties to its clients, Mem. 5; Ney Decl. Ex. C, at 3,[2] the SEC served a subpoena duces tecum on Covington demanding a broad array of information concerning the cyberattack. Covington promptly and fully responded to nine of the agency's ten document requests, producing "*all* of the documents called for in the subpoena with the exception of documents related to Request No. 3." Mem. 3 (emphasis added).

Request No. 3 demanded that Covington produce documents revealing the names of every public company client affected by the cyberattack, the number and size of files accessed, and all of the firm's communications with those clients about the cyberattack. All told, Request No. 3 sought information about 298 of Covington's public company clients. Covington explained to the SEC that it could not comply with that request consistent with the attorney-client privilege and the firm's fiduciary and ethical duties, including the duty of confidentiality embodied in D.C. Bar Rule of Professional Conduct 1.6. Rule 1.6 requires Covington to protect all information that may be "embarrassing" or "detrimental" to its clients or that "the client has requested be held inviolate."

Covington did, however, try to satisfy the SEC by other means. This included providing information not called for by the subpoena, such as details from its own investigation showing that the threat actor was engaged in geopolitical espionage for the Chinese state—not financial sleuthing. Covington also spent hundreds of hours exhaustively reviewing its affected client files, under the aegis of a firm general counsel and the supervision of a veteran Covington partner with

[2] Covington will use the abbreviation "Appl." to refer to the SEC's application for an order to show cause (Dkt. 1), "Mem." to refer to the SEC's memorandum of law (Dkt. 1-1), and "SEC Exs. A, B, and C" to refer to the exhibits to W. Bradley Ney's declaration (Dkt. 1-2).

20 years of experience in the SEC's Division of Enforcement. Following that investigation, Covington informed the SEC that it had not found material, nonpublic information ("MNPI") in the files of at least 291 of the 298 clients.[3]

Despite all of this, the SEC has been very clear that Covington's clients are in the agency's crosshairs. The SEC says it wants to use the names of those clients to investigate not only whether the hackers engaged in "illegal insider trading" based on information in Covington's files, but also whether Covington's clients made "all required disclosures to the investing public." Mem. 8. In other words, the SEC wants to compel Covington to facilitate the agency's fishing expedition targeting the firm's clients, despite the absence of any evidence to suggest that those clients or anyone else violated the securities laws.

The SEC has not pointed to any suspected violation; instead, it is using the threat actor's wrongful access to Covington's network as an excuse to rummage through protected information to which the SEC would never otherwise have access. By the SEC's logic, once cyber criminals broke into Covington's confidential files, those files suddenly became fair game to federal regulators as well—a collection of information that might prove useful in an open-ended search for violations of the securities laws. The SEC's overly expansive view of its investigatory power should be rejected for several reasons.

First, the names of Covington's clients are privileged under the circumstances of this case, where the SEC inevitably will use those names to leverage additional demands from Covington (and/or from the clients themselves) for privileged communications and work product. Indeed, Request No. 3 itself reflects the SEC's belief that it is entitled to that privileged information, and

[3] Covington could not rule out whether, for seven of the 298 clients, the threat actor had stumbled on MNPI.

reveals that the agency's initial narrowing of its demands is only its first step. For now, the SEC says it wants client names in order "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." Mem. 8. But the agency has no obvious way to determine whether the information contained in Covington's files was both material and nonpublic unless it also plans to press for details concerning the contents of those files. Request No. 3, in other words, is a transparent first step toward a piecemeal dismantling of the fundamental protections for attorney-client communications, attorney work product, and client confidences.

Second, even putting aside privilege, this action represents an unprecedented assault on the privacy and confidentiality interests of Covington's clients and the firm. The SEC argues that it can force Covington to divulge client names on a bare showing of relevance—with relevance "determined by the investigators" themselves. Mem. 7, 9 (citing *United States v. Powell*, 379 U.S. 48, 57–58 (1964)). But the Supreme Court recently cabined the authority on which the SEC relies and barred agencies from exercising such sweeping powers except in cases involving "diminished privacy interests." *Carpenter*, 138 S. Ct. at 2221–22. Where, as here, a federal agency seeks to penetrate a confidential attorney-client relationship, without any evidence of wrongdoing by Covington or its clients, the Fourth Amendment requires the agency to show an investigative need that is sufficiently compelling to overcome legitimate expectations of privacy. The SEC's demand that Covington divulge client names—so that the agency can investigate those very clients—merely "because it wants assurance" that no laws have been violated, falls far short of the *Carpenter* standard. *See* SEC Ex. C, at 3.

Third, even under the antiquated and more lenient standard advocated by the SEC, this Court can and should reject the agency's demand for confidential client information. Indeed, one

of the SEC's lead cases, *United States v. Morton Salt Co.*, 338 U.S. 632 (1950), itself enjoins federal agencies from enforcing subpoenas that impose undue burdens on third parties that are not the target of the agency's investigation. *Id.* at 652–53. Covington undisputedly is not being investigated for any wrongdoing; Covington was the target of the wrongdoers.

Covington has identified no previous case in which the SEC has attempted to raid the files of a third-party law firm whose lawyers *and* clients are not suspected of any wrongdoing. Yet the SEC has pressed ahead with its demand for the names of nearly 300 Covington clients, unreasonably burdening Covington's client relationships even though the agency has multiple other avenues to investigate whether the cyberattack led to any insider trading. This Court should not permit the SEC to forcibly outsource basic investigatory work by turning an unwilling law firm against its own clients. *See, e.g.*, *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174 (1977) (inquiring whether "providing assistance" to the government would be "offensive" to a third party).

Fourth, the SEC's action is dangerously short-sighted and will have broad societal implications. Cyberattacks have become an ever-increasing part of commercial life and have affected many law firms in addition to Covington. *See* Steven Lerner, *Troutman Pepper Hit By Cyberattack*, Law360 (Feb. 9, 2023) (noting Troutman Pepper was only "the latest in the legal industry to suffer a data breach"); Xiumei Dong, *Law Firm Data Breaches Continue to Rise*, Law360 (Feb. 6, 2023) (discussing "100 law firms that reported data breaches to authorities" in 2022); Appendix A (listing recent law firm victims of cyberattacks). As such, the SEC's action threatens a cascading series of dilemmas for law firms with concomitant adverse consequences for law enforcement and our society as a whole: suffer a cyberattack, and, even after cooperating fully with the FBI, expect an SEC subpoena; expect that subpoena to focus on your clients' public disclosures and the related advice and information you may have provided; anticipate the SEC will

share your information with other federal agencies and state attorneys general that might also investigate your clients; given all of this, consider carefully your fiduciary duties and ethical duties of loyalty and confidentiality; ergo, keep your head down, stay off the government's radar, and do not cooperate with the FBI.

In effect, then, the SEC's aggressive new posture toward the victims of cybercrime threatens to chill not only the relationship between public companies and their counsel, but also between the victims of cybercrime and the FBI. It also guarantees new burdens on the federal courts, which must referee inevitable disputes between the SEC and law firms that are ethically bound to resist disclosure. *See* D.C. Bar. Op. No. 124, at 207 (Mar. 22, 1983) (requiring attorneys to resist disclosure of client names in response to agency subpoenas until "the firm has exhausted available avenues of appeal").

Covington's voice here is not a solitary one. The outcry already has been swift and damning. The former chief of the SEC's Office of Internet Enforcement described the agency's enforcement action as "disturbing and unprecedented." John Reed Stark, *Victimizing a Victim Twice: The SEC's Attack on Covington & Burling* (Jan. 12, 2023), https://tinyurl.com/4p5c3e5a. Even one of the SEC's five commissioners, Mark Uyeda, told the press that he has "concerns" about the agency's decision to bring this subpoena enforcement action, emphasizing that "[t]here should be rightful concern about the role of government and to what extent can government authority pierce these relationships." Jessica Corso, *SEC Commissioner Uneasy Over Suit Against Covington*, Law360 (Jan. 12, 2023). Mr. Uyeda rightfully compared the SEC's demand for client names to the subpoenas the agency served on journalists in 2006 demanding that they identify confidential sources—subpoenas that generated such an uproar that the agency was forced to issue new regulations limiting the discovery that could be sought from reporters. *See* 17 C.F.R.

§ 202.10(b) (requiring SEC staff to make "all reasonable efforts" to obtain information from "alternative sources" before issuing subpoena to journalists); *see also* U.S. Dep't of Just. Manual § 9-13.410 (imposing similar requirement for DOJ subpoenas to lawyers).

Despite all of this, the SEC is again demanding to invade a sacred precinct of trust and confidence. This Court should bar the door.

BACKGROUND

I. Covington Was The Victim Of Political Espionage Aimed At Obtaining Information About The Incoming Biden Administration.

On March 2, 2021, Microsoft disclosed that a threat actor had exploited vulnerabilities in its Exchange Server software to gain "access to email accounts" and to install "malware to facilitate long-term access to victim environments." Microsoft Security Blog, *Hafnium Targeting Exchange Servers with 0-Day Exploits* (Mar. 2, 2021), https://tinyurl.com/3h9m4wnh. Microsoft expressed "high confidence" that Hafnium, a group of hackers associated with the Chinese government, had perpetrated the attacks. *Id.* The White House likewise blamed these malicious attacks on the Chinese military. *See* Ben Kochman & Stewart Bishop, *US, Allies Say China Behind Massive Microsoft Server Attack*, Law360 (July 19, 2021). The reach of the cyberattack was enormous, with the hackers targeting the emails or files of "tens of thousands of organisations around the world." Alex Hern, *What Is the Hafnium Microsoft Hack and Why Has the UK Linked It to China?*, The Guardian (July 19, 2021).

Because it uses Microsoft's Exchange Server software, Covington promptly launched an investigation and ultimately determined that a threat actor indeed had infiltrated its Exchange environment. Fagan Decl. ¶¶ 5–6. Until Covington discovered, promptly contained, and remediated the breach, the threat actor undertook a series of malicious activities, including stealing credentials and engaging in search, reconnaissance, and export activity. *Id.* ¶ 8. More specifically,

the threat actor collected email from certain Outlook accounts and accessed folders on dedicated network drives for a small group of lawyers and advisors whose work touches on policy issues or investigations of interest to China. *Id.* ¶ 9; SEC Ex. B, at 5. Upon discovering the incident in March 2021, Covington promptly reported the malicious activity to the FBI and, within a matter of days, began working cooperatively with law enforcement as part of Covington's investigation into the incident. Fagan Decl. ¶¶ 6–7.

II. The SEC Issues A Subpoena Seeking Confidential Client Information Related To the Cyberattack.

Roughly a year later, on March 21, 2022, the SEC served a document subpoena on Covington regarding the Hafnium cyberattack. Appl. ¶¶ 3, 5; SEC Ex. A. The subpoena contained ten document requests, covering when and how Covington learned of the cyberattack; the data, files, or other information that were "viewed, copied, modified, or exfiltrated" in the attack; the dates of the unauthorized activity; and the names of the employees responsible for responding to the incident. SEC Ex. A § C. Covington timely produced documents or provided detailed written responses to nine of the ten requests. Hodgkins Decl. ¶ 16. The SEC acknowledges that those responses were satisfactory. Mem. 3.[4]

Covington, however, objected to Request No. 3—the lone outstanding request—which demands the identity of clients whose files were implicated in the cyberattack *and* production of the firm's communications with those clients concerning "the suspected unauthorized activity":

> **Request No. 3**: Documents and Communications sufficient to identify all Covington clients or other impacted parties that are public companies whose data, files, or other information may have been viewed, copied, modified, or exfiltrated in the course of [the Hafnium cyberattack]. Include in Your production information sufficient to identify the following for each entity:

[4] The SEC misleadingly states that Covington produced a "very small" number of documents pursuant to the subpoena. Mem. 4 n.3. But the SEC fails to advise the Court that Covington also provided detailed narrative responses to many of the SEC's requests.

> (a) 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 (e.g., number of files, size of files, etc.); and
>
> (c) Any Communications provided to the client or other impacted party Concerning the suspected unauthorized activity.

SEC Ex. A § C(3).

Covington understandably viewed this request as a serious and improper intrusion into its confidential client relationships. Hodgkins Decl. ¶ 20. In detailed written objections, Covington explained that it could not comply with Request No. 3 consistent with applicable privilege and work product protections and its fiduciary and ethical duties, including those imposed by Rule 1.6 of the D.C. Bar Rules of Professional Conduct. SEC Ex. B. Rule 1.6(a), for example, instructs that a lawyer "shall not knowingly . . . reveal a confidence or secret of the lawyer's client," and Rule 1.6(b) defines a client confidence or secret not only as "information protected by the attorney-client privilege," but also as "*other* information gained in the professional relationship that the client has requested be held inviolate, or the disclosure of which would be embarrassing, or would be likely to be detrimental, to the client." D.C. Bar R. 1.6(b) (emphasis added).

Covington explained that its communications with its clients concerning the cyberattack were privileged, and in any event, both the communications and the identity of Covington's clients in the context of a cyberattack constituted client secrets—that is, private information the firm was duty-bound to keep confidential. SEC Ex. B, at 6–10. As a result, the SEC's subpoena placed the firm in an unfair and untenable bind: resist disclosure and face a subpoena enforcement action by the SEC, or comply and potentially breach its duties to its clients—none of whom consented to the release of information. *Id.* at 13. Covington's response to this Hobson's choice was, naturally, to protect its clients.

After receiving Covington's objections, the SEC staff proposed a purported "compromise." SEC Ex. C, at 7. The staff asked Covington for (1) all requested information to which Covington's clients would consent, (2) the names of public company clients affected by the Hafnium cyberattack, (3) a description of the scope of the impact on those clients, and (4) Covington's initial communication informing those clients of the cyberattack. *Id.* Even though this asserted compromise was barely distinguishable from the original Request No. 3, Covington communicated the proposal to the 298 public company clients covered by the subpoena. Only one consented to the revised request, and Covington promptly produced to the SEC responsive information regarding that client. Hodgkins Decl. ¶ 24.

Still unsatisfied, the SEC staff threatened a subpoena enforcement action. The staff proposed that it would delay such litigation if Covington would produce "only the names of its impacted public company clients *in the first instance*," instead of all documents and communications demanded by Request No. 3. Meeks Decl. Ex. 1, at 1 (emphasis modified). Yet under the guise of this purported compromise, the staff *broadened* the subpoena by informing Covington that it should construe "public company clients" to include not only companies whose securities trade in public U.S. markets, but also all other SEC-regulated entities, such as broker-dealers and investment advisers. *Id.* at 1 & n.2. The staff also made no guarantee that the proposal would completely resolve the parties' dispute. On the contrary, the staff phrased the offer in conditional and subjective terms: "*If that list is sufficient for our purposes*, we would not seek the additional information. . . ." *Id.* at 1 (emphasis added).

Covington again communicated the staff's offer to the affected clients. This time, one additional client agreed to the disclosure of its name, and only its name, to the SEC. Covington promptly identified that client on August 12, 2022, Hodgkins Decl. ¶ 26, while reiterating to the

staff that it could not produce the names of the other 296 non-consenting clients consistent with its ethical and other duties and obligations.

In late August 2022, Covington went even further to try to accommodate the SEC by providing additional information while protecting its clients' identities and confidences. Covington explained to the staff that the threat actor was engaged in an intelligence operation and did not target Covington's system for insider trading purposes. Fagan Decl. ¶¶ 9–10; Hodgkins Decl. ¶¶ 28–29. Following that presentation, the staff requested that Covington investigate whether the threat actor may have incidentally accessed material, nonpublic information ("MNPI")[5]—including information about nonpublic mergers, investigations, or government approvals—during the course of its illicit intelligence gathering. Hodgkins Decl. ¶ 30.

To fulfill the SEC's request, Covington embarked on an intensive, multi-week review of the client files affected by the cyberattack. Hodgkins Decl. ¶ 31; Ney Decl. ¶ 13. The firm deputized a team of seven review attorneys working under the supervision of a firm general counsel and led by a senior partner who had spent 20 years in the SEC's Enforcement Division, rising to the level of an Associate Director. Hodgkins Decl. ¶¶ 5, 31, 33. Applying well-settled principles, including an assessment of materiality from *Basic Inc. v. Levinson*, 485 U.S. 224 (1988), Covington reviewed the client files to determine whether information viewed by the threat actor was both material and nonpublic at the time of the attack. Hodgkins Decl. ¶ 31. Ultimately, Covington concluded that the client files of only seven of the 298 impacted clients *might possibly* contain MNPI, *id.* ¶ 36; Ney Decl. ¶ 14—a finding that is fully consistent with all available evidence that the cyberattack was an act of geopolitical, rather than corporate, espionage.

[5] Information is "material" for purposes of the securities laws if a "reasonable investor" would view it "as having significantly altered the 'total mix' of information" available concerning a security. *Basic Inc. v. Levinson*, 485 U.S. 224, 231–32 (1988).

Without identifying its clients, Covington reported this conclusion and Covington's methodology to the SEC staff through outside counsel. Hodgkins Decl. ¶ 37. Covington also provided basic information concerning the types of client files that potentially contained MNPI (e.g., documents referencing nonpublic acquisitions or deals) and those that did not (e.g., documents relating to general legal advice). *Id.* ¶ 37. Following multiple rounds of questioning from the staff, for which Covington diligently provided answers, the staff informed Covington that the firm's extensive internal review, involving more than 490 hours of attorney time, had been for naught. *Id.* ¶¶ 34, 39; Ney Decl. ¶¶ 13–14. The staff again demanded that Covington produce the names of *all* 296 as-yet-unidentified clients, no matter how unlikely that their files contained MNPI, or face a subpoena enforcement action. Ney Decl. ¶¶ 15–16. In effect, then, the SEC was fishing in a dead lake, though the staff did purport to narrow the subpoena by deferring, but not withdrawing, their demand for Covington's communications with its clients concerning the cyberattack.

After Covington reiterated yet again that it could not ethically identify its clients absent their consent—which no additional clients had granted—the SEC moved pursuant to 15 U.S.C. § 78u(c) for an order enforcing Request No. 3(a). The agency, for now, has limited its application to client names. Appl. ¶ 5.

ARGUMENT

"By turns both sacred and controversial, the principle of the confidentiality of client information is well-embedded in the traditional notion of the Anglo-American client-lawyer relationship." *In re Gonzalez*, 773 A.2d 1026, 1030–31 (D.C. 2001). The SEC would force Covington to forswear its time-honored obligation to protect client confidences and secrets by divulging the names of 296 clients affected by the Hafnium cyberattack. The SEC admits that it seeks this information to investigate not only the perpetrators of the attack, but also its victims—

Covington's clients—simply to rule out the possibility that those clients violated disclosure obligations under the securities laws (without any evidence to suggest such a violation occurred). Mem. 8; SEC Ex. C, at 3. The SEC's unprecedented request threatens to erode the "confidence and trust" that lies at the heart of the attorney-client relationship, *Trammel v. United States*, 445 U.S. 40, 51 (1980), and it inappropriately demands that Covington serve up its own clients for agency scrutiny.

The SEC has not come close to justifying this overreaching demand. The SEC has offered no evidence suggesting that the attack on Covington's network—an undisputed act of geopolitical espionage—precipitated any illegal trading in securities. In fact, in its letter exchange with Covington, the SEC candidly acknowledged that it is seeking discovery merely to satisfy itself that no violation of the securities laws occurred. SEC Ex. C, at 3. While "official curiosity" may entitle the SEC to discovery in garden-variety cases, *Morton Salt*, 338 U.S. at 652, that lenient standard does not govern actions like this one that implicate the significant privacy and confidentiality interests of clients and their law firm, as the Supreme Court has made clear. *See Carpenter*, 138 S. Ct. at 2221. Indeed, even under the antiquated, more government-friendly standard the SEC advocates, this Court can and should reject the SEC's efforts to co-opt Covington to satisfy its mere curiosity.

I. Covington Could Not Comply With Request No. 3 When Served Because An Administrative Subpoena Does Not Overcome A Law Firm's Ethical And Fiduciary Duties To Its Clients.

The SEC argues that its subpoena overrides the duty of confidentiality Covington owes to its clients because the D.C. Bar Rules of Professional Conduct permit attorneys to divulge client names and communications when "required by law or court order." Mem. 13 (quoting D.C. Bar R. 1.6(e)). A fatal problem with the SEC's argument, aside from ignoring broader duties owed by law firms, is that its administrative subpoena does not qualify as a "law or court order." The SEC

therefore cannot compel production of this information until it satisfies a federal court that its investigative need for this information is sufficiently compelling to overcome the substantial privacy and confidentiality interests of Covington's clients and the firm itself. *See Carpenter*, 138 S. Ct. at 2221.

A. The SEC's Subpoena Demands Information Covington Is Ethically Obligated To Withhold Under Rule 1.6.

Rule 1.6(a) commands that a lawyer "shall not knowingly . . . reveal a confidence or secret of the lawyer's client" without that client's consent. The D.C. Bar has specifically interpreted "secrets" under Rule 1.6 to include "the mere fact that a client is being represented by an attorney." D.C. Bar. Op. No. 124, at 207; *see also* Am. Bar Ass'n Formal Op. 480, at 2 (Mar. 6, 2018) ("Even client identity is protected under Model Rule 1.6.").[6] Here, moreover, the staff is seeking a list of all Covington clients who were affected by the Hafnium cyberattack. The fact that a given client has been affected by the cyberattack is itself a secret under Rule 1.6(b) insofar as it would reveal information the clients have asked Covington to hold "inviolate" and that could prove "embarrassing" or "detrimental" to Covington's clients.

The D.C. Bar has specifically instructed that a law firm "may not automatically comply" with a demand from a federal agency to release client names. D.C. Bar. Op. No. 124, at 207. In the matter at issue in Opinion 124, the IRS directed an attorney to identify his firm's clients in connection with a routine audit of the firm's income tax returns. *Id.* at 206. The Ethics Opinion was clear—"the firm remains under an ethical obligation to resist disclosure until either the consent of the clients is obtained or the firm has exhausted available avenues of appeal with respect to the summons." *Id.* at 207.

[6] ABA Opinion 480 is available at https://www.abajournal.com/files/FO_480_FINAL.pdf.

The D.C. Bar has reiterated this position in other opinions, admonishing that a lawyer has an "ethical duty" to "assert . . . every objection or claim of privilege available to him" in response to a subpoena from "a government regulatory agency" when "fail[ure] to do so might be prejudicial to the client." D.C. Bar Op. No. 214 (Sept. 18, 1990); *see also* D.C. Bar. Op. No. 14, at 80–81 (Jan. 26, 1976) (same); Restatement (Third) of the Law Governing Lawyers § 63 cmt. b (2000) ("A lawyer generally is required to raise any reasonably tenable objection to another's attempt to obtain confidential client information . . . if revealing the information would disadvantage the lawyer's client and the client has not consented").

In fact, had Covington ignored these rules and failed to resist the subpoena, it could have faced possible disciplinary action from the D.C. Bar and civil actions by its clients for breach of fiduciary duty. *See, e.g.*, *In re Koeck*, 178 A.3d 463, 463–64 (D.C. 2018) (affirming 60-day suspension the D.C. Board of Professional Responsibility imposed on attorney whistleblower for disclosures to SEC); *Bode & Grenier, L.L.P. v. Knight*, 821 F. Supp. 2d 57, 65 (D.D.C. 2011) (recognizing that disclosure of client confidences can give rise to an action for breach of fiduciary duty of loyalty); *Sealed Party v. Sealed Party*, No. 04-cv-2229, 2006 WL 1207732, at *19 (S.D. Tex. May 4, 2006) (recognizing "fiduciary duty of confidentiality"); D.C. Bar R. 1.7 cmt. 16 (enshrining lawyer's "duty of loyalty" to client).

B. The SEC's Subpoena Does Not Override Covington's Ethical Duties To Its Clients.

The SEC argues that Covington's duty to safeguard client names is irrelevant because Rule 1.6(e)(2) permits disclosure when "required by law or court order." But the SEC's administrative subpoena is not a "law or court order." Mem. 13–14.

"Subpoenas issued by the Commission are not self-enforcing." *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 741 (1984); *see also* Ralph C. Ferrara & Philip S. Khinda, *SEC Enforcement*

Proceedings: Strategic Considerations for When the Agency Comes Calling, 51 Admin. L. Rev. 1143, 1167 (1999) ("SEC-issued subpoenas are not self-executing."). The targets of SEC administrative subpoenas typically cannot bring motions to quash in the federal courts because such subpoenas "are not self-enforcing, and therefore threaten no sanction for failure to comply." *Fleet/Norstar Fin. Grp. v. SEC*, 769 F. Supp. 19, 20 (D. Me. 1991). Instead, the SEC has "to bring suit in federal court to compel compliance with its process." *Jerry T. O'Brien*, 467 U.S. at 741; *see also* 15 U.S.C. § 78u(c).

Congress thus interposed the federal courts between the SEC and the target of an administrative subpoena as a critical check on the agency's discovery power. And the role of the district court certainly is "not that of a mere rubber stamp, but of an independent reviewing authority called upon to insure the integrity of the proceeding." *Wearly v. Fed. Trade Comm'n*, 616 F.2d 662, 665 (3d Cir. 1980). "The system of judicial enforcement is designed to provide a meaningful day in court for one resisting an administrative subpoena." *Id.*; *see also See v. City of Seattle*, 387 U.S. 541, 545 (1967) (admonishing that an administrative subpoena "will not be the product of . . . unreviewed discretion"); *United States v. Hunton & Williams*, 952 F. Supp. 843, 856 (D.D.C. 1997) ("The enforcement of a subpoena is an independent judicial action, and the court is free to change the terms of an agency subpoena as it sees fit."). Accordingly, given the inherent limits on the agency's power to compel compliance, an SEC subpoena does not qualify as a "law or court order" that overrides the lawyer's duty of confidentiality in Rule 1.6.

The SEC rejoins that "[m]ultiple courts have interpreted similar provisions in state ethics rules to allow the production of documents in response to subpoenas from executive agencies." Mem. 14. But only one of the four cases on which the SEC relies involved an administrative subpoena, and the recipient of that subpoena was *not an attorney* bound by Rule 1.6.

In *Selevan v. SEC*, 482 F. Supp. 3d 90, 91 (S.D.N.Y. 2020), the SEC sought bank records of an account in the name of a corporation's general counsel, which investigators believed functioned as a shadow corporate account. When the general counsel challenged the subpoena, citing his ethical obligations under New Jersey Rule 1.6, the district court found such arguments unavailing because "Rule 1.6 speaks of an attorney's duties to his or her clients—not limitations on access to confidential information once it is out of the attorney's control, *i.e.*, in the possession of a bank subject to an SEC subpoena." *Id.* at 94–95. Although the court went on to state, in dictum, that Rule 1.6 permits an attorney to reveal client-related information "to the extent necessary to comply" with a subpoena, *id.*, a New York federal court's nonbinding interpretation of New Jersey state ethical rules does not override compliance with the D.C. Bar's specific guidance "to resist disclosure until . . . the firm has exhausted available avenues of appeal." D.C. Bar Op. No. 124, at 207.[7]

The three remaining cases cited by the SEC involved subpoenas issued under Rule 45 of the Federal Rules of Civil Procedure in ongoing civil cases—subpoenas that differ fundamentally from the administrative subpoena at issue here. For example, in civil cases, third-party discovery ordinarily does not begin until the defendant has had the opportunity to test the sufficiency of the government's complaint in a motion to dismiss—a procedural safeguard that is absent when an agency serves an administrative subpoena. Additionally, a Rule 45 subpoena issues from a court, not a government agency. *See* Fed. R. Civ. P. 45(a) ("Every subpoena must [] state the court from which it issued."). As one of the SEC's cited cases observes, "a subpoena issued under Rule 45 is

[7] For law firms like Covington that have lawyers and offices in multiple states, determining which states' ethical rules apply to a particular subpoena may involve a complex and burdensome analysis and could precipitate forum shopping by the SEC. Here, the D.C. Bar Rules plainly apply to Covington, a D.C.-based firm served with a subpoena in D.C.

a court order that compels compliance absent some other valid objection." *FTC v. Trudeau*, No. 03-cv-3904, 2013 WL 842599, at *4 (N.D. Ill. Mar. 6, 2013) (emphasis added); *see also Powell*, 379 U.S. at 57 (noting an agency's power to issue administrative subpoenas "is not derived from the judicial function").

Even in the Rule 45 context, where a subpoena may qualify as a "law" under Rule 1.6, a lawyer or law firm is required to reveal confidential client information only where "a valid basis for objection" is "absent." Mem. 14 (quoting *SEC v. Sassano*, 274 F.R.D. 495, 497 (S.D.N.Y. 2011)); *see also Trudeau*, 2013 WL 842599, at *4 (same). Thus, even under the SEC's own cases, a law firm's ethical duty to its clients does *not* yield to a subpoena as long as the firm's objections are not frivolous or insubstantial. Where "any reasonably tenable objection" exists, Restatement (Third) of the Law Governing Lawyers § 63 cmt. b, the D.C. Bar's mandate is clear—the lawyer must "resist disclosure" through and including appeal if necessary. D.C. Bar Op. No. 124, at 207.

In sum, the SEC's administrative subpoena did not overcome Covington's duty under Rule 1.6 to protect the identity of its clients. Covington had an obligation to resist the subpoena and present its objections to this Court, which in turn must evaluate whether Request No. 3 complies with substantive and procedural limits on agency discovery—here, the attorney-client privilege, the work product doctrine, the Fourth Amendment, and Federal Rule 45's proscription on undue burdens to third parties. *See* Fed. R. Civ. P. 81(a)(5) (providing that Federal Rules apply to agency actions to enforce subpoenas). As a New Jersey appellate court explained just a few weeks ago, a reviewing court cannot simply order production of client names, but must instead identify a "sufficient supporting legal or policy-driven reason" why "disclosure of the client's information may be compelled." *Evolution AB v. Marra*, — A.3d —, No. A-3341-21, 2023 WL 350576, at *3 (N.J. App. Div. Jan. 23, 2023). For the reasons more fully explained below, the SEC has not

shown an investigative need "sufficient" to overcome the privacy and confidentiality interests of Covington and its clients. *Id.*

II. This Court Should Deny The SEC's Application Because Client Names Are Privileged Under The Circumstances Of This Case.

Although, as a "general rule," client names fall outside the attorney-client privilege, this Court and others have recognized an exception where "a client's identity is sufficiently intertwined with the client's confidences," or where disclosing the name of the client "would reveal its motive in seeking legal representation." *Cause of Action Inst. v. U.S. Dep't of Just.*, 330 F. Supp. 3d 336, 350 (D.D.C. 2018) (collecting cases). For at least two reasons, this case rests comfortably within that exception.

First, the SEC's demand for client names is only the first step toward an inevitable demand for privileged information and work product. The SEC says that one purpose of its investigation is to determine "whether the Hafnium threat actors *viewed or exfiltrated MNPI* related to any of Covington's public company clients and, if so, for which clients." Mem. 8 (emphasis added). For now at least, the SEC is asking only the second half of that question: "which clients." *Id.* But to investigate an insider trading case, the SEC also will need to ask and answer the first half: "whether the Hafnium threat actors viewed or exfiltrated MNPI" related to those clients. *Id.* In other words, the SEC will need to probe for details about the content of the files accessed by the threat actor—specifically, whether they contained information that was material and nonpublic and could be exploited for insider trading. Where, as here, client names and the content of client files are two closely "intertwined" halves of the agency's inquiry, *see Cause of Action Inst.*, 330 F. Supp. 3d at 350, the attorney-client privilege extends to the names themselves.

Second, the SEC's demand for client names will effectively reveal the content of privileged client communications either in whole or in part. Covington already informed the SEC that, upon

discovering the cyberattack, it sent its affected clients "a very simple message alerting them" to the unauthorized activity and "inviting each client to discuss the matter." SEC Ex. B, at 2. The "great majority" of those clients then had "further substantive communications with Covington" concerning the implications of the cyberattack. *Id.* And those communications in turn may have informed the clients' judgment about whether they were required to disclose the cyberattack to investors. The demand for client names thus would reveal more than which public companies had a relationship with Covington; it would apprise the SEC which clients received specific information and advice from Covington in connection with the cyberattack. In these circumstances, the client names are privileged and work product.[8] *See Cause of Action Inst.*, 330 F. Supp. 3d at 350.

III. This Court Also Should Deny The SEC's Application Because The SEC Has Not Overcome The Substantial Privacy Interests At Stake.

In addition to, and independent of, the privilege argument discussed above, Request No. 3(a) should be rejected because it is an unreasonable fishing expedition that violates the Fourth Amendment. The SEC contends that this Court must enforce that request so long as the agency makes a minimal showing that the information sought is "within [its] authority," "not too indefinite," and "reasonably relevant" to its investigation. Mem. 7 (quoting *U.S. Int'l Trade Comm'n v. ASAT, Inc.*, 411 F.3d 245, 253 (D.C. Cir. 2005)). Not so. As the Supreme Court recently held, the government-friendly test the SEC advocates applies only to "garden-variety

[8] The SEC's enforcement action against Covington has placed all law firms on notice that any future cyberattacks inevitably will result in an intrusive subpoena for client names. As a result, in future cases, a law firm's compilation of affected client names would constitute work product because the firm could reasonably anticipate litigation with the SEC—or another state or federal agency. *See Judicial Watch, Inc. v. Dep't of Justice*, 432 F.3d 366, 369 (D.C. Cir. 2005) (recognizing that work product protection shields "materials prepared in anticipation of litigation"). Covington should be afforded no less protection here than other firms will receive in future cases.

request[s] for information from a third-party witness," not to administrative subpoenas that invade recognized privacy interests. *Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018); *see also In re McVane*, 44 F.3d 1127, 1137–38 (2d Cir. 1995) (applying "more exacting scrutiny" to third-party subpoena that implicated privacy interests); *In re Public Def. Serv.*, 831 A.2d 890, 900 (D.C. 2003) (recognizing that attorney subpoenas "necessitate careful judicial scrutiny").

Because both Covington and its clients have a legitimate expectation of privacy in their attorney-client relationship, the Fourth Amendment requires that the Court balance the SEC's purported "need to search" against "the invasion which the search entails." *Camara v. Municipal Ct. of City & Cnty. of San Francisco*, 387 U.S. 523, 537 (1967). The SEC has not come close to showing that its speculative, untargeted curiosity about client names justifies breaching the relationship of trust and confidence between Covington and its clients—particularly where Covington's comprehensive internal review established that very few, *if any*, compromised files contained MNPI that the hackers could have exploited for insider trading.

A. The Government-Friendly Standard On Which The SEC Relies Does Not Apply To Third-Party Subpoenas Implicating Recognized Privacy Interests.

Relying on a line of cases beginning with *United States v. Morton Salt*, 338 U.S. 632 (1950), and *United States v. Powell*, 379 U.S. 48 (1964), the SEC claims it can insert itself between attorney and client if the agency concludes that the information sought "*may be* relevant" to a "legitimate" investigation, with the relevance determination left to the agency's sole discretion. Mem. 7, 9 (emphasis added); *see also* SEC Ex. C, at 3. But none of the SEC's cases implicates the kind of sensitive and confidential relationships at issue here. As the Supreme Court recently explained, it "has *never* held that the Government may subpoena third parties for records in which a [potential target] has a reasonable expectation of privacy." *Carpenter*, 138 S. Ct. at 2221 (emphasis added); *see also Couch v. United States*, 409 U.S. 322, 336 n.19 (1973) (recognizing

that an "expectation of privacy" can "launch a valid Fourth Amendment claim" in the context of an agency subpoena). The SEC does not even acknowledge this case law in its brief.

In *Carpenter*, the Supreme Court expressly limited *Morton Salt* and *Powell* to administrative subpoenas seeking information over which the targeted entity has a diminished privacy interest. The Court considered the validity of an order compelling third-party wireless carriers to produce cell-site data under the Stored Communications Act, which permits such orders upon a showing that the government has "reasonable grounds to believe" the records "are relevant and material to an ongoing investigation." 138 S. Ct. at 2210–11 (quoting 18 U.S.C. § 2703(d)). Citing *Morton Salt* and its progeny, the government—like the SEC here, *see* Mem. 7—argued that the order was proper "so long as the investigation is authorized by Congress, is for a purpose Congress can order, [and] the documents sought are relevant to the inquiry." U.S. Br. 44–45, *Carpenter v. United States*, No. 16-402, 2017 WL 4311113 (Sept. 25, 2017) (quoting *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 209 (1946)).

The Supreme Court squarely rejected the government's position, which it described as "set[ting] forth a categorical rule . . . subjecting subpoenas to lenient scrutiny without regard to the suspect's expectation of privacy in the records." *Carpenter*, 138 S. Ct. at 2221. The Court expressly distinguished *Morton Salt* and *Powell* because they "contemplated requests for evidence implicating diminished privacy interests or for a corporation's own books." *Id.* at 2222 & n.5. *Morton Salt* involved an FTC subpoena to salt producers for "a complete statement of the prices, terms, and conditions of sale of salt," 338 U.S. at 637, and *Powell* concerned an IRS summons for corporate tax records. Neither salt prices nor tax records subject to an IRS audit implicated any recognized privacy interest vis à vis the government. *See Carpenter*, 138 S. Ct. at 2222 & n.5.

This case falls squarely within the ambit of *Carpenter*, rather than *Morton Salt* or *Powell*,

because Covington's clients have an expectation of privacy in their retention of Covington that "society is prepared to recognize as reasonable." *Carpenter*, 138 S. Ct. at 2213 (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967)). This expectation is reflected in formal and informal rules that require attorneys to protect, and prevent third parties from discovering, the identity of a lawyer's clients—from Rule 1.6 to the common law of fiduciary duty to the Department of Justice's rules restricting when discovery may be sought from lawyers. Indeed, this Court's cases repeatedly have recognized such a privacy interest: "Parties have a legitimate expectation that even the *fact* of their engagement will not become a matter of public knowledge." *Hunton & Williams*, 952 F. Supp. at 857 (emphasis added); *see Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 15 (D.D.C. 2021) (recognizing "privacy interests" in "the precise identity" of a firm's clients); *Thomas v. Nat'l Legal Prof. Assocs.*, 594 F. Supp. 2d 31, 34 (D.D.C. 2009) (recognizing the "ever present fiduciary responsibility that arches over *every aspect* of the lawyer-client relationship" (emphasis added)); *see also In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 180 (4th Cir. 2019) (admonishing that "the government demonstrated a lack of respect" for a law firm's "duty of confidentiality to its clients" by demanding that the firm "furnish . . . a client list").

The SEC argues that neither Covington nor its clients have an interest in withholding the client names because they are not protected by the attorney-client privilege or work product doctrine. Mem. 12. The SEC misses the point. While client names *are* privileged here, *see* Section II, *supra*, privilege does not define the outer boundaries of the clients' privacy interests vis à vis the government. *See Guo Wengui*, 338 F.R.D. at 14–15 ("privilege is not the only consideration here"); *State v. Sugar*, 417 A.2d 474, 480 (N.J. 1980) ("Any interference with the intimate relationship between attorney and client may do profound violence to the individual privacy of the client.").

The D.C. Bar Rules of Professional Conduct reinforce the principle that the client's privacy interest extends well beyond information covered by the attorney-client privilege—and includes the fact of the attorney-client relationship itself. Those rules prohibit lawyers from revealing *any* "information gained in the professional relationship that the client has requested be held inviolate, or the disclosure of which would be embarrassing, or would be likely to be detrimental, to the client," regardless of whether it is privileged. D.C. Bar R. 1.6(a), (b). Indeed, in disciplinary actions, the D.C. Court of Appeals has underscored that a lawyer's duty of confidentiality "extends not only to privileged 'confidences,' but also to unprivileged secrets." *Herbin v. Hoeffel*, 806 A.2d 186, 197 (D.C. 2002). And those secrets include client names. *See* p. 14, *supra*; Am. Bar Ass'n Formal Op. 480, at 2 ("Even client identity is protected under Model Rule 1.6.").

The Justice Department's discovery guidelines further confirm that Covington's clients have a privacy interest in their relationship with the firm that "society is prepared to recognize as reasonable." *Carpenter*, 138 S. Ct. at 2213. Those guidelines allow subpoenas to attorneys only as a last resort and impose various hurdles before they may issue. For example, the Justice Department must have "reasonable grounds to believe that a crime has been or is being committed, and that the information sought is reasonably needed for the successful completion of the investigation or prosecution." U.S. Dep't of Just. Manual § 9-13.410(C)(3). Prosecutors cannot seek discovery from lawyers merely for "speculative" purposes. *Id.* In addition, the Department heads approving the subpoena must satisfy themselves that line attorneys have made "all reasonable attempts" to obtain the information from "alternative sources" and that the need "outweigh[s] the potential adverse effects upon the attorney-client relationship." *Id.* § 9-13.410(B), (C)(5).

While these guidelines may not formally bind the SEC, they reflect a broad consensus,

even among federal law enforcement agencies, that the government cannot invade the privacy of the attorney-client relationship except in unusual circumstances and only on reasonable grounds where the information cannot be obtained from other sources. If the agency principally responsible for enforcing this country's criminal laws can respect the privacy of this relationship, then so too can a civil authority like the SEC.

Clients have a plethora of reasons why they would not want it publicly known they have retained outside counsel, let alone that their confidential files have been compromised by a malicious cyberattack. Hiring a law firm with expertise in a particular area of law may signal that a company is considering a new business venture it is not ready to unveil to regulators or the public. It may suggest that a company faces legal jeopardy, labor unrest, or a government investigation. Retaining a law firm could simply mean that a company wants sophisticated advice behind the scenes for myriad non-public reasons. Indeed, forcing a law firm to identify client names is no different from requiring a psychiatrist, an oncologist, a plastic surgeon, or other physician with a specialized medical practice to reveal patient names—a result that effectively would disclose the patient's private medical condition.

Whatever the reason, the rules requiring lawyers to jealously guard the identity of their clients foster trust that in turn incentivizes clients to communicate frankly and heed their lawyers' advice. In this way, these confidentiality obligations "promote broader public interests in the observance of law and administration of justice." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981); *see also* Thomas J. Snyder, *Attorney-Client Confidentiality Is a Moral Good: Expanding Protections of Confidentiality and Limiting Exceptions*, 32 Geo. J. Legal Ethics 411, 419 (2019) ("Confidentiality is one of the means through which the lawyer serves his or her client as effectively as possible.").

These privacy interests are not diminished because Covington's representation of *some* of these clients may have been disclosed in other circumstances—for example, where Covington publicly filed a brief on behalf of such a client. *See U.S. Dep't of Just. v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 767 (1989) (recognizing a "privacy interest . . . in . . . nondisclosure" may exist "even where the information may have been at one time public"); *see also Carpenter*, 138 S. Ct. at 2217 (recognizing a privacy interest in cell-phone location data although such data traced a suspect's movements throughout "the public sphere"). Many clients have a longstanding relationship with Covington and retain the firm to handle many different matters. Hodgkins Decl. ¶ 11. The fact that some of Covington's work for a client is publicly known does not mean that all such work is known; nor does it mean that all Covington lawyers with particular specialties associated with a particular case or client have been publicly identified.

Indeed, the specific focus of the SEC's investigation here is whether the threat actor accessed information about Covington's clients that was both material and *nonpublic*—e.g., information about trade secrets, proposed mergers, or confidential investigations not yet known to investors. The risk is thus especially high that the SEC's subpoena will expose a client relationship that has not been publicly revealed. To the extent the client relationship *is* publicly known, the SEC can search for this information itself, rather than conscript Covington to do this investigative work for it. *Cf. Powell*, 379 U.S. at 58 (requiring agency to show subpoenaed information "is not already within [its] possession").

Nor are the foregoing privacy interests vitiated simply because the clients affected by the subpoena include publicly traded corporations rather than individuals. Corporations unquestionably enjoy privacy rights under the Fourth Amendment. *See, e.g.*, *Dow Chemical Co. v. United States*, 476 U.S. 227, 236 (1986); *GM Leasing Corp. v. United States*, 429 U.S. 338, 353

(1977); *Wearly*, 616 F.2d at 664 (expressing "concern" that agency subpoena would violate the "constitutional rights" of corporate plaintiff by exposing trade secrets); *cf. Citizens United v. FEC*, 558 U.S. 310, 342 (2010) (recognizing speech rights in "for-profit corporations"). Although *Morton Salt* suggested that corporations enjoy fewer privacy rights than individuals because they "are endowed with public attributes" and "derive the privilege of acting as artificial entities" from the state, 338 U.S. at 652, more recent Supreme Court cases have recognized that only specific, heavily regulated industries—namely, liquor sales, firearms dealing, mining, and running an automobile junkyard—lack any expectation of privacy protected by the Fourth Amendment.[9] *See City of Los Angeles v. Patel*, 576 U.S. 409, 424 (2015). And even if corporations enjoy fewer privacy rights than individuals for *some* purposes, Covington is aware of no case suggesting that corporations enjoy diminished privacy rights *with respect to their attorney-client relationships*. *See United States v. Hubbard*, 650 F.2d 293, 306 (D.C. Cir. 1980) ("the nature of the interest sought to be protected will determine the question whether under given facts the corporation per se has a protectible privacy interest").

Quite apart from the privacy interests of Covington's clients, the firm's lawyers retain an independent interest in the privacy of their business records, including client names. *See Patel v. City of Los Angeles*, 738 F.3d 1058 (9th Cir. 2013) (en banc), *aff'd*, 576 U.S. 409 (2015). In *Patel*,

[9] *Morton Salt*'s reasoning likely has not survived the evolution in the Supreme Court's case law concerning the constitutional rights of corporations. In the First Amendment context, for example, the Supreme Court has abjured *Morton Salt*'s conclusion that the government enjoys a free hand to regulate corporations with limited constitutional oversight because they are artificial entities that exist at sufferance of the state. *See, e.g.*, *Citizens United*, 558 U.S. at 342 ("First Amendment protection extends to corporations"); *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 587–88 (1980) (Rehnquist, J., dissenting) (expressing a solitary view among nine Justices that states have "broad discretion" to regulate the speech of utility companies because the states "created" utilities "to provide important and unique public services"). And the Supreme Court has held that the Due Process Clause prohibits grossly excessive civil punishments against for-profit corporations. *See BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 575 (1996).

for example, the Ninth Circuit held that hotel owners have a Fourth Amendment privacy interest in their guest registries, even though "the hotel records at issue contain information mainly about the hotel's guests," rather than the hotel itself. *Id.* at 1061–62. "That expectation of privacy is one society deems reasonable because businesses do not ordinarily disclose, and are not expected to disclose, the kind of commercially sensitive information contained in the records—e.g., *customer lists*." *Id.* at 1062 (emphasis added); *see also Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 483–84 (S.D.N.Y. 2019) (holding that online home-sharing platforms have their own privacy interest in business records reflecting "guests' names and addresses").

And that expectation carries all-the-more force with lawyers, whose relationship with their clients is uniquely venerated and privileged in our legal system. An attorney's "expectation of privacy" in his "client files" has deep "roots in federal and state statutory and common law and in the United States Constitution, among other sources." *DeMassa v. Nunez*, 770 F.2d 1505, 1507 (9th Cir. 1985). "Indeed, there is no body of law or recognized source of professional ethics in which this 'source' or 'understanding' is lacking." *Id.*

The privacy interests in this case are especially compelling because the SEC's ordinary information sharing practices permit the agency to share any information gleaned from the subpoena with a wide variety of third parties. Indeed, a notice attached to the subpoena here warns Covington that the SEC "often makes its files available to other governmental agencies, particularly United States Attorneys and state prosecutors." SEC Ex. A (p. 33 of PDF). The agency also supplies information to foreign law enforcement agencies, a wide variety of federal regulatory authorities, state bar organizations, members of Congress, the press and the public—including competitors of Covington or its clients. *Id.* at 33–34. The prospect that Covington's attorney-client relationships will be broadly disseminated, without specific notice or opportunity

to object, provides yet another reason to reject the SEC's application here.

** ** **

Carpenter holds that the government cannot compel production of documents implicating a reasonable expectation of privacy unless it obtains "a warrant supported by probable cause." 138 S. Ct. at 2221. Although *Carpenter* was a criminal case, the Supreme Court has extended the probable cause requirement to civil administrative searches that invade recognized privacy interests, as it "surely" would be "anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is suspected of criminal behavior." *Camara*, 387 U.S. at 530, 534. At the same time, the Court saw fit to "vary the probable cause test from the standard applied in criminal cases." *Id.* at 538. In *Camara*, for example, the Court concluded that "the facts that would justify an inference of probable cause" to conduct the search at issue—a municipal health and safety inspection of a residential apartment building—"are clearly different from those that would justify such an inference where a criminal investigation has been undertaken." *Id.*

In this case, the SEC cannot show probable cause, however it is defined. Ultimately, this Court need not decide whether probable cause supplies the standard or how that standard may "vary" when the search is conducted by civil law enforcement authorities. *Id.* That is because "the ultimate measure of the constitutionality of a government search is reasonableness." *Carpenter*, 138 S. Ct. at 2221; *Camara*, 387 U.S. at 539 (same).

Here, the strength of the privacy interests at stake demands a robust reasonableness review. As the SEC candidly acknowledges, it is attempting to raid Covington's confidential files "just because it wants assurance" that no violation of the securities laws occurred. SEC Ex. C, at 3 (quoting *Morton Salt*, 338 U.S. at 643). But "official curiosity" alone, *Morton Salt*, 338 U.S. at

652, is hardly reasonable.

B. This Court Must Balance The Privacy Rights Of Covington's Clients And Covington Itself Against The SEC's Speculative Investigative Interests In This Case.

The Fourth Amendment mandates "a flexible standard of reasonableness," *See v. City of Seattle*, 387 U.S. 541, 545 (1967), that requires "balancing the need to search against the invasion which the search entails." *Camara*, 387 U.S. at 537; *see also Maryland v. King*, 569 U.S. 435, 448 (2013) ("Even if a warrant is not required . . . we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable."); *Delaware v. Prouse*, 440 U.S. 648, 654 (1979) (similar). Here, the SEC's speculative interest and curiosity about whether a securities violation resulted from the attack on Covington's network without even a reasonable suspicion, and contrary to all available information, cannot justify its unprecedented invasion of Covington's attorney-client relationships.

1. The SEC's Subpoena Constitutes A Serious Intrusion Into Covington's Confidential Client Relationships.

"There are few of the business relations of life involving a higher trust and confidence than that of attorney and client." *Stockton v. Ford*, 52 U.S. (11 How.) 232, 247 (1850). "[T]he basic trust between counsel and client . . . is a cornerstone of the adversary system." *United States v. Koblitz*, 803 F.2d 1523, 1528 (11th Cir. 1986); *Linton v. Perini*, 656 F.2d 207, 209 (6th Cir. 1981) (same). This trust is predicated on the expectation that attorneys will keep their clients' confidences and secrets—whatever they may be. *See Swidler & Berlin v. United States*, 524 U.S. 399, 407–08 (1998) ("Knowing that communications will remain confidential . . . encourages the client to communicate fully and frankly with counsel."). "When an attorney unnecessarily discloses the confidences of his client, he creates a chilling effect which inhibits the mutual trust and independence necessary to effective representation." *United States ex rel. Wilcox v. Johnson*,

555 F.2d 115, 122 (3d Cir. 1977).

Time and again, courts have acknowledged the damage that subpoenas can inflict on the attorney-client relationship. In a case involving a grand jury—whose subpoena powers the SEC (albeit erroneously) likens to its own, *see* SEC Ex. C, at 3—the First Circuit explained that "the serving of a . . . subpoena on an attorney to compel evidence concerning a client may: (1) chill the relationship between lawyer and client; (2) create an immediate conflict of interest for the attorney/witness; (3) divert the attorney's time and resources away from his client; (4) discourage attorneys from providing representation in controversial criminal cases; and (5) force attorneys to withdraw as counsel because of ethical rules prohibiting an attorney from testifying against his client." *Whitehouse v. U.S. Dist. Ct. for the Dist. of R.I.*, 53 F.3d 1349, 1354 (1st Cir. 1995).

Indeed, "the mere issuance of the subpoena may undermine the integrity of the attorney-client relationship." *In re Grand Jury Subpoena to Attorney (Under Seal)*, 679 F. Supp. 1403, 1411 (N.D.W.V. 1988); *see also United States v. Rico*, 619 F. App'x 595, 602 (9th Cir. 2015) (acknowledging that "the sanctity of the attorney-client relationship . . . can be threatened when a subpoena directed to another party's attorney is issued"). This is because "[t]he very presence of the attorney in the grand jury room, even if only to assert valid privileges, can raise doubts in the client's mind as to his lawyer's unfettered devotion to the client's interests and thus impair or at least impinge upon the attorney-client relationship." *In re Grand Jury Investigation*, 412 F. Supp. 943, 946 (E.D. Pa. 1976).

Given the threat that attorney subpoenas pose to the attorney-client relationship, federal courts have quashed such subpoenas "even though the subpoenaed materials are not covered by a statutory, constitutional, or common law privilege." *In re Grand Jury Matters*, 751 F.2d 13, 17–18 (1st Cir. 1984). The "potential disruption" that attorney subpoenas cause to "the attorneys'

relationships with their clients" may suffice to render such subpoenas "unreasonable and oppressive" regardless of whether they implicate privilege concerns. *Id.* at 18.

Request No. 3 cuts to the very heart of the relationship of trust between Covington and its clients. If Covington's clients (or any client of any law firm) knew that their attorneys might be forced to disclose their relationship or communications to the SEC simply to assist in the search for potential investigative targets—*including themselves*—the free flow of information between client and attorney would be unduly inhibited. Indeed, even *outside* the attorney-client context, federal courts have declined to compel third parties to assist in federal investigations where doing so "could threaten the trust between [the third party] and its customers and substantially tarnish the [third party's] brand." Mem. & Order, *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, No. 15-mc-1902, Dkt. 29, at 39 (E.D.N.Y. Feb. 29, 2016); *cf. N.Y. Tel. Co.*, 434 U.S. at 174 (instructing lower court to consider whether the third party "ha[s] a substantial interest in not providing assistance" and whether providing assistance would be "offensive to it").

The SEC's subpoena is particularly "offensive" here, *N.Y. Tel. Co.*, 434 U.S. at 174, because the SEC intends to use this information to investigate whether Covington's clients complied with their disclosure obligations (if any) under the securities laws. Mem. 3, 8 (citing Ney Decl. ¶ 18). Few actions could rupture the trust between attorney and client more than a subpoena that forces lawyers to serve up those clients for federal scrutiny. An attorney is supposed to stand *between* his client and the power of the government. *See* 1 McCormick on Evid. § 87 (8th ed. 2022) ("Our system of litigation casts the lawyer in the role of fighter for the party whom he represents."); Albert W. Alschuler, *The Preservation of a Client's Confidences: One Value Among Many or a Categorial Imperative?*, 52 U. Colo. L. Rev. 349, 351–52 (1981) (arguing that a "sense

of fairness" is enhanced when clients engage "the services of other people . . . whose function within the system is to be on their side"). Yet the SEC's subpoena turns advocate into informant, conscripting Covington as a source for investigative leads against its own clients. This Court should not endorse the SEC's heedless subversion of Covington's attorney-client relationships.

The SEC rejoins that "Covington's position as . . . a law firm" does not "insulate it from the Commission's legitimate investigative responsibilities." Mem. 5. Covington has never argued that lawyers enjoy categorical immunity from discovery—the firm fully complied with all requests except for Request No. 3—only that the special nature of the attorney-client relationship precludes enforcement of an administrative subpoena as to confidential information absent a showing of special investigative need. The "strong tradition of loyalty [that] attaches to the relationship of attorney and client . . . would be outraged by routine examination of the lawyer as to the client's confidential disclosures regarding professional business." 1 McCormick on Evid. § 87; *see also* U.S. Dep't of Just. Manual, p. 24, *supra*. Yet that is exactly what the SEC attempts here.

2. The SEC's Speculative Need For Information Concerning Covington Clients Does Not Justify Its Substantial Disruption Of The Attorney-Client Relationship.

The SEC has not identified any "need to search," *Camara*, 387 U.S. at 537, that outweighs the substantial privacy interests of Covington and its clients. The SEC has no evidence that the perpetrator of the cyberattack used or sold any ill-gotten MNPI; nor does it have any reason to believe that any Covington client failed to satisfy its disclosure obligations (if any) under the securities laws. The subpoena is thus an aimless effort "to cast about for potential wrongdoing," *In re Sealed Case (Admin. Subpoena)*, 42 F.3d 1412, 1418 (D.C. Cir. 1994)—that is, "to determine" in the first instance "whether the malicious activity resulted in violations of the federal securities laws to the detriment of investors." Mem. 2; SEC Ex. C, at 3; *see also* SEC Litig. Release No. 25612, *SEC Files Subpoena Enforcement Action Against Law Firm Covington & Burling LLP*

(Jan. 12, 2023) ("The SEC . . . has not concluded that any individual or entity has violated the federal securities laws.").

Absent reasonable grounds to believe a violation of the securities laws has occurred, the SEC cannot rummage through Covington's files or disrupt its attorney-client relationships. *See In re Sealed Case*, 42 F.3d at 1418 (recognizing that a federal agency "cannot rely on its broad investigatory powers to pursue 'other wrongdoing, as yet unknown'"). Indeed, the SEC's justification for the subpoena is especially weak because Covington already provided the agency with evidence from its own exhaustive investigation confirming that the cyberattack sought information of political significance to China, rather than information that could be exploited for insider trading. Fagan Decl. ¶¶ 9–10; Hodgkins Decl. ¶ 29; SEC Ex. B, at 5. Not surprisingly, Covington's analysis found that very little, if any, of the information accessed by the threat actor was MNPI that could be deployed for insider trading. Hodgkins Decl. ¶ 35; Ney Decl. ¶ 14. Although Covington reported these findings to the SEC, the agency has refused to withdraw its demand that the firm identify *every single public company client* affected by the cyberattack, regardless of the likelihood that those client files contain potential MNPI. Ney Decl. ¶¶ 16–17.

The SEC argues that it would abdicate its responsibility to investors if it failed to investigate potential illegal trading or disclosure violations arising from the breach of Covington's network. SEC Ex. C, at 3. But the agency can satisfy its curiosity without trampling the duty of confidentiality Covington owes its clients and those clients' privacy rights. Indeed, the SEC has multiple other avenues for gathering information.

Start with the FBI, "the lead federal agency for investigating cyberattacks and intrusions." FBI.gov, *What We Investigate*, https://tinyurl.com/4hs67pa8. Gurbir Grewal, the director of the SEC's Enforcement Division, told the press that the Covington subpoena "is key to helping the

SEC identify the hackers." Alison Frankel, *The SEC's Subpoena Fight With Covington—A 'Perilous New Course'?*, Reuters (Jan. 12, 2023). But the FBI, which had Covington's extensive cooperation, surely already identified the hackers—or else it appears exceedingly unlikely that the SEC will succeed by strong-arming client names from Covington where the nation's leading cyber enforcement agency has failed.

The SEC also has what it describes as "proprietary tools to survey the market for potential illicit trading in the stock of all publicly traded companies." Mem. 10–11; *see also* Robert A. Cohen and Angela W. Guo, *The SEC and FINRA's Use of Big Data in Investigations . . . and the Implications for Defense Counsel*, 53 Rev. Sec. & Commodities Reg. 125, 127 (2020) (describing such tools).[10] Under the SEC's regulations, exchange members, brokers, and dealers must electronically submit detailed information to the SEC concerning the number of shares involved in particular trades, the transaction price, the date of execution, the relevant account numbers, and the clearinghouse numbers of the exchange members, brokers, or dealers on each side of the transaction. *See* 17 C.F.R § 240.17a-25.[11] The SEC then uses a "specialized tool" called ARTEMIS to analyze this data and "detect potentially complex, more wide-spread patterns of suspicious trading." Cohen & Guo, *supra*, at 127. In fact, this is the "primary" method by which the SEC investigates insider trading. *Id.* The stock exchanges, such as the New York Stock Exchange and NASDAQ, and the Financial Industry Regulatory Authority likewise regularly

[10] This article is available at https://www.davispolk.com/sites/default/files/cohen.pdf.

[11] The commentary to the SEC's final rule describes the process of gathering information from exchange members and brokers in more detail: "[T]he Commission staff regularly sends requests for securities trading records to the most active clearing firms," which must "submit . . . information concerning transactions by all proprietary and customer accounts that bought or sold a security during a specified review period." SEC Final Rule, *Electronic Submission of Securities Transaction Information by Exchange Members, Brokers, and Dealers*, 66 Fed. Reg. 35,836, 35,836 (2001).

surveil the markets to determine unusual trading patterns, which they then pass on to the SEC. *See, e.g.*, SEC Staff Paper on Cross-Market Regulatory Coordination (Dec. 15, 2020), https://tinyurl.com/436ektrv; Hodgkins Decl. ¶¶ 47–50.

The SEC surely could harness these powerful investigative tools to identify suspicious trading, especially alongside the information Covington already provided in response to nine of the agency's ten document requests—including the dates of the cyberattack. And there is nothing to stop the SEC from mining court appearances, securities filings, or other public records to identify clients whose affiliation with Covington may have already become public. But the SEC's own litigation release in this case suggests the agency has not even tried these ready alternatives, instead issuing its intrusive subpoena for client names just as "soon" as it learned of the cyberattack on Covington. SEC Litig. Release No. 25612, *supra*.

The SEC also has the benefit of Covington's thorough review of the affected client files that concluded the threat actor may have gained access to *potential* MNPI concerning only a tiny minority of Covington clients covered by the subpoena. Hodgkins Decl. ¶¶ 35–36.[12] Yet the agency continues to insist on the names of *all* 296 affected clients and has refused to accept the materiality determinations of a well-respected multinational law firm whose review team was led by a veteran partner with 20 years of experience serving in the SEC's Enforcement Division. Mem. 4–5; Ney Decl. ¶¶ 13–17.

[12] The names of the seven clients whose files contained *potential* MNPI are protected work product because they reflect the efforts, opinions, and legal conclusions of Covington's lawyers and were compiled in anticipation of a subpoena enforcement action from the SEC. *See SEC v. Volkswagen Aktiengesellschaft*, No. 19-cv-01391, 2023 WL 1793870, at *2 (N.D. Cal. Feb. 7, 2023) (rejecting SEC's demand that Volkswagen identify the officers and directors whom the company *believed* had certain knowledge on the ground that such information constituted attorney work product). Covington specifically preserved its work product and/or privilege claim when it told the SEC how many of its clients had files that might contain potential MNPI.

Having a list of Covington's affected clients tells the SEC nothing about whether such clients' files had MNPI exfiltrated from them. While the list might expedite the SEC's analysis, mere "administrative convenience" does not entitle the SEC to run roughshod over the privacy rights of Covington's clients and the firm itself. *Cf. Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2376 (2021) (describing "administrative convenience" as a "weak" justification for a California rule requiring mandatory disclosure of donor names to the state attorney general). Nor does it justify the substantial burdens the subpoena places on Covington, which "remains under an ethical obligation to resist disclosure until . . . the firm has exhausted available avenues of appeal." D.C. Bar Op. No. 124, at 207. A subpoena that drains the resources of an innocent third party like Covington and forces it into litigation is a quintessential example of an unreasonable search. *Accord* Fed. R. Civ. P. 81(a)(5) (providing that Federal Rules, including Rule 45(d)(1)'s injunction against undue burdens on subpoena recipients, apply to agency actions to enforce subpoenas); *see also* pp. 41–42, *infra*.

Covington has found *no* case in which a federal court has compelled a disinterested third-party law firm to produce client names or communications in response to an SEC subpoena, nor has the SEC pointed to one. Instead, courts have exercised their authority to enforce agency subpoenas in two limited circumstances—neither of which exists here. The first is where the federal agency has reasonable grounds to suspect that either the firm or its clients have violated the law. *See, e.g.*, *Taylor Lohmeyer Law Firm PLLC v. United States*, 957 F.3d 505 (5th Cir. 2020) (enforcing IRS summons for client names where agency had reason to believe that firm was assisting clients in avoiding federal taxes).[13] The second is where the firm serves as a federal

[13] Other examples include *United States v. Cal. Rural Legal Assistance, Inc.*, 722 F.3d 424 (D.C. Cir. 2013) (enforcing inspector general's subpoena to nonprofit legal services group for client names where group was the subject of a complaint that it was violating statutory limitations on use

contractor and the agency seeks to ensure compliance with federal program guidelines. *See Adair v. Rose Law Firm*, 867 F. Supp. 1111 (D.D.C. 1994) (enforcing inspector general's subpoena against law firm that entered legal services agreements with FDIC while allegedly failing to disclose other client relationships that created a conflict of interest). Because neither of these circumstances is presented here, the SEC's speculative targeting of the files of an innocent third-party law firm is wholly without precedent.

If the Court enforces this subpoena, it surely will not be the last. The SEC proclaims that the "significance and importance of cybersecurity issues to the Commission's mission has never been more apparent." Mem. 5; *see also* Robert L. Hickok et al., *Cyber Breaches Pose Risk of SEC Enforcement Actions, Derivative Suits to Public Companies*, Law.com (Aug. 29, 2022) (noting that the SEC plans to expand staffing "to pursue more cyber-related enforcement actions"). As more law firms increasingly become victims of cyberattacks exploiting software vulnerabilities or otherwise, these pernicious invasions of privacy will soon be followed by a second invasion—demands by the SEC (or another federal agency) for their confidential client names and communications. Every lawyer in private practice and the companies and people they represent would be threatened by the consequences of a decision favoring the SEC in this action.

Indeed, consider the next case where the SEC pursues a smaller firm with fewer clients rather than a 1,300-lawyer firm with the resources to litigate to uphold its clients' rights. If the SEC prevails here, the agency's inevitable subpoenas could cause even greater harm to small firms and solo practitioners that have the same ethical duties (but not the same resources) to resist

---

of grant money); *United States v. Servin*, 721 F. App'x 156, 159 (3d Cir. 2018) (sustaining IRS summons requiring attorney to disclose client list as part of investigation into attorney's own tax arrears); *Sassano*, 274 F.R.D. at 497 (enforcing a subpoena to law firm for client financial records where client was in arrears on judgment payable to SEC).

disclosure, as well as of course their clients.

The federal courts will also suffer the consequences of the SEC's overreaching. Lawyers confronted with a subpoena demanding client confidences and secrets have an ethical obligation to oppose the subpoena, through and including an appeal if necessary. *See* pp. 14–15, *supra*. As a result, each and every attorney subpoena will precipitate litigation. The Department of Justice has wisely avoided burdening the courts with these actions by serving attorney subpoenas only as a last resort. *See* p. 24, *supra*. The judiciary's interest in docket management is yet another reason for limiting the SEC's blatant fishing expedition in this case.

3. The SEC's Attempt To Take Discovery From The Innocent Victims Of Cyberattacks Undermines Law Enforcement Interests More Generally.

The SEC's speculative interest in enforcing its subpoena here is ***not*** synonymous with the government's interests more generally. On the contrary, recent comments from the FBI Director suggest the SEC's investigative demand to Covington—a cybercrime victim—places it at cross purposes with other federal law enforcement agencies, which depend on the cooperation of private entities like Covington to identify, report, and remediate cyberattacks. Subpoenas like the one at issue here are a powerful disincentive to act as good citizens and provide that cooperation.

Combatting cybercrime presents a unique challenge for the federal government because, unlike traditional threats to national security, "[c]yber is the sole arena where private companies are the front line of defense." President's Nat'l Infrastructure Advisory Council, *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure* 3 (Aug. 2017), https://tinyurl.com/yc8cwupj. For this reason, federal law enforcement has consistently emphasized the importance of enlisting the private sector as an ally in countering cyber threats. As FBI Director Christopher Wray observed: "If American businesses don't report attacks and intrusions, we won't know about most of them, which means we can't help you recover, and we

don't know how to stop the next attack, whether that's another against you or a new attack on one of your partners." Christopher Wray, *FBI Partnering With the Private Sector to Counter the Cyber Threat,* Fed. Bureau of Investigation (Mar. 22, 2022), https://tinyurl.com/2s3suvn9. Chris Inglis, the national cyber director in the Executive Office of the President, echoed these comments, noting that private-public "partnerships can identify and address threats far more effectively than a single organization operating alone." Chris Inglis & Harry Krejsa, *The Cyber Social Contract: How to Rebuild Trust in a Digital World*, Foreign Affairs (Feb. 21, 2022), https://tinyurl.com/3pz6b5u3.

But this cooperation between the federal government and the private sector is imperiled when agencies effectively punish law firms that come forward with information about possible cyberattacks by reflexively slapping them with a subpoena to serve up their clients for investigation.[14] For example, in the wake of a zero-day vulnerability in the Log4j Java logging library, the Federal Trade Commission began threatening legal action against companies whom it deemed to be too slow to patch their systems. *See* Carly Page, *FTC Warns of Legal Action Against Organizations That Fail to Patch Log4j Flaw*, Tech Crunch (Jan. 5, 2022), https://tinyurl.com/yc2xunnj. This—and other instances in which "the government is perceived as confrontational" in responding to cybersecurity threats—was cited as a source of "distrust between the public and private sectors" at recent roundtables between senior government officials and private sector executives. Eugenia Lostri, James Andrew Lewis & Georgia Wood, *A Shared Responsibility: Public-Private Cooperation for Cybersecurity*, Center for Strategic & Int'l Studies 6 (Mar. 2022), https://tinyurl.com/y93mvrrd.

In an effort to rebuild the trust that is essential to presenting a united defense against

[14] The SEC probably learned about the cyberattack from the FBI. But the mere possibility that such information will pass from one law enforcement agency (including the FBI) to another agency (including the SEC) plainly will deter future cooperation with the FBI.

cybersecurity threats, FBI Director Wray has assured private sector leaders that "we're not asking you for information so we can turn around and share it with regulators looking into the adequacy of your cybersecurity after a breach." Wray, *Working With Our Private Sector Partners to Combat the Cyber Threat*, Fed. Bureau of Investigation (Oct. 28, 2021), https://tinyurl.com/374uz69y. Instead, "[o]ur investigators are laser-focused on the bad guys." *Id.* Notably, he made these comments in detailing the federal government's response to the Hafnium attack. Yet the SEC has done precisely what Director Wray said the FBI would not do—target the victims of a malicious cybercrime based solely on their status as victims. If successful, the long-term effect of the SEC's effort will be to disincentivize law firms from voluntarily reporting cyberthreats or providing more than the bare minimum information needed to contain the threat. Not only will this new regime deprive law firms of the sophisticated tools in the FBI's arsenal for responding to cyberthreats, but it will also frustrate the FBI's and other agencies' interest in encouraging voluntary cooperation by the private sector.

IV. This Court Should Deny The SEC's Motion To Enforce The Subpoena Even Under The *Morton Salt* Standard The Agency Advocates.

Even under the more government-friendly standard advanced by the SEC, this Court should not enforce Request No. 3, because compliance would be unreasonable and otherwise "unduly burdensome" to Covington. *See v. City of Seattle*, 387 U.S. at 544; *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1992). *Morton Salt* itself instructs that "the disclosure sought shall not be unreasonable." 338 U.S. at 652–53; *see also EEOC v. Aerotek, Inc.*, 815 F.3d 328, 333 (7th Cir. 2016) ("Under . . . the *Morton Salt* test, disclosure may be restricted where it would impose an unreasonable or undue burden on the party from whom production is sought."); *SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1031–33 (D.C. Cir. 1978) (similar). This limitation is also embedded in the Federal Rules of Civil Procedure, which prohibit the SEC from "imposing

undue burden or expense on a person subject to the subpoena." Fed. R. Civ. P. 45(d)(1); *see also* Fed. R. Civ. P. 81(a)(5) (incorporating Federal Rules into agency subpoena enforcement proceedings in federal court).[15]

The burdens imposed by Request No. 3 are closely intertwined with the ethical obligations Covington owes its clients, which distinguish a law firm from a typical third-party subpoena recipient. For all of the same reasons explained in Section III.C, *supra*, the subpoena places serious burdens on the attorney-client relationship. Beyond these burdens, however, are the substantial costs Covington has incurred as a result of its obligation under the D.C. Bar Rules of Professional Conduct "to resist disclosure" of client names and confidences in response to the subpoena until it has "exhaust[ed] available appeals." D.C. Bar. Op. No. 124, at 208; D.C. Bar R. 1.6(a).

For Covington, that resistance has consisted of an extensive pre-litigation effort to explain its ethical obligations to the SEC and provide information to satisfy the agency's investigative demands without divulging client names or communications. Either directly or through outside counsel, Covington exchanged detailed letter briefs with the agency, SEC Exs. B, C; participated in more than 20 telephone or video conferences with the SEC's staff attorneys; and gave a lengthy presentation to supervising SEC attorneys explaining the basis for Covington's conclusion that the cyberattack was an act of political espionage unlikely to result in insider trading. Meeks Decl. ¶ 4; Hodgkins Decl. ¶¶ 21, 29. Covington also undertook an exhaustive review of its compromised client files, involving at least 490 hours of attorney time, confirming that only a tiny fraction of affected clients had files that even potentially contained MNPI. Hodgkins Decl. ¶¶ 34–36.

[15] The SEC argues in a footnote that this subpoena enforcement action "can be heard without strict adherence to the Federal Rules." Mem. 6 n.7 (citing *SEC v. Sprecher*, 594 F.2d 317, 320 (2d Cir. 1979)). The SEC appears to mean only that it can bring a subpoena enforcement action as a "summary" proceeding without filing a civil complaint. *Id.* Covington does not understand the SEC to argue that it can somehow avoid the undue burden restriction in Rule 45.

Covington's negotiations with the SEC have spanned more than ten months and consumed hundreds of attorney hours. Through it all, Covington engaged in repeated rounds of communication with its nearly 300 affected clients, whether (a) at the SEC's behest to inquire whether the clients would consent to disclosure, or (b) to keep the clients "reasonably informed" about the discussions with the SEC. D.C. Bar R. 1.4(a). Those communications alone were a formidable task given the sheer number of clients covered by the vastly overbroad subpoena. Hodgkins Decl. ¶¶ 24, 26.

Nor could Covington reduce its burden by disclosing only the names of clients whose affiliation with Covington was already public. Even when a law firm's representation becomes known to third parties, the D.C. Bar's Rules of Professional Conduct prohibit the firm from making *cumulative* disclosures without the consent of the client. As noted, the D.C. Bar instructs that, "even if the fact of representation were known by someone other than the attorney or client, . . . [it] could still constitute a 'secret' if the avoidance of additional disclosure was, nevertheless, desirable." D.C. Bar Op. No. 124, at 207; *see also* Am. Bar Ass'n Formal Op. 480, at 3 ("The duty of confidentiality extends generally to information related to a representation . . . without regard to the fact that others may be aware of or have access to such knowledge."). Here, Covington's clients have every reason to "desir[e]" that Covington "avoid[] additional disclosure" of their identity to the SEC—and they have so instructed Covington—because the agency intends to use that information to investigate those clients for possible disclosure violations and otherwise.

Furthermore, even if Covington were permitted to identify only those clients whose representation was already public, actually doing so is no easy task and still would require client consent in any event. For example, Covington could start by determining whether it had entered appearances in court for litigation clients affected by the data breach, but it would then need to

take the additional step of determining whether the files accessed in the cyberattack concerned that litigation or other matters that never became public.

For transactional clients, Covington would need to undertake a search of securities filings, news stories, or other records to determine whether these representations were ever publicly reported. Here, too, it would need to ascertain whether the files accessed in the cyberattack involved those deals or other, unrelated transactions. Covington also would need to make a judgment whether representations reported years in the past—say, in an article from 2010 that remains behind a paywall—remain "public" in any meaningful sense. In short, even if this proposal were acceptable to the SEC, it would impose multiple undue burdens on Covington. If the SEC wishes to identify client relationships that are already public, it can run those searches itself, rather than conscript Covington to do the agency's spadework for it.

Forcing Covington to undertake any of these burdens is particularly unreasonable in light of the firm's status as an innocent third party. Courts are "reluctant" to allow federal agencies to pursue even legitimate investigative needs by burdening "third parties who were not targets of the agency's investigation." *In re McVane*, 44 F.3d at 1137; *see also Arthur Young & Co.*, 584 F.2d at 1031–33 (recognizing that agencies must limit burdens on third parties who are "not the primary target" of an investigation); Fed. R. Civ. P. 45(d)(1), 81(a)(5). Yet here the SEC has forced Covington into an expensive, nearly year-long fight to safeguard its client information even though the firm is neither regulated by the SEC nor accused of any wrongdoing. This Court should not permit the SEC to victimize the firm twice over.

CONCLUSION

For all of the foregoing reasons, this Court should discharge the order to show cause and deny the SEC's application for an order compelling compliance with Request No. 3(a) in the March 21, 2022 subpoena issued to Covington.

Dated: February 14, 2023

Respectfully submitted,

/s/ *Kevin S. Rosen*

Theodore J. Boutrous Jr. (D.C. Bar 420440)
Kevin S. Rosen (*pro hac vice*)
Samuel Eckman (*pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, CA 90071-3197
tboutrous@gibsondunn.com
krosen@gibsondunn.com
seckman@gibsondunn.com

Richard W. Grime (*pro hac vice*)
Katherine Moran Meeks (D.C. Bar 1028302)
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
rgrime@gibsondunn.com
kmeeks@gibsondunn.com

Attorneys for Respondent Covington & Burling LLP

CERTIFICATE OF SERVICE

I, Kevin S. Rosen, hereby certify that on February 14, 2023, I caused the foregoing Opposition of Covington & Burling LLP to the SEC's Application for an Order Compelling Compliance with Investigative Subpoena to be filed and served on counsel of record via CM/ECF. All parties required to be served have been served.

s/ *Kevin S. Rosen*

APPENDIX A

Law Firms that Have Suffered Recent Cyberattacks

Source: Xiumei Dong, *Amid BigLaw Data Attacks, Breaches Surge for Smaller Firms*, Law360 (June 15, 2022)

	LAW FIRMS
1.	Anderson McPharlin & Conners LLP
2.	Ansell Grimm & Aaron PC
3.	Aronsohn Weiner Salemo & Kaufman PC
4.	Axley Brynelson LLP
5.	Ballisle Family Law Legal Counsel C
6.	Barclay Damon LLP
7.	Bayard PA
8.	Bird Marella Box Wolpert Nessim Drooks Lincenberg & Rhow PC
9.	Black Mann & Graham LLP
10.	Bleakley Platt & Schmidt LLP
11.	Bricker & Eckler LLP
12.	Brownstein Rask LLP
13.	Brubaker Connaughton Goss & Lucarelli LLC
14.	Brunini Grantham Grower & Hewes PLLC
15.	Bryce Downey & Lenkov LLC
16.	Burns Figa & Will PC
17.	Charles J. Hilton & Associates
18.	Chiesa Shahinian & Giantomasi PC
19.	Christensen O'Connor Johnson Kindness PLLC
20.	Cleary Gottlieb Steen & Hamilton LLP
21.	Cohen Milstein Sellers & Toll PLLC
22.	Colin Rockey Hackett Law PC
23.	Colligan Law LLP
24.	Corbally Gartland and Rappleyea LLP
25.	Costello Cooney & Fearon PLLC
26.	Coughlin & Gerhart LLP
27.	D'Aurizio Law Firm PLLC
28.	Daniels Porco & Lusardi LLP
29.	Davis O'Sullivan & Priest LLC
30.	DeCotiis FitzPatrick Cole & Giblin LLP
31.	Devine Millimet & Branch
32.	Dodds Hennessy & Stith LLP
33.	Duncan Disability Law SC
34.	Dutton Daniels Hines Kalkhoff Cook & Swanson PLC
35.	Edwards Law Office PC
36.	Fay Sharpe LLP
37.	Finnegan Henderson Farabow Garrett & Dunner LLP

38.	Flaherty Salmin LLP
39.	Fletcher Tilton PC
40.	Foley & Lardner LLP
41.	Foster LLP
42.	Frankel Wyron LLP
43.	Freund Freeze & Arnold LLP
44.	Fross Zelnick Lehman & Zissu PC
45.	Gilbride, Tusa, Last & Spellane LLC
46.	Gilmore Rees & Carlson PC
47.	Gonzales Gonzales & Gonzales Immigration Law Offices
48.	Goodspeed & Merrill dba Rome LLC
49.	Goodwin Procter LLP
50.	Goosmann Rose Colvard & Cramer PA
51.	Granderson Des Rochers LLP
52.	GreeneHurlocker PLC
53.	Grund & Leavitt PC
54.	Hannis T. Bourgeois LLP
55.	Harris Altman PC
56.	Hartzog Conger Cason
57.	Heidell Pittoni Murphy & Bach LLP
58.	Hinkhouse Williams Walsh LLP
59.	Holmes Yates & Johnson
60.	Howard Law LLC
61.	J.V. Dell PC
62.	Kahan Kerensky Capossela LLP
63.	Kasting Kauffman & Mersen PC
64.	Kaufman Dolowich & Voluck LLP
65.	Kleinberg Lang Cuddy & Cario LLP
66.	Knych & Whritenour LLC
67.	Kohn Law Firm
68.	Krupnik & Speas PLLC
69.	Law Offices of Pullano & Farrow PLLC
70.	Levinson Arshonsky & Kurtz LLP
71.	Lightfoot Franklin & White LLC
72.	Lippes Mathias Wexler Friedman LLP
73.	Locks Law Firm
74.	Long & Levit LLP
75.	Morgan Brown & Joy LLP
76.	Norwood, Armstrong & Stokes PLLC
77.	Offitt Kurman PA
78.	Olson Remcho LLP
79.	Payne and Fears LLP
80.	Peabody & Arnold LLP
81.	Phillip Galyen
82.	Pietragallo Gordon Alfano Bosick & Raspanti LLP

83.	Porter Hedges LLP
84.	Robbins Salomon & Patt LTD
85.	Rushton Stakely Johnston & Garrett PA
86.	Ryan Swanson & Cleveland PLLC
87.	Sachs Sax Caplan PL
88.	Schiller DuCanto & Fleck LLP
89.	Schlam Stone & Dolan LLP
90.	Schochor Federico & Staton PA
91.	Schultz & Pogue LLP
92.	Sher Tremonte LLP
93.	Sherin and Lodgen LLP
94.	Sims & Campbell
95.	Siskind Susser PC
96.	Steven & Lee
97.	Stokes Law Office PLLC
98.	Stone Pigman Walther Wittmann LLC
99.	Taylor Ganson & Perrin LLP
100.	Thaler & Thaler PC
101.	The Law Office of Sue E. Berman
102.	The Law Offices of Joseph L. Bornstein
103.	Triangle Property Law PC
104.	Trustlawyer LLC
105.	W&D Law LLP
106.	Waller Lansden Dortch & Davis LLP
107.	Ward Arcuri Foley & Dwyer Law Firm
108.	Waters & Kraus LLP
109.	Weiss Zarett Brofman Sonnenklar & Levy PC
110.	White & Associates
111.	White Arnold & Dowd PC
112.	Wiggin and Dana LLP
113.	Wolfsdorf Rosenthal LLP
114.	Ziegler Metzger LLP