GIBSON DUNN

Gibson, Dunn & Crutcher LLP

1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Tel 202.955.8500
www.gibsondunn.com

FOIA CONFIDENTIAL TREATMENT REQUESTED

June 10, 2022

Ms. Lory Stone
Mr. W. Bradley Ney
Division of Enforcement
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549

Re: *In re Microsoft Hafnium Cyberattack*, HO-14224

Dear Ms. Stone and Mr. Ney:

We represent Covington & Burling LLP ("Covington" or "the Firm") in connection with the above-captioned investigation and are submitting this letter to explain why Rule 1.6 of the D.C. Bar Rules of Professional Conduct, the attorney-client privilege, the work product doctrine, and general duties pertaining to client confidentiality prohibit Covington from complying with the single outstanding request in the Staff's March 21, 2022 investigative subpoena (the "Subpoena"). Covington already has complied with all other aspects of the Subpoena. However, absent informed client consent or a court order, Covington ethically cannot comply with Request No. 3 by providing to the Staff the names of its clients affected by a cyberattack on the Firm, much less its communications with those clients concerning that attack.

Covington and its clients were the victims of a crime, evidently perpetrated by a nation-state engaged in espionage. Covington fully cooperated with law enforcement and undertook a considerable effort to identify and inform its affected clients. A year later, the Staff apparently considers this incident an opportunity to obtain confidential client information in the hope that it might turn up some investigative leads. The Staff's attempt to pry client confidences from an innocent law firm to assess whether any securities violations have taken place charts a perilous new course that threatens to chill the relationship between public companies and their counsel.

Nonetheless, Covington has contacted (or is in the process of contacting) approximately 300 publicly traded clients and certain other regulated clients affected by the Hafnium cyberattack to inform them of the Staff's demand and ask whether they consent to the disclosure of their identity and communications. Absent such consent, we are writing to explain the many legal and policy reasons why the Staff should not seek a court order forcing Covington to comply with Request No. 3. Requiring Covington to identify its clients affected by the cyberattack and turn over related communications would be an unprecedented and unwarranted invasion of, and burden on, Covington's confidential attorney-client

relationships, and it will have serious, adverse consequences for law firms and their clients in their interactions with the SEC and other federal agencies in the future.

As described in more detail below, Covington has no discretion in this situation; it cannot comply with Request No. 3 under the current circumstances and still uphold its professional obligations to its clients. Rather than pursue this matter to subpoena enforcement, we ask that the Staff consider the multiple compelling reasons for withdrawing its demand for the names of clients affected by the cyberattack on Covington and the Firm's related communications with those clients. The Staff has made clear that it views this matter as one of high importance; the same is true for Covington and, indeed, for all lawyers in private practice. As indicated in the concluding paragraph of this letter, we request a meeting to discuss these concerns if this letter does not persuade the Staff to withdraw this last remaining request in the Subpoena.

I. SUMMARY OF RESPONSES & OBJECTIONS

At its most fundamental level, Request No. 3 requires Covington to identify potential subjects for the Staff to investigate from the ranks of the Firm's own clients. Although the Staff has suggested that it is focused on potential unlawful trading in the securities of Covington clients, it has expressly left open the possibility that it will investigate the clients themselves for potential violations of the federal securities laws, including whether Covington clients adequately disclosed the Hafnium cyberattack. That the Staff would even ask Covington to serve up its own clients for agency scrutiny is deeply troubling. Covington has no choice but to decline this overreaching request for at least five reasons.

First, Covington is obligated to protect attorney-client communications and attorney work product. Covington does not have the option of complying with the Staff's demand to produce Covington's attorney-client privileged communications concerning the Hafnium cyberattack, nor information arising from Covington's investigation of the cyberattack, which is attorney work product in which both Covington's clients and the Firm itself have well-established, protected interests. When Covington learned of the unauthorized activity on its network, the Firm contacted certain clients—a universe that the Firm arrived at based on an analysis of the nature of the information suspected of having been accessed and Covington's work for each client—with a very simple message alerting them to that fact and inviting each client to discuss the matter. The great majority of those clients had further substantive communications with Covington, either orally or in writing, and to considerably varying degrees, but in all cases reflective of attorney-client communications and attorney work product. Covington is ethically bound not to disclose any of those privileged communications or work product materials.

Second, Covington is duty-bound to protect the names of clients potentially impacted by the cyberattack. Clients hire Covington for their most serious and sensitive matters, and they expect the Firm to hold all information provided, including the fact of their representation, in the strictest confidence. From Covington's perspective, maintaining the

sanctity of these client relationships is not simply a business imperative, but a mandate imposed by applicable law and the District of Columbia Bar. These ethical rules require the Firm, as well as all other attorneys licensed in D.C., to interpose objections and "resist disclosure" of a client's identity in response to an agency subpoena until either "the consent of the clients is obtained or the firm has exhausted available avenues of appeal." D.C. Bar Op. No. 124, at 207 (March 22, 1983); D.C. Rule of Professional Conduct ("D.C. Rule") 1.6(a), (b).

The Staff, however, takes the position that it is entitled to discover the "names" of clients affected by the cyberattack because a law firm's client roster is not privileged. We respectfully disagree. What the Staff seeks is not simply a list of all clients, but a list of clients with whom Covington determined it should communicate about the cyberattack and invite a dialogue. Such a list would reveal client "secrets"—that those clients on the list are represented by Covington and were affected by the cyberattack on their law firm. *See* D.C. Rule 1.6(b). The fact that particular clients heard from Covington is attorney work product, because it reflects the Firm's thought process and decision-making in advising clients regarding anticipated litigation. Moreover, Covington is ethically bound to protect the identities of its clients, rendering the Subpoena uniquely problematic.

We recognize that in some circumstances federal agencies have succeeded in compelling lawyers to divulge the identity of their clients—for example, where the lawyers themselves may have committed a possible regulatory infraction. Our position is not that lawyers are categorically exempt from an agency's subpoena powers. But the previous cases in which agencies have obtained discovery of client names arise under very different scenarios. We have yet to identify a case, other than this one, in which the SEC has even attempted to pry open client confidences or intrude on the attorney-client relationship where neither the law firm, nor its partners, nor its clients are suspected of violating any law.

Third, the SEC should look to the DOJ's policy for guidance. We acknowledge and appreciate that the SEC has an important interest in identifying potential illegal insider trading by the actual bad actors—the hackers who infiltrated Covington's network—even if that were the exclusive goal of this investigation. Even then, however, the SEC should, at a minimum, exhaust all other investigative options before it asks a law firm to divulge confidential client information based on a broad subpoena directed indiscriminately at a large number of the law firm's publicly traded or regulated clients. Indeed, the Department of Justice has adopted a policy that lawyers should be the last, rather than the first, step for information relevant to a criminal investigation, and even then only where the information is essential. *See* Dep't of Justice Manual § 9-13.410. Under the Justice Department's guidelines, the SEC has no basis for pursuing discovery of client names from Covington because any benefits it might obtain from that information, far from being essential, are purely speculative.

Fourth, Request No. 3 is unduly burdensome. Request No. 3 also imposes unique burdens on Covington related to the sacrosanct relationship lawyers have with their clients. By seeking to force Covington to divulge information and communications that clients expect

the Firm to withhold, the request undermines the foundation of trust between attorneys and clients that is central to the functioning of our judicial system. If a law firm can be forced to disclose protected client information merely to assist the Staff in identifying potential subjects for investigation, then open discussion between attorneys and clients will be chilled. Any effort to enforce this Subpoena against Covington will reverberate well beyond the confines of this investigation.

Beyond its effects on the attorney-client relationship, Request No. 3 also imposes significant practical burdens on Covington, which must either resist disclosure of the requested information or face possible disciplinary action by the D.C. Bar. We understand that the Staff has proposed potential solutions that would allegedly relieve this burden on Covington—*i.e.*, the Firm could seek the consent of its clients to disclose their identities, or else reveal the names of clients whose representation by Covington in already publicly known. But the burdens associated with seeking the informed consent of approximately 300 publicly traded clients affected by the breach are significant—and, at the end of the day, Covington will still have to resist the subpoena if any client withholds such consent. Nor is it any solution to divulge only Covington's publicly known clients, because the D.C. ethical rules require Covington to hold the identity of its clients in confidence even if the representation becomes known to others. It would also be immensely burdensome to parse through, redact, and log myriad communications and documents in multiple forms involving hundreds of clients.

Notwithstanding the significant burdens associated with seeking client consent, Covington has begun notifying its clients of the Staff's demand and asking whether they wish to provide their consent. The Firm will keep the Staff apprised of the progress of those discussions.

Fifth, enforcement of Request No. 3 will harm important law enforcement goals. As the director of the FBI has acknowledged, the private sector is an important partner for the FBI in responding to and preventing computer hacks. But private law firms inexorably will reevaluate that cooperation and transparency if there is a risk that the SEC will return their acts of good citizenship with an intrusive, unfocused, and burdensome discovery request targeting the attorney-client relationship and the confidences and privileges that arise from that relationship, as well as the clients themselves.

Again, Covington appreciates the important role the SEC plays in investigating and prosecuting violations of the securities laws. But the agency must remain "fully" alert "to the dual necessity of safeguarding adequately the public and the private interest" against intrusive discovery that burdens innocent third parties and invades the attorney-client relationship. *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 204 (1946). Request No. 3 is a bridge too far.

II. BACKGROUND

A. The Cyberattack on Covington & Burling

On March 2, 2021, Microsoft disclosed vulnerabilities in its Exchange Server software. Based on these public reports, and because Covington utilizes Exchange Server software, Covington launched an investigation to determine whether there had been any unauthorized access to Covington's network. Later in March, Covington's investigation discovered indicators of threat activity and ultimately determined that a threat actor had been able to compromise Covington's Exchange environment starting in late November 2020. Covington also discovered that, over the course of approximately four months, the threat actor had undertaken a series of malicious activities, including stealing credentials and engaging in search, reconnaissance, and export activity.

Through its own investigation and its cooperation with the Federal Bureau of Investigation ("FBI"), Covington determined that the threat actor was a Chinese state-sponsored actor whose activity was principally directed at a small group of lawyers and advisors, and principally focused on state espionage to learn about policy issues of specific interest to China in light of the incoming Biden Administration. With very few exceptions, none involving U.S.-listed publicly traded companies or investment advisors, it did not appear to Covington that the Chinese state-sponsored actor focused on or targeted particular clients or their files. Nevertheless, Covington concluded that the threat actor collected email from the Outlook accounts of the Firm lawyers and staff who were targeted. The threat actor also, with respect to a small group of lawyers and advisors, accessed folders on dedicated network drives and on the local hard drive of one user's firm-supplied laptop computer.

Within days of discovering the malicious activity, Covington began cooperating extensively with the FBI, and Covington believes that the indicators of compromise that it shared with the government proved helpful to the government's investigation and response to the threat actors at issue. The FBI was able to conduct its investigation without asking for the names of firm clients. Within weeks of its discovery, Covington contained and remediated the incident.

As you know, Covington provided the Staff with more details of the attack in its letter dated April 27, 2022. If helpful, the Firm is prepared to provide the Staff with more information about the attack and Covington's remediation and cooperation with law enforcement.

B. The SEC Subpoena

On March 21, 2022, Covington received the Subpoena. Covington reached out to the Staff shortly thereafter. In its first call with the Staff, Covington identified its concerns about complying with the Request, which asked the Firm in part to identify its clients affected by the cyberattack. In its second call with the Staff, Covington shared its concern that Rule 1.6 of the

D.C. Bar Rules of Professional Conduct limited the Firm's ability to identify the affected clients to a federal agency. Nevertheless, the Firm continued to comply with all other aspects of the Subpoena, completing the relevant document productions and information sharing required by the Subpoena on May 27, 2022. Covington also served responses and a privilege log in connection with Request No. 5 and supplemental responses to Request No. 7 on June 9, 2022.

The one item in the Subpoena to which Covington continues to object is Request No. 3, which states as follows:

> **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 activity identified in response to Item 2 above [*i.e.*, the Hafnium cyberattack]. Include in Your production information sufficient to identify the following for each entity:
>
> (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.

We understand the term "Public Company" in Request No. 3 means an entity whose securities trade in public markets in the United States. In the course of its discussions with Covington, the Staff has broadened Request No. 3 to include the names of entities regulated by the SEC affected by the cyberattack, such as broker-dealers and investment advisers, even if they are not public companies.

III. DETAILED RESPONSES & OBJECTIONS

A. The SEC Should Not Compel Covington to Disclose Client Confidences or Secrets

D.C. Rule 1.6(a)(1) bars a lawyer from "knowingly . . . reveal[ing] a confidence or secret of the lawyer's client." The rule defines a client "confidence" as "information protected by the attorney-client privilege under applicable law" and a client "secret" 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. Rule 1.6(b) (emphasis added). Thus, the rule binds attorneys practicing in D.C. to protect the confidentiality of information about their clients, "regardless

of whether such information is privileged." *United States v. Bikundi*, 80 F. Supp. 3d 9, 20 (D.D.C. 2015).

Request No. 3 asks Covington to divulge two types of documents that implicate this rule: (1) documents that identify publicly traded clients affected by the Hafnium cyberattack against Covington; and (2) documents that identify communications between Covington and its clients concerning that attack. We will start with the contents of the communications themselves, which fall under the protection of the attorney-client privilege and work-product doctrine, as well as of course client confidentiality and secrets. We will then discuss the request to identify clients Covington determined should be notified—information that constitutes protected client confidences and secrets, as well as attorney work product. In neither case is the SEC entitled to penetrate the sanctity of the attorney-client relationship.

1. Request No. 3 Improperly Targets Privileged Communications and Attorney Work Product That Covington Is Duty-Bound to Protect.

By Request No. 3 and subsequent discussions with the Staff, Covington has been asked to produce "[a]ny Communications provided to the client or other impacted party Concerning the" Hafnium cyberattack. *See* Request No. 3(c). Communications concerning a data breach that could have legal implications for Covington's clients are plainly shielded by the attorney-client privilege and the work-product doctrine. Indeed, we do not think this point can seriously be disputed. And even if they were somehow not privileged, these communications still constitute client confidences and secrets that Covington cannot "knowingly . . . reveal" in response to Request No. 3. D.C. Rule 1.6(a)(1).

When Covington learned of the unauthorized activity on its network, the Firm undertook to determine which of its clients should be notified by analyzing, among other things, the lawyers whose files may have been affected, their clients, and the Firm's work for those clients. Covington then contacted those potentially affected clients simply to notify them of that fact and invited each client to discuss the matter. For most of Covington's publicly traded clients, that initial outreach served to initiate further substantive discussions—orally or in writing or both—concerning the nature, risks, and implications of the cyberattack. Request No. 3 seeks the entire universe of these communications. And this broadly worded request covers a time period of over two years—January 1, 2020 to the date of the Subpoena. It also extends to "*any*" communications Covington had with its clients concerning the cyberattack. *See* Request No. 3(c) (emphasis added). The subpoena then defines "Communications" in sweeping terms to include all "correspondence, contact, discussion, e-mail, instant message, or any other kind of oral or written exchange or transmission of information . . . and any response thereto."

The content of Covington's communications with its clients concerning the potential implications of the cyberattack falls squarely within the heartland of the attorney-client privilege, "[t]he importance and sanctity" of which "is well established." *In re Grand Jury Subpoenas*, 144 F.3d 653, 659 (10th Cir. 1998). "The attorney client privilege is one of the

oldest recognized privileges for confidential communications . . . . The privilege is intended to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice." *Swidler & Berlin v. United States*, 524 U.S. 399, 403 (1998) (quotation marks omitted). For this reason, "[t]he privilege covers both (i) those communications in which an attorney gives legal advice; and (ii) those communications in which the client informs the attorney of facts that the attorney needs to understand the problem and provide legal advice." *FTC v. Boehringer Ingelheim Pharms., Inc.*, 892 F.3d 1264, 1267 (D.C. Cir. 2018) (Kavanaugh, J.).

Covington's discussions with its clients concerning the potential legal implications of the cyberattack involved the exchange of "facts that [Covington] need[ed] to understand the problem," and the provision by Covington of "legal advice." *Id.* And that suffices to bring those communications within the privilege. *See In re Cty. of Erie*, 473 F.3d 413, 422 (2d Cir. 2007) ("When a lawyer has been asked to assess compliance with a legal obligation, the lawyer's recommendation of a policy that complies (or better complies) with the legal obligation—or that advocates and promotes compliance, or oversees implementation of compliance measures—is legal advice."); *Gen. Elec. Co. v. Johnson*, 2007 WL 433095, at *21 (D.D.C. Feb. 5, 2007) ("The remainder of the document is protected by the attorney-client privilege, since it is a communication among agency attorneys that contains legal analysis of . . . potential litigation risks.").

In addition to privilege, the content of these communications is protected from disclosure by the work-product doctrine. "The work-product doctrine shields materials 'prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent).'" *Judicial Watch, Inc. v. Dep't of Justice*, 432 F.3d 366, 369 (D.C. Cir. 2005) (quoting Fed. R. Civ. P. 26(b)(3)). The D.C. Circuit has made clear that "[t]he work-product privilege simply does not distinguish between factual and deliberative material." *Martin v. Office of Special Counsel, Merit Sys. Protection Bd.*, 819 F.2d 1181, 1187 (D.C. Cir. 1987). On the contrary, "[a]ny part of a[document] prepared in anticipation of litigation, not just the portions concerning opinions, legal theories, and the like, is protected by the work product doctrine." *Tax Analysts v. IRS*, 117 F.3d 607, 620 (D.C. Cir. 1997). For a document to be prepared in anticipation of litigation, "the lawyer must at least have had a subjective belief that litigation was a real possibility, and that belief must have been objectively reasonable." *In re Sealed Case*, 146 F.3d 881, 884 (D.C. Cir. 1998).

There can be no dispute that Covington's communications with its clients were prepared in anticipation of litigation. The unauthorized breach of Covington's computer systems by a foreign actor certainly gave rise to a reasonable belief that its clients might face litigation, and that belief was objectively reasonable considering the frequency with which data breaches precipitate civil lawsuits. *See* Joseph F. Yenouskas & Levi W. Swank, *Emerging Legal Issues in Data Breach Class Actions*, Am. Bar Ass'n (July 17, 2018), https://tinyurl.com/5dy9u8zz ("Many data breaches have spawned multi-plaintiff or class action lawsuits by customers whose PII was accessed by unauthorized third parties as a result

of the breach."). Indeed, the SEC's own inquiry here into the adequacy of disclosures by Covington's clients only underscores that the Firm rightly anticipated litigation related to the cyberattack. The work-product doctrine therefore protects Covington's communications even where they contain only factual information about the breach.[1]

2. The Subpoena Improperly Seeks Client Names That Covington Is Duty-Bound to Protect.

Request No. 3 further seeks the "name[s]" of Covington "[c]lient[s] or other . . . part[ies]" impacted by the Hafnium cyberattack. *See* Request No. 3(a). But, under the D.C. Rules of Professional Conduct, Covington can no more disclose the identity of its clients than its privileged communications. The D.C. Bar has specifically interpreted protected "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. Moreover, the Staff is not seeking a list of all Covington clients, but a discrete group of clients who were affected by the cyberattack on the Firm, which itself is a client secret under D.C. Rule 1.6.

The Staff has taken the position that Rule 1.6 contains an exception that allows law firms to "reveal client confidences or secrets" when "required by law or court order," including for the purpose of complying with an administrative subpoena. D.C. Rule 1.6(e)(2)(A). The Staff's argument is inconsistent with the D.C. Bar's position on the issue and is also contrary to public policy.

The D.C. Bar has issued specific guidance that a law firm "may not automatically comply" with a demand from a federal agency to release the names of its clients. D.C. Bar Op. No. 124, at 207. In the matter at issue in D.C. Bar Opinion 124, the IRS directed an attorney to name his firm's clients in connection with a routine audit of the firm's income tax returns. *Id.* at 206. However, the Ethics Opinion clearly stated that "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 (emphasis added). In other words, the attorney must go to court in an effort to protect client secrets from administrative compulsory disclosure. 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

[1] For the reasons explained below, Covington also cannot disclose the names of clients affected by the breach. Accordingly, providing a privilege log that lacks a key field—the name of the client with whom Covington communicated—seemingly would not advance the SEC's investigatory interests. Such a log would disclose only that Covington communicated the fact of the breach to its affected clients. But Covington is, of course, open to discussing this issue further.

regulatory agency" when "fail[ure] to do so might be prejudicial to the client." D.C. Bar Op. No. 214 (Sept. 18, 1990); D.C. Bar. Op. No. 14, at 80–81 (January 26, 1976) (same).[2]

The Staff's position is also contrary to the public interest. Considering how easy it is for a federal agency to issue an administrative subpoena, the protection for client secrets under Rule 1.6 would essentially be nonexistent in government investigations. There is nothing in D.C. Bar Opinions or the Rule itself, however, suggesting that the protections of Rule 1.6 have a carveout for the government, and we believe it is unlikely that any federal court or state bar would endorse such a sweeping vitiation of the protections Rule 1.6 affords law firm clients.

3. Compelling Disclosure of Client Secrets For Speculative Investigations Is Contrary to the Public Interest and Inconsistent with the Approach Taken by the DOJ and the SEC.

The Staff has said that it seeks the names of Covington's publicly traded clients and other regulated clients because these would provide an expedient investigative option for the agency. Once it has those names, we understand the Staff plans to search for any unusual or suspicious trades in that company's stock, and look for SEC disclosure violations by the clients themselves. In other words, the Staff asks Covington to divulge client secrets merely as a first step in determining whether a potential violation of the securities laws even exists.

At least one coordinate federal agency bars its prosecutors from seeking discovery from lawyers for such "speculative" purposes. Dep't of Justice Manual § 9-13.410(C)(3). In recognition that the attorney-client relationship occupies a special role in our judicial system, Department of Justice guidelines direct that subpoenas may issue to attorneys only as a last resort. Not only must an assistant or deputy assistant attorney general approve service of a subpoena to a private law firm, *id.* § 9-13.410(A), that subpoena may issue only if the Justice Department has "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," *id.* § 9-13.410(C)(3). 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).

The request the Staff has issued here falls far outside the reasonable limits the Justice Department has placed on attorney discovery. At this stage, the Staff does not even have "reasonable grounds to believe" that a securities law violation has been or is being committed. Dep't of Justice Manual § 9-13.410(C)(3). That is the predicate fact it is seeking to investigate.

---

[2] The D.C. Bar's rules comport with those of other jurisdictions. *See, e.g.*, Ill. Adv. Op. 21-02, 2021 WL 1332188, at *4 (Mar. 1, 2021) ("the lawyer should object to the subpoena and only provide the documents after the court enters an order to comply with the subpoena."); Utah Ethics Op. 21-01, 2021 WL 2188317, at *3 (Apr. 13, 2021) ("The lawyer's duty is to maintain client confidentiality unless and until compelled to do so by proper order of a tribunal.").

Nor is it clear why the SEC cannot conduct its investigation using possible sources of information other than a law firm's client secrets. The Staff's speculative need for this information does not come close to outweighing "the potential adverse effects upon the attorney-client relationship." *Id.* § 9-13.410(B), (C)(5).

While the Justice Department guidelines do not bind independent agencies such as the SEC, they should serve at a minimum as persuasive guidance. All lawyers—whether in government service or private practice—ought to respect the ethical principles requiring a lawyer to preserve client secrets. And the Department of Justice guidelines recognize that those ethical rules themselves serve important public interests that would be undermined if prosecutors could seek discovery from lawyers as a routine investigative tool. As a government agency guided by a similar mission to serve the public interest, the SEC has every reason to follow the Justice Department's lead and desist from seeking client secrets except in pressing circumstances not present here.

Indeed, the SEC has adopted a virtually identical policy for issuing subpoenas to the news media, 17 C.F.R. § 202.10—a policy that applies even though the D.C. Circuit has held that no First Amendment or other privilege protects journalists from having to disclose confidential sources in analogous circumstances. *See In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1141, 1142 (D.C. Cir. 2006). We respectfully submit that a law firm's interest in protecting the confidentiality of its client relationships is at least as strong as a journalist's interest in protecting the confidentiality of his or her sources.

4. Compelling Covington to Disclose Client Secrets is Unduly Burdensome.

Although the SEC "is entitled to great freedom in conducting its investigations," its subpoena powers remain limited by the principle that "compliance [must] not be unduly burdensome." *SEC v. Arthur Young & Co.*, 584 F.2d 1018, 1031–33 (D.C. Cir. 1978). No single test governs whether a document request imposes undue burdens: the inquiry depends on "context." *United States v. Capitol Supply, Inc.*, 27 F. Supp. 3d 91, 102 (D.D.C. 2014). Here, Request No. 3 is unduly burdensome in two respects. First, it significantly undermines the trust that is central to the relationship between Covington and its clients. Second, even if there were some way for Covington to comply with Request No. 3 without running afoul of the D.C. Bar Rules of Professional Conduct, it would require a substantial expense of time and effort on the part of Covington—an innocent third-party victim of a malicious, state-sponsored cyberattack.

a. Compliance With Request No. 3 Would Place an Undue Burden on the Relationship of Trust Between Attorneys and Clients on Which Clients—and the SEC—Depend.

For the Staff to seek enforcement of the Subpoena would impose an undue burden on Covington by undermining the trust relationship the Firm has with its clients. It has long been

recognized that "the basic trust between counsel and client . . . is a cornerstone of the adversary system." *Linton v. Perini*, 656 F.2d 207, 209 (6th Cir. 1981); *see also Stockton v. Ford*, 52 U.S. (11 How.) 232, 247 (1850) ("There are few of the business relations of life involving a higher trust and confidence than that of attorney and client."). This trust is predicated on the expectation that attorneys will keep the confidences of their clients—whatever those confidences may be. *See Swidler & Berlin*, 524 U.S. at 407–08 ("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 attorney subpoenas can do to the attorney-client relationship. For example, the First Circuit explained in an analogous context that "the serving of a grand jury 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). These concerns provide an independent basis for declining to enforce an attorney subpoena. *See In re Grand Jury Matters*, 751 F.2d 13, 18 (1st Cir. 1984) ("The district court could weigh those policies and conclude that the potential disruption of the attorneys' relationships with their clients . . . made the subpoenas unreasonable and oppressive at the time they were served."); *In re Public Defender Serv.*, 831 A.2d 890, 900 (D.C. 2003) (noting that, "while a grand jury subpoena to an attorney may be perfectly proper, the fundamental interests at stake necessitate careful judicial scrutiny").

Request No. 3 cuts at the very heart of the relationship of trust between law firms like Covington and their clients. If clients knew that Covington might disclose their communications, or even their relationship, to the SEC simply to assist the Staff in searching for potential investigative subjects (including themselves), the free flow of information between client and attorney may be unduly inhibited. Indeed, Covington prides itself on its professionalism and discretion with its clients' most sensitive confidences. And courts have declined to compel third parties to assist in the investigation of misconduct where, as here,

doing so "could threaten the trust between [the third party] and its customers and substantially tarnish the [third party's] brand." *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) (citation omitted); *cf. United States v. N.Y. Tel. Co.*, 434 U.S. 159, 174 (1977) (indicating that, in considering the propriety of an order compelling a third party to assist in an ongoing criminal investigation, a court should consider whether the third party "ha[s] a substantial interest in not providing assistance" and whether providing assistance would be "offensive to it"). Furthermore, the Supreme Court has recognized that, when evaluating the "burden" imposed on a party by a government action, the courts should go beyond "practical problems" to consider "the more abstract matter of submitting to the coercive power of a State that may have little legitimate interest in the claims in question." *Bristol-Myers Squibb Co. v. Super. Ct.*, 137 S. Ct. 1773, 1780 (2017).

Undermining the trust between lawyers and their clients could be especially damaging to the interests of the federal law enforcement agencies, including the SEC and the FBI, which rely on the private bar to assist clients in complying with the law. *See* Section III.B, *infra*. Administrative subpoenas that jeopardize the trust clients place in their attorneys serve only to undermine that cooperative relationship between the public and private sector.

b. Compliance With Request No. 3 Would Impose Substantial Practical Burdens on Covington.

Request No. 3 also places unique burdens on Covington in light of its ethical obligations to maintain client secrets, as discussed above. As a result of the Staff's request, Covington faces a double bind. If the Firm refuses to comply with the subpoena, as required by D.C. ethical rules, it faces a possible enforcement action from the SEC. If Covington accedes to the demand notwithstanding these ethical regulations, it faces possible disciplinary action from the D.C. Bar and the specter of civil actions by its clients. *See 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).

The Staff has proposed two potential alternatives that it claims could relieve this burden on Covington, neither of which comes close to resolving the issue.

First, we understand that the Staff has suggested that Covington need not take on the burden of resisting Request No. 3 in a possible enforcement action because Covington could simply ask its clients to consent to the release of their names. As a compromise with the Staff, Covington offered to notify its clients of the Subpoena and ask whether they consent to the release of their names in connection with Request No. 3. But the Staff rejected Covington's offer, insisting that Covington present its clients with a "binary choice" either to consent to the disclosure of their confidential information or refuse.

Covington cannot put its clients to such a binary choice consistent with its ethical obligations. At the outset, the D.C. Bar's Rules of Professional Conduct provide that "[a] lawyer may use or reveal client confidences or secrets" only "with the *informed* consent of the client." D.C. Rule 1.6(e)(1) (emphasis added). But a client can give informed consent only "after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct." D.C. Rule 1.0(e). The type of binary choice demanded by the Staff is inconsistent with the options available to each client, as well as with the active and substantive dialogue that may be necessary in connection with a client's informed consent.

For example, Request No. 3 seeks a broad swath of documents and communications, some of which Covington's clients may deem innocuous, and some of which they may view as highly sensitive. Requiring Covington to put its clients to the choice of either consenting to the disclosure of all of those documents or else refusing to produce any of them is inconsistent with Covington's obligation to apprise clients of "available alternatives"—such as agreeing to disclose some documents but not others, or simply not responding at all.

In a good-faith effort to resolve this dispute while maintaining its obligations to its clients, Covington is in the process of notifying approximately 300 affected clients of the SEC's subpoena to see if they consent. Covington will apprise the Staff if any clients consent to the release of their names. But if any client withholds its consent or does not respond—an outcome that appears all but certain given the number of clients at issue—Covington remains duty-bound to resist disclosure should the SEC proceed with an enforcement action.

Second, we understand the Staff has proposed that Covington disclose only the names of clients whose representation by Covington is already public knowledge—whatever "public knowledge" means and whatever its temporal scope. This proposal by the Staff would not relieve Covington of its ethical obligation either to resist the subpoena or seek consent from its clients—obligations that render compliance with Request No. 3 unduly burdensome, as previously discussed.

Even in cases where a law firm's representation of a client has become public, the D.C. Bar's Rules of Professional Conduct still prohibit the firm from making incremental disclosures without the consent of the client. Thus, the Bar has counseled 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* D.C. Rule 1.6 cmt. 8 ("This ethical precept . . . exists without regard to . . . the fact that others share the knowledge"). And Covington's clients would have every reason to "desir[e]" that Covington "avoid[] additional disclosure" of their identity to the SEC where, as here, the Staff has refused to give any assurance that it will not use the information to investigate those clients for possible violations of the federal securities laws. *See* D.C. Bar Op. No. 124, at 207.

In any event, even if D.C. ethical rules permitted Covington to identify clients whose representation was already public, which they do not, identifying such clients is no easy task. 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 then 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 a Law360 article from 2010 that remains behind a paywall—remain "public" in any meaningful sense. In short, this proposal is just as burdensome as the Staff's original request.

Asking Covington to undertake these burdens is particularly unreasonable in light of the Firm's status as an innocent third party. As in private civil litigation, courts are "reluctant" to allow federal agencies to pursue even legitimate investigative needs by invading the privacy of "third parties who were not targets of the agency's investigation." *In re McVane*, 44 F.3d 1127, 1137 (2d Cir. 1995); *see also Arthur Young & Co.*, 584 F.2d at 1031–32 (recognizing that agencies must limit burdens on third parties who are "not the primary target" of an investigation).

In *McVane*, the Second Circuit quashed a document subpoena issued by the FDIC seeking financial information from the family members of the directors of a failed bank. The purpose of the subpoena was to seek targeted information in service of a well-developed investigation—namely, whether the directors had engaged in any fraudulent transfers of wealth that the agency should seek to unwind. *See* 44 F.3d at 1131. Although the Second Circuit acknowledged the FDIC's purpose was legitimate, it noted that an agency is not "automatically entitled to obtain all material that may in some way be relevant to a proper investigation." *Id.* at 1138. And while the FDIC had broad powers to extract information from third parties "directly associated" with the target of an investigation, it had to satisfy "more exacting scrutiny" to obtain discovery from individuals whose relationship with the bank directors was purely personal. *Id.* at 1137–38. Ultimately, the court concluded that the family members' privacy interests outweighed the agency's interest in discovery of their personal financial information.

The same result should follow here. In this case, as in *McVane*, neither Covington nor its clients is "directly associated" with the target of the SEC's investigation. *Id.* at 1137–38. To the contrary, the SEC does not appear to have identified a target at all, and is instead simply fishing for possible securities violations by the individuals or entities that perpetrated the Hafnium cyberattack. Covington and its clients are associated with these potential targets in only one limited sense—as their victims. What is more, Covington and its clients have an even stronger claim to privacy than the one at issue in *McVane*. In that case, the family members interposed only a general interest in shielding their personal financial records from inspection.

Here, however, Covington seeks to protect its ethical obligations and the sanctity of the attorney-client relationship—a relationship that holds special status in our legal system and is protected by the rules of professional conduct.

We have found no reported case in which a federal agency has succeeded in forcing an innocent third-party law firm to produce a list of its clients. When courts have compelled production of such records, it has been where either the firm or its clients is suspected of some kind of regulatory infraction. *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 suspect, based on the account of one client, that firm was assisting other clients in avoiding federal taxes); *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 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); *SEC v. Sassano*, 274 F.R.D. 495, 497 (S.D.N.Y. 2011) (enforcing a subpoena to law firm for client financial records where client was in arrears on judgment payable to SEC). Courts have also allowed agencies to discover client names from law firms in the inapposite context where the law firms serve as federal contractors in order to ensure compliance with federal program guidelines. *See Adair v. Rose Law Firm*, 867 F. Supp. 1111 (D.D.C. 1994) (enforcing subpoena in an inspector general's investigation of allegations that law firm entered legal services agreements with FDIC while failing to disclose client relationships creating a conflict of interest). By contrast, the demand by the Staff in this case—a demand to search the files of an innocent law firm to discover the names of its innocent clients—is wholly without precedent.

To the extent the Staff wishes to use this information to inquire whether any public companies represented by Covington failed adequately to disclose the cyberattack, the request is all the more problematic. At this time, any such disclosure violation is purely speculative. Absent any basis to believe a violation has occurred, the Staff cannot breach attorney confidences to cast suspicion on a client in the first instance in the unique circumstances of this matter. Covington cannot be used as an instrument by which the Staff seeks to implicate Covington's own clients.

Finally, with respect to Covington's communications with its clients about the cyberattack sought by Request 3(c), in the unlikely event that Covington engaged in some number of nonprivileged communications with its clients concerning the breach, locating those documents in a sea of protected communications would impose an unreasonable burden on the Firm. *See Arthur Young & Co.*, 584 F.2d at 1031–33 (noting compliance with subpoena must not be "unduly burdensome"). Covington's communications about the Hafnium cyberattack with approximately 300 affected public company clients unfolded over the course of weeks or months, yielding multiple communications with many of these clients in various forms and within Covington. Once it identified all potentially responsive documents, Covington would need to conduct a line-by-line review of those documents for any material that might be subject

to the attorney-client privilege or work-product doctrine. Any demand that Covington comb through these files on the off-chance of identifying a nonprivileged communication simply is not reasonable—particularly where there is nothing in those communications that could conceivably shed light on any potential insider trading by the hackers. The content of these communications has no possible relevance to the Staff's investigation into unknown trading by those who carried out the cyberattack.

B. Compelling Covington to Identify Its Clients Would Undermine Federal Law Enforcement Interests.

Compelling Covington to produce the names of its clients will also have negative, long-term policy implications for the federal government. While Covington does not know how the SEC became aware of the cyberattack, Covington did self-disclose to the FBI the occurrence of the crime and fully cooperated in the FBI's investigation, and it painstakingly informed certain of its clients about the incident. It is regrettable that, after these conscientious actions, Covington now faces an intrusive subpoena that burdens the Firm's relationships with its clients. If that is the inevitable—or even a possible—consequence of cooperating with the FBI, then law firms like Covington will be obligated to carefully consider those consequences and their implications before reporting data breaches to law enforcement in the future.

In recent years, "cyberspace has become the most active threat domain in the world and the most dynamic threat to the Homeland." *See* Dep't of Homeland Security, *Secure Cyberspace and Critical Infrastructure* (Feb. 23, 2022), https://tinyurl.com/mry3yy6v. Between 2019 and 2021, the number of ransomware attacks reported to the FBI increased by 82 percent. Christopher Wray, *FBI Partnering With the Private Sector to Counter the Cyber Threat* (Mar. 22, 2022), https://tinyurl.com/2s3suvn9. And the total cost of cybercrime to the global economy is expected to reach $10.5 trillion annually by 2025, representing "the greatest transfer of economic wealth in history." Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, Cybercrime Mag. (Nov. 13, 2020), https://tinyurl.com/czw7bce9.

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 recently 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." Wray, *FBI Partnering With the Private Sector*. 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.

Moreover, the SEC itself, in carrying out its mandate to enforce the securities laws, is uniquely dependent on the cooperation of public companies and their counsel. Chairman Gensler has acknowledged that the securities laws "entrust[]" lawyers "with certain responsibilities" to "uphold[] the law" and thereby "protect[] investors and our markets." Gary Gensler, *Prepared Remarks At the Securities Enforcement Forum* (Nov. 4, 2021), https://tinyurl.com/5frdk5xr.

But this cooperation between the federal government and the private sector is imperiled when agencies effectively punish companies that come forward with information about possible cyberattacks. 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 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." Christopher Wray, *Working With Our Private Sector Partners to Combat the Cyber Threat*, Federal 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.

Covington has been a willing partner in responding to that attack, having reported and consistently and admirably cooperated with the FBI's investigation. Covington now faces an SEC subpoena that seeks to coerce production of information concerning numerous clients—information that is burdensome to produce, as well as highly confidential, privileged, and protected by the work-product doctrine. The long-term effect of this effort, if successful, will be to disincentivize law firms from voluntarily disclosing potential cyberthreats to the government in the future. This would be directly contrary to the federal government's express interest in encouraging voluntary cooperation by the private sector.

C. Covington Must Also Decline to Comply with Additional Components of Request No. 3.

1. Covington Cannot Comply with the Request for Documents that Identify the Nature of the Unauthorized Activity Concerning Its Clients.

Request No. 3(b) seeks documents sufficient to identify "[t]he nature of the suspected unauthorized activity Concerning the client," including "when the activity took place" and "the amount of information . . . viewed." Covington already disclosed the dates of the unauthorized activity and the number and types of files breached in response to Request No. 2. It cannot take the further step of connecting those files to any individual client for the reasons discussed above. Complying with this request would only compound the burden associated with disclosing client identities in the first instance.

2. The Request that Covington Identify Parties Other Than Its Clients Potentially Affected by the Hafnium Cyberattack Is Unduly Burdensome.

Request No. 3(a) asks Covington to produce documents sufficient to identify "other . . . part[ies]" besides its clients that "may" have been "impacted" by the data breach. This request would potentially require Covington to produce documents from a large universe of third parties, ranging from opposing parties in litigation to companies on the other side of a transaction. This request, too, plainly imposes undue burdens on Covington.

As an initial matter, Covington cannot produce third-party documents that would allow the SEC to deduce the identity of its own clients. For example, if Covington were to produce information about the target of a successful acquisition, the agency might reasonably deduce that Covington represented the acquiring entity. Similarly, if Covington produced materials relevant to an ongoing suit in which it had not entered an appearance, one might reasonably conclude that Covington was serving in a confidential advisory role to one of the parties to that litigation. And Covington certainly cannot produce any third-party documents that would disclose the Firm's role representing a client in a nonpublic SEC investigation.

Covington therefore must decline at this time to produce documents that identify "other impacted parties" whose materials may be found within Covington's files. These third parties may include parties who produced documents to Covington or its clients in the course of civil litigation. In civil cases, parties typically produce documents to the other side pursuant to a confidentiality agreement and/or protective order. These agreements and orders often require each party to provide notice and an opportunity to object if it has received a subpoena for the other side's documents. The Staff's demand thus would require Covington to review an unknown number of protective orders and other agreements and possibly provide notice to opposing counsel before it may release third-party documents to the SEC. The burdens this process would impose on Covington, as well as its potential negative impact on Covington's

clients, far exceed any speculative benefit to the SEC from discovering "other impacted parties." And these burdens are of course cumulative, since Covington also would be required to review its files for client information as discussed above.

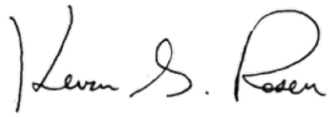
If, however, the Staff has a proposal for narrowing this request so as to limit the burden on Covington, we remain open to considering limitations on information relating to non-clients impacted by the cyberattack.

IV. CONCLUSION AND MEETING REQUEST

For the reasons explained above, Request No. 3 improperly invades the attorney-client privilege, the work-product doctrine, and client confidentiality. In so doing, it imposes undue burdens on Covington and Covington's attorney-client relationships. While this letter was designed to explain Covington's position, given the future implications of the Staff's current position to law firms throughout the country, we request a meeting with Gurbir Grewal, the SEC's Enforcement Director, and the Division of Enforcement's Chief Counsel, Sam Waldon.

Should you wish to discuss this matter further, please contact Ted Boutrous at (213) 229-7804 or tboutrous@gibsondunn.com; Kevin Rosen at (213) 229-7635 or krosen@gibsondunn.com; or Richard Grime at (202) 955-8219 or rgrime@gibsondunn.com.

Sincerely,



GIBSON, DUNN & CRUTCHER LLP
Theodore J. Boutrous, Jr.
Kevin S. Rosen
Richard W. Grime
Katherine Moran Meeks
Samuel Eckman

****

Covington requests that the SEC accord confidential treatment under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and 17 C.F.R. § 200.83 to this letter and any information contained in or derived from the letter (collectively, "Confidential Information"). We believe that the Confidential Information is entitled to protection as private and confidential records. If the SEC receives a request under FOIA for the Confidential Information, we respectfully request immediate notification by telephone or e-mail so that Covington may provide any additional information necessary regarding the request for

confidential treatment. We believe that the fact that we have provided this information may be exempt from disclosure under FOIA. If you have a different view, please let us know so that we may address this issue further and, if necessary, request a hearing on the subject.

The request set forth in the preceding paragraph also applies to any memoranda, notes, transcripts, or other writings of any sort whatsoever that are made by, or at the request of, any employee of the SEC or any other government agency and that (1) incorporate, include, or relate to any of the Confidential Information; or (2) refer to any conference, meeting, telephone conversation, or interview between (a) Covington, or any of its current or former partners, employees, representatives, agents, accountants, or counsel and (b) employees of the SEC or any other government agency.

A copy of this written request for confidential treatment will be mailed to the SEC Office of Information and Privacy Act Operations at 100 F Street NE, Washington, DC 20549.