

**UNITED STATES DISTRICT COURT  
DISTRICT OF COLUMBIA**

SECURITIES AND EXCHANGE  
COMMISSION,

Applicant,

vs.

COVINGTON & BURLING LLP,

Respondent.

Case No.

**DECLARATION OF W. BRADLEY NEY IN SUPPORT OF AN  
APPLICATION FOR AN ORDER TO SHOW CAUSE AND FOR  
AN ORDER COMPELLING COMPLIANCE WITH SUBPOENA**

I, W. Bradley Ney, Pursuant to 28 U.S.C. §1746, do hereby declare as follows:

1. I am an attorney admitted to the Bars of the District of Columbia and State of California. Since November 2015, I have been employed as an attorney in the Enforcement Division of the Applicant, Securities and Exchange Commission (the "Commission") in the Commission's Home Office in Washington, D.C.
2. This Declaration is submitted in support of the Commission's Application for an Order to Show Cause and an Order Requiring Compliance With Subpoena directed to Covington & Burling LLP, and is based upon my direct participation in the investigation captioned *In the Matter of Microsoft Hafnium Cyberattack*.
3. On March 6, 2021, the Commission's Division of Enforcement opened an investigation into possible violations of the Federal securities laws concerning a reported cyberattack targeting a vulnerability in Microsoft Exchange Servers that were connected to the Internet (the "Cyberattack").

4. On March 17, 2021, pursuant to Section 20(a) of the Securities Act of 1933 (the “Securities Act”) and Section 21(a) of the Exchange Act of 1934 (the “Exchange Act”), the Commission issued an Order Directing Private Investigation and Designating Officers to Take Testimony in an investigation entitled In the Matter of Microsoft Hafnium Cyberattack (the “Formal Order”). Among other things, the Formal Order:

- a. Directs, pursuant to Section 20(a) of the Securities Act, 15 U.S.C. § 77t(a), and Section 21(a) of the Exchange Act, 15 U.S.C. § 78u(a), that the Commission conduct a private investigation to determine whether any persons or entities had engaged, or is engaging, in acts or practices in violation of various provisions of the federal securities laws; and
- b. Designates, pursuant to Section 19(c) of the Securities Act, 15 U.S.C. § 77s(c), and Section 21(b) of the Exchange Act, 15 U.S.C. § 78u(b), certain individuals, including myself, as officers of the Commission empowered to administer oaths and affirmations, subpoena witnesses, compel their attendance, take evidence, and require the production of any books, papers, correspondence, memoranda, or other records deemed relevant to the investigation.

5. The Commission, through its Division of Enforcement, is investigating, among other things, whether threat actors associated with the Cyberattack or their affiliates may have accessed and traded on the basis of material, non-public information; whether any other persons may have traded on material, non-public information concerning the Cyberattack; or whether any person may otherwise have made materially false or misleading statements, or omitted to state material facts, concerning the impact of the Cyberattack in violation of federal securities laws.

6. In connection with that investigation, the Commission learned in early 2022 that threat actors exploiting the Microsoft Exchange vulnerability had gained access to the internal network environment of the law firm Covington & Burling LLP (“Covington”). According to publicly available information, Covington is an American multinational law firm headquartered in Washington, D.C., with 13 offices located in the United States and abroad. The firm advises clients on transactional, litigation, regulatory, and public policy matters. From its investigation, the Commission understands that the threat actors were able to gain access to certain client files, including the files of various public companies regulated by the Commission who were either represented by Covington, or about whom Covington possessed information.

7. On March 21, 2022, the Commission issued a subpoena to Covington, electronic service of which was agreed to and accepted by Anne M. Scott on Covington’s behalf (the “Subpoena”). Ms. Scott acknowledged service of the Subpoena, which was sent by Lory Stone via encrypted electronic mail message, on March 24, 2022. Ms. Stone is named in the Formal Order as an officer of the Commission authorized to require production of documents and other information. The Subpoena called for the production of certain documents concerning the threat actors’ access to Covington’s systems, including the identity of any public companies whose files may have been accessed in connection with the Cyberattack. A true and correct copy of the Subpoena is attached hereto as Exhibit A.

8. As relevant to this matter, Request No. 3 in the Subpoena called for (a) the name of any public companies that were impacted by the unauthorized activity; (b) the nature of the suspected unauthorized activity concerning the companies, including when the activity took place and the amount of information that was viewed, copied, modified, or exfiltrated if known, and (c) any communications provided to the companies concerning the suspected unauthorized

activity. While negotiating the scope of the subpoena, the parties agreed that the phrase public companies would include any companies publicly traded on a U.S. exchange, as well as any other entities regulated by the Commission, including investment advisers, brokers and dealers, collectively referred to herein as “public company clients” or the “clients.”

9. The original return date for the production of documents pursuant to the Subpoena was April 4, 2022. On April 4, 2022, the day that documents were due, Covington contacted the Commission to explain that it would not meet the deadline. Covington also indicated that there might be some challenges in complying with Request No. 3, citing the firm’s confidentiality obligations under the D.C. Rules of Professional Conduct. Following the April 4, 2022 communication and at Covington’s request, the Commission and Covington entered into protracted negotiations regarding the scope of Request No. 3.

10. On June 10, 2022, at the Commission’s request, Covington sent its formal objections in a white paper setting out Covington’s position. In the paper, Covington informed the Commission that foreign actors had intentionally and maliciously accessed Covington’s IT network and certain individual devices. During that time, the threat actors accessed files, communications, and information relating to approximately 300 of Covington’s clients, including clients regulated by the Commission. After learning of the unauthorized access, Covington compiled a list of potentially affected clients, “contacted those potentially affected clients simply to notify them of that fact[,] and invited each client to discuss the matter.” In refusing to provide the information requested by the Subpoena, Covington argued that: (1) the information was protected under client confidentiality rules under D.C. Rule of Professional Conduct 1.6 (“Rule 1.6”); (2) certain of the information was protected by the attorney-client or work product privilege; and (3) Request No. 3 was overbroad. A true and correct copy of

Covington's June 10, 2022 white paper is attached as Exhibit B.

11. On July 14, 2022, the Commission responded to Covington's June 10, 2022 white paper. In its letter, the Commission asserted, among other things, that: (1) its lawful administrative subpoena provided an exception to Rule 1.6; (2) the requested information was not work product or, even if it was factual work product, that the Commission satisfied the requirements for its production; (3) the Commission had specifically excluded from production any privileged materials, which should be identified on a privilege log; and (4) Request No. 3 was not overbroad. A true and correct copy of the Commission's July 14, 2022 letter to Covington's counsel is attached as Exhibit C.

12. As a result of the Commission's negotiations with Covington, the Commission has significantly reduced the scope of information sought under Request No. 3, and now limits its request to production of the names of clients whose information was accessed by the threat actors. To date, Covington has provided the names of only two entities, both of whom consented to the production of their names to the Commission.

13. As part of the negotiations, Covington undertook a review to identify how many, if any, of the 298 clients it believed had material, non-public information that may have been viewed, copied, modified, or exfiltrated by the threat actors. The Commission has been unable to verify the information provided by Covington and disagrees with Covington's methodology for determining what constitutes material, non-public information.

14. From its review, Covington concluded that of the original 298 clients whose files the threat actor viewed, copied, modified, or exfiltrated, only seven clients had material, non-public information. However, the Commission has been unable to verify Covington's assertion. Covington provided the Commission with certain examples of categories of information that it

did not consider market moving, but based on Covington's general descriptions the Commission could not agree that the information described by Covington could categorically be described as not market moving. Moreover, Covington has refused to provide the Commission with the names of the seven clients who the firm concedes had material, non-public information at the time their files were viewed, copied, modified, or exfiltrated by the threat actors.

15. In order to determine the materiality of the information accessed, evaluate any patterns of potential illicit trading based on the information accessed, and evaluate any disclosure obligations arising from the illegal access to the information, the Commission has asked Covington to provide the names of the 298 public company clients whose files and information were accessed by the threat actors.

16. Throughout the course of the negotiations, the Commission has made every effort to accommodate Covington in its efforts to comply with Request No. 3 of the Subpoena. Despite the Commission's willingness to negotiate the scope of its lawful Subpoena, the parties were unable to reach agreement. On November 15, 2022, the Commission informed Covington that as a final compromise attempt, it would accept disclosure of the names of the 298 regulated clients whose information was accessed by the threat actors in satisfaction of Request No. 3 of the Subpoena.

17. On November 30, 2022, Covington informed the staff that it would not provide the names of the impacted entities absent consent, which had been provided by only two of the companies. As a result, the Commission now seeks an order compelling Covington to provide the subpoenaed information—specifically, the names of clients whose information may have been viewed, copied, modified or exfiltrated in connection with the threat actor's intrusion into Covington's IT network.

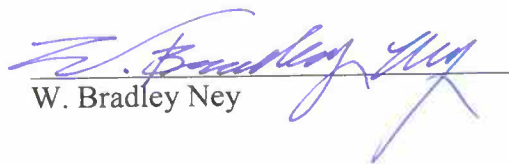
18. During my more than seven years at the Commission, I have seen numerous instances where the Commission seeks information from companies that have been victims of cyberattacks, including other non-public investigations with which I have been involved. Among other things, the Commission seeks such information to: (1) understand the nature and scope of the attacks on public issuers and registered entities; (2) assess and identify potential illegal trading based on material, non-public information gathered during the attack; (3) assess and identify potential illegal trading based on material, nonpublic knowledge of the attack itself; and (4) determine and ensure compliance with the relevant disclosure obligations for public companies and registered entities impacted by the attack.

19. The Commission has previously brought cases against threat actors who traded on material, non-public information obtained through cyberattacks, including cyberattacks on law firms, against insiders who traded on material, nonpublic knowledge of cyberattacks, as well as against companies that failed to disclose the material impact of cyberattacks to investors.

20. The Commission has made no prior application to any court for similar relief relating to this matter.

Under the penalty of perjury, I declare that the foregoing is true and correct.

Executed on January 9, 2023.

  
W. Bradley Ney

# **Exhibit A**





UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
WASHINGTON, D.C. 20549

DIVISION OF ENFORCEMENT

Lory Stone  
Senior Counsel  
(202) 551-4931  
StoneL@sec.gov

March 21, 2022

VIA ENCRYPTED EMAIL

Covington & Burling LLP  
c/o Anne Scott, Esq.  
One CityCenter  
850 Tenth Street, NW  
Washington, DC 20001-4956

Re: In the Matter of Microsoft Hafnium Cyberattack, (HO-14224)

Dear Ms. Scott:

The enclosed subpoena has been issued pursuant to a formal order entered by the United States Securities and Exchange Commission. Pursuant to Rule 8 of the United States Securities and Exchange Commission's Rules Relating to Investigations, 17 C.F.R. § 203.8, I have enclosed a subpoena for documents issued to Covington & Burling LLP ("Covington"), in connection with the above-referenced investigation.

The enclosed subpoena requires Covington to produce documents to the SEC by April 4, 2022. Please deliver the materials by April 4, 2022 at 5:00 p.m. EST to:

ENF-CPU  
U.S. Securities and Exchange Commission  
14420 Albemarle Point Place, Suite 102  
Chantilly, VA 20151-1750

For smaller electronic productions under 10MB in size, the materials may be emailed to the following email address: [ENF-CPU@sec.gov](mailto:ENF-CPU@sec.gov).

Please also provide a duplicate copy of any document production cover letters to me at StoneL@sec.gov. Additionally, please include the SEC matter number and the name of the requesting attorney when responding.

Please carefully read the subpoena attachment, which contains, among other things, important instructions related to the manner of producing documents. In particular, if Covington prefers to send us copies of original documents, **the staff requests that you scan and produce hard copy documents, as well as electronic documents, in an electronic format consistent with the SEC Data Delivery Standards attached hereto. All electronic documents responsive to the subpoena, including all metadata, should also be produced in their native software format.** If you have any questions concerning the production of documents in an electronic format, please contact me as soon as possible and in any event before producing documents. For security reasons, we strongly encourage the encryption of sensitive documents before production.

When producing the records, please consecutively number and mark each document produced with a symbol that identifies it as being produced by Covington, and provide an index that briefly identifies the documents produced.

In your cover letter(s) accompanying the production of responsive documents, please enclose a list briefly describing each item you send. The list should identify the paragraph(s) in the subpoena attachment to which each item responds. Please also state in the cover letter(s) whether you believe Covington has met the obligations of the subpoena by searching carefully and thoroughly for everything called for by the subpoena, and sending it all to us.

A copy of the subpoena should be included with the documents that are produced. Correspondence should reference case number, case name and requesting SEC staff member.

Passwords for documents, files, compressed archives, and encrypted media should be provided separately either via email addressed to [ENF-CPU@sec.gov](mailto:ENF-CPU@sec.gov), or in a separate cover letter mailed separately from the data. Password correspondence should reference case number, case name and requesting SEC staff member.

In addition, for any documents that qualify as records of regularly conducted activities under Federal Rule of Evidence 902(11), please have the appropriate representative(s) of Covington complete a business records certification (a sample of which is enclosed) and return it with the document production. Execution of this certification may allow the Commission to introduce the documents provided by Covington in any subsequent judicial proceeding, without requiring the testimony of a records custodian.

Please note that, in any matter in which enforcement action is ultimately deemed to be warranted, the Division of Enforcement will not recommend any settlement to the Commission unless the party wishing to settle certifies, under penalty of perjury, that all documents responsive to Commission subpoenas and formal and informal document requests in this matter have been produced.

Enclosed is a copy of the Commission's Form 1662, entitled "Supplemental Information for Persons Requested to Supply Information Voluntarily or Directed to Supply Information Pursuant to a Commission Subpoena." This form explains how we may use the information that Covington provides to the Commission and has other important information.

Please note that the subpoena does not call for the production of any “financial records,” or information contained in such records, maintained by Covington in relation to an account in the name of any “customer,” as those terms are defined in the Right to Financial Privacy Act of 1978 [12 U.S.C. 3401-22] (the “RFPA”), and no such record or information is to be produced in response to this subpoena.

This investigation is a non-public, fact-finding inquiry. We are trying to determine whether there have been any violations of the federal securities laws. The investigation does not mean that we have concluded that anyone has violated the law. Also, the investigation does not mean that we have a negative opinion of any person, entity, or security.

If you have any questions or would like to discuss this matter, you may contact me at (202) 551-4931 or Brad Ney at (202) 551-5317.

Sincerely,



Lory Stone  
Senior Counsel  
Division of Enforcement  
(202) 551-4931  
StoneL@sec.gov

CC: Brad Ney, Senior Counsel, Division of Enforcement

Enclosures: Subpoena and Attachment  
SEC Data Delivery Standards  
SEC Form 1662  
Business Records Certification



## SUBPOENA

# UNITED STATES OF AMERICA SECURITIES AND EXCHANGE COMMISSION

**In the Matter of Microsoft Hafnium Cyberattack, (HO-14224)**

**To:** Covington & Burling LLP  
c/o Anne Scott, Esq.  
One CityCenter  
850 Tenth Street, NW  
Washington, DC 20001-4956

---

☒ **YOU MUST PRODUCE** everything specified in the Attachment to this subpoena to officers of the Securities and Exchange Commission, at the place, date and time specified below:

ENF-CPU, U.S. Securities and Exchange Commission, 14420 Albemarle Point Place, Suite 102  
Chantilly, VA 20151-1750, no later than April 4, 2022 at 5:00 p.m. EST.


---

☐ **YOU MUST TESTIFY** before officers of the Securities and Exchange Commission, at the place, date and time specified below:

---

### FEDERAL LAW REQUIRES YOU TO COMPLY WITH THIS SUBPOENA.

If you do not comply with this subpoena, the SEC may bring an action in Federal Court to enforce this subpoena.  
Failure to comply with a court order enforcing this subpoena may result in the court imposing a fine, imprisonment, or both.

By:   
Lory Stone, Senior Counsel  
U.S. Securities and Exchange Commission  
100 F. Street, NE  
Washington, DC 20549

Date: March 21, 2022

I am an officer of the U.S. Securities and Exchange Commission authorized to issue subpoenas in this matter. The Securities and Exchange Commission has issued a formal order authorizing this investigation under Section 20(a) of the Securities Act of 1933 and Section 21(a) of the Securities Exchange Act of 1934.

---

NOTICE TO WITNESS: If you claim a witness fee or mileage, submit this subpoena with the claim voucher.

**SUBPOENA ATTACHMENT FOR COVINGTON & BURLING LLP**  
**In the Matter of Microsoft Hafnium Cyberattack, (HO-14224)**

March 21, 2022

**A. Definitions**

As used in this subpoena, the words and phrases listed below shall have the following meanings:

1. “Covington & Burling LLP” or “You” or “Your” means the entity doing business under the name “Covington & Burling LLP” (“Covington”), including parents, subsidiaries, affiliates, predecessors, successors, officers, directors, employees, agents, general partners, limited partners, partnerships and aliases, code names, or trade or business names used by any of the foregoing.
2. “Communication” means any correspondence, contact, discussion, e-mail, instant message, or any other kind of oral or written exchange or transmission of information (in the form of facts, ideas, inquiries, or otherwise) and any response thereto between two or more Persons or entities, including, without limitation, all telephone conversations, face-to-face meetings or conversations, internal or external discussions, or exchanges of a Document or Documents.
3. “Concerning” means directly or indirectly, in whole or in part, describing, constituting, evidencing, recording, evaluating, substantiating, concerning, referring to, alluding to, in connection with, commenting on, relating to, regarding, discussing, showing, describing, analyzing or reflecting.
4. “Document” shall include, but is not limited to, any written, printed, or typed matter including, but not limited to all drafts and copies bearing notations or marks not found in the original, letters and correspondence, interoffice communications, slips, tickets, records, worksheets, financial records, accounting documents, bookkeeping documents, memoranda, reports, manuals, telephone logs, facsimiles, messages of any type, telephone messages, text messages, voice mails, tape recordings, notices, instructions, minutes, summaries, notes of meetings, file folder markings, and any other organizational indicia, purchase orders, information recorded by photographic process, including microfilm and microfiche, computer printouts, spreadsheets, and other electronically stored information, including but not limited to writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations that are stored in any medium from which information can be retrieved, obtained, manipulated, or translated.
5. “ESD” means all electronic storage devices which can input, process, output, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. ESD includes, but is not limited to, any data-processing devices (*e.g.*, personal computers, workstations, central processing units, memory, typewriters, printers, facsimile machines, self-contained “laptop” or “notebook”

computers); file, application, or communication servers; internal and peripheral storage devices (*e.g.*, internal and external hard drives, removable media, thumb drives, flash drives, floppy disk drives and diskettes, tape drives and tapes, flash drives, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other memory storage devices); and related communications devices (*e.g.*, modems, cables and connections, recording equipment, RAM or ROM units), or parts that can be used to restrict access to computer hardware (*e.g.*, physical keys and locks).

6. “ESI” means electronically stored information of any kind, type, nature, or description, including metadata; word processing files, including drafts and revisions; spreadsheets, including drafts and revisions; digital communications (*e.g.*, email, instant messages, and voicemails); database files, including schemas and data dictionaries; Documents created or modified by drawing, computer aided design software, Document management software, or project management software; accounting application Documents; presentation software Documents including, but not limited to, slide shows, audio, video files; Documents created or modified by calendaring, task management, collaboration group management, or personal software (*e.g.*, Microsoft Outlook, Office 365, Slack, Google Workspace, Lotus Notes, and Novell Group Wise); image or sound recordings; video; animation; audiovisual recordings; facsimile files; information created or modified through personal data assistants (*e.g.*, Palm Pilot), mobile telephones and smartphones (*e.g.*, iPhone, Android);, including, but not limited to, email, voicemail, short message service (“SMS”) and multimedia message service (“MMS”) messages; information created or modified through forensic imaging technology (*e.g.*, files with .e01 extensions); information created or modified with virtualization software (*e.g.*, virtual hard drives, virtual machine (VM) images, VM configuration files, VM memory files); information created or modified using cloud-based services (*e.g.* Instance Snapshots); information created or modified with the use of compression or archival software (*e.g.*, files with .gho, .zip, .tar, or .dmg extensions); information from network and server activity, including but not limited to, logging files, electronic mail login, routine software logs, access logs, etc.; and information created or modified using development, rapid development, and prototyping software. ESI includes all of the foregoing items in whatever form and by whatever means created, modified, maintained, or stored.
7. “Hafnium Cyberattack” means the cyberattacks described in a March 2, 2021 Microsoft on the Issues blog posting entitled “New nation-state cyberattacks,” and any related cyberattacks by the same or other threat actors.<sup>1</sup>
8. “Informed,” and its derivatives, means to be notified by a third-party Concerning the applicability of the Hafnium Cyberattack or Other Compromise to You.
9. “Learn,” and its derivatives, means to gain or acquire knowledge as to the Hafnium Cyberattack or Other Compromise, or to have reason to believe or to suspect applicability

---

<sup>1</sup> <https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/>.

of the Hafnium Cyberattack or Other Compromise.

10. “Microsoft” means the entity doing business under the name “Microsoft Corporation” including parents, subsidiaries, affiliates, predecessors, successors, officers, directors, employees, agents, general partners, limited partners, partnerships and aliases, code names, or trade or business names used by any of the foregoing.
11. “Other Compromise” means any unauthorized access, other than the Hafnium Cyberattack, to any computer (including any computer system, computer network, or data storage facility) owned or operated by Covington or on Covington’s behalf lasting longer than one day (*i.e.*, longer than 24 consecutive hours), including hacks, data breaches, or ransomware attacks, without limitations based on materiality or access to material non-public information.
12. “Person” means a natural person, firm, association, organization, partnership, business, trust, corporation, bank or any other private or public entity.
13. The term “Reviewed” means examined, assessed, considered, analyzed or evaluated.
14. “Vulnerabilities” includes the vulnerabilities related to the Hafnium Cyberattack that Microsoft has publicly referred to on Microsoft.com as CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065.
15. To the extent necessary to bring within the scope of this this subpoena any information or Documents that might otherwise be construed to be outside its scope:
  - a. the word “or” means “and/or”;
  - b. the word “and” means “and/or”;
  - c. the functional words “each,” “every” “any” and “all” shall each be deemed to include each of the other functional words;
  - d. the masculine gender includes the female gender and the female gender includes the masculine gender; and
  - e. the singular includes the plural and the plural includes the singular.
16. “Relevant Period” means the time period beginning January 1, 2020, and continuing to the present, unless otherwise specified.

**B. Instructions**

1. Unless otherwise specified, this subpoena calls for production of the original Documents and all copies and drafts of same. Documents responsive to this subpoena may be in electronic or paper form. Electronic Documents such as email should be produced in accordance with the attached Document entitled SEC Data Delivery Standards. All responsive electronic Documents, including all metadata, should also be produced in their native software format.
2. For Documents in paper format, you may send the originals, or, if you prefer, you may

send copies of the originals. The Commission cannot reimburse you for the copying costs. If you are sending copies, the staff requests that you scan (rather than photocopy) hard copy Documents and produce them in an electronic format consistent with the SEC Data Delivery Standards. Alternatively, you may send us photocopies of the Documents in paper format. If you choose to send copies, you must secure and retain the originals and store them in a safe place. The staff may later request or require that you produce the originals.

3. Whether you scan or photocopy Documents, the copies must be identical to the originals, including even faint marks or print. Also, please note that if copies of a Document differ in any way, they are considered separate Documents and you must send each one. For example, if you have two copies of the same letter, but only one of them has handwritten notes on it, you must send both the clean copy and the one with notes.
4. In producing a photocopy of an original Document that contains post-it(s), notation flag(s), or other removable markings or attachments which may conceal all or a portion of the markings contained in the original Document, photocopies of the original Document both with and without the relevant post-it(s), notation flag(s), or removable markings or attachments should be produced.
5. Documents should be produced as they are kept in the ordinary course of business or be organized and labeled to correspond with the categories in this request. In that regard, Documents should be produced in a unitized manner, i.e., delineated with staples or paper clips to identify the Document boundaries.
6. Documents should be labeled with sequential numbering (bates-stamped).
7. You must produce all Documents created during, or Concerning, the period from January 1, 2020 to the date of this subpoena, unless otherwise specified.
8. The scope of any given request should not be limited or narrowed based on the fact that it calls for Documents that are responsive to another request.
9. You are not required to produce exact duplicates of any Documents that have been previously produced to the Securities and Exchange Commission staff in connection with this matter. If you are not producing Documents based upon a prior production, please identify the responsive Documents that were previously produced.
10. For any Documents that qualify as records of regularly conducted activities under Federal Rule of Evidence 902(11), please complete a business records certification (a sample of which is enclosed) and return it with the Document production.
11. This subpoena covers all Documents in or subject to your possession, custody or control, including all Documents that are not in your immediate possession but that you have the effective ability to obtain, that are responsive, in whole or in part, to any of the individual requests set forth below. If, for any reason – including a claim of attorney-client privilege



– you do not produce something called for by the request, you should submit a list of what you are not producing. The list should describe each item separately, noting:

- a. its author(s);
  - b. its date;
  - c. its subject matter;
  - d. the name of the Person who has the item now, or the last Person known to have it;
  - e. the names of everyone who ever had the item or a copy of it, and the names of everyone who was told the item's contents;
  - f. the basis upon which you are not producing the responsive Document;
  - g. the specific request in the subpoena to which the Document relates;
  - h. the attorney(s) and the client(s) involved; and
  - i. in the case of the work product doctrine, the litigation for which the Document was prepared in anticipation.
12. If Documents responsive to this subpoena no longer exist because they have been lost, discarded, or otherwise destroyed, you should identify such Documents and give the date on which they were lost, discarded or destroyed.

**C. Documents to be Produced**

1. If, prior to the receipt of this Subpoena, Covington Learned or was Informed that its Exchange server was subject to the Hafnium Cyberattack, produce Documents and Communications sufficient to identify when and how Covington Learned or was Informed, and who Informed Covington.
2. If Covington Learned or was Informed of information suggesting that any unauthorized activity took place in Covington's systems or networks, produce Documents and Communications sufficient to identify the information below. For purposes of responding to this item, include unauthorized activity related to the Hafnium Cyberattack indicative of access and/or compromise.
  - a. When and how Covington was Informed of or Learned this information, and who Informed Covington;
  - b. The nature of the unauthorized or suspected activity at issue, including but not limited to (i) Indicators of Compromise such as web shell hashes, web shell file paths, web shell file names, and web shell signatures, and (ii) what data, files, metadata, or other information was viewed, copied, modified, or exfiltrated; and
  - c. Date(s) or date range(s) of the unauthorized activity.
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. 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.
4. Documents reflecting minutes or notes from all meetings of Covington's board of directors, if applicable, where the Hafnium Cyberattack was discussed, as well as any related Communications regarding the Cyberattack Attack.
5. All forensic investigation reports, penetration or vulnerability testing reports, and assessment reports conducted by Covington or third parties such as security firms Concerning the Microsoft products that contained the Vulnerabilities exploited during the Hafnium Cyberattack; and, for any penetration or Vulnerabilities identified, Covington's response, if any.
6. Documents sufficient to show any tips or complaints from any source Concerning information security incidents, concerns, risks, or flaws Concerning the Microsoft products that contained the Vulnerabilities exploited during the Hafnium Cyberattack, and Covington's response, if any.
7. Documents Concerning any audits of Covington's information security controls by Covington internal audit, independent auditors, and security firms, including but not limited to:
  - a. Any reviews examining Covington's policies and procedures related to cybersecurity,
  - b. Any assessments of the effectiveness of Covington's policies and procedures related to cybersecurity,
  - c. Any resulting recommendations, and
  - d. Any efforts to address the resulting recommendations, including modification, remediation, or calibration of internal controls.
8. Documents sufficient to identify organizational charts reflecting employees responsible for identifying, responding to or otherwise investigating any cybersecurity issues, including those Concerning the Hafnium Cyberattack.

9. Documents Concerning the Hafnium Attack that have been produced to any state or federal agencies, legislative bodies, executive branch offices, or law enforcement agencies (collectively, the “Soliciting Entities”), including the requests/subpoenas from the Soliciting Entities, Covington’s responding cover letters, and bates labeling from the prior productions. This request is continuing and Covington’s productions to the Commission should be updated in the event of future productions to the Soliciting Entities.
10. Documents sufficient to identify how Covington Learned or was Informed of any Other Compromise. Include in Your production information sufficient to identify:
  - a. Date(s) the incident occurred;
  - b. Type of incident (ransomware, data breach, intrusion, *etc.*);
  - c. Strain of malware or ransomware used (if known); and
  - d. Summary description of the incident.

**D. Preservation Request**

In addition to the items responsive to the requests above, please preserve the following:

1. All Documents, Communications, ESD, ESI, logging files, access files, and any other data or metadata related to, Concerning, or reflecting the Hafnium Cyberattack.
2. All Documents, Communications, ESD, ESI, logging files, access files, and any other data or metadata related to, Concerning, or reflecting any Other Compromise.

**DECLARATION OF *[Insert Name]* CERTIFYING RECORDS  
OF REGULARLY CONDUCTED BUSINESS ACTIVITY**

I, the undersigned, *[insert name]*, pursuant to 28 U.S.C. § 1746, declare that:

1. I am employed by Covington & Burling LLP as *[insert position]* and by reason of my position am authorized and qualified to make this declaration. *[if possible supply additional information as to how person is qualified to make declaration, e.g., I am custodian of records, I am familiar with the company's recordkeeping practices or systems, etc.]*
2. I further certify that the documents *[attached hereto or submitted herewith]* and stamped *[insert bates range]* are true copies of records that were:
  - (a) made at or near the time of the occurrence of the matters set forth therein, by, or from information transmitted by, a person with knowledge of those matters;
  - (b) kept in the course of regularly conducted business activity; and
  - (c) made by the regularly conducted business activity as a regular practice.

I declare under penalty of perjury that the foregoing is true and correct. Executed on *[date]*.

---

*[Name]*



## U.S. Securities and Exchange Commission

### Data Delivery Standards

This document describes the technical requirements for paper and electronic document productions to the U.S. Securities and Exchange Commission (SEC). **\*\*Any questions or proposed file formats other than those described below must be discussed with the legal and technical staff of the SEC Division of Enforcement prior to submission.\*\***

---

General Instructions .....	1
Delivery Formats.....	2
I. Imaged Productions.....	3
1. Images .....	3
2. Image Cross-Reference File .....	3
3. Data File.....	3
4. Text.....	3
5. Linked Native Files .....	3
II. Native File Productions without Load Files.....	4
III. Adobe PDF File Productions .....	4
IV. Audio Files.....	4
V. Video Files .....	4
VI. Electronic Trade and Bank Records.....	4
VII. Electronic Phone Records .....	4
VIII. Audit Workpapers.....	5
IX. Mobile Device Data .....	5

---

#### General Instructions

Due to COVID-19 restrictions the current, temporary mailing address for all physical productions sent to the SEC is:  
**ENF-CPU (U.S. Securities & Exchange Commission), 14420 Albemarle Point Place, Suite 102, Chantilly, VA 20151-1750**

Electronic files must be produced in their native format, i.e. the format in which they are ordinarily used and maintained during the normal course of business. For example, an MS Excel file must be produced as an MS Excel file rather than an image of a spreadsheet. **(Note: An Adobe PDF file is not considered a native file unless the document was initially created as a PDF.)**

In the event produced files require the use of proprietary software not commonly found in the workplace, the SEC will explore other format options with the producing party.

The proposed use of file de-duplication methodologies or *computer-assisted review* or *technology-assisted review* (TAR) during

the processing of documents must be discussed with and approved by the legal and technical staff of the Division of Enforcement (ENF). If your production will be de-duplicated it is vital that you 1) preserve any unique metadata associated with the duplicate files, for example, custodian name and file location and, 2) make that unique metadata part of your production to the SEC.

General requirements for **ALL** document productions are:

1. A cover letter must be included with each production and should include the following information:
  - a. Case number, case name and requesting SEC staff member name
  - b. A list of each piece of media included in the production with its unique production volume number
  - c. A list of custodians, identifying the Bates range for each custodian
  - d. The time zone in which the emails were standardized during conversion
  - e. Whether the production contains native files produced from Mac operating system environments
2. Data can be produced on CD, DVD, thumb drive, etc., using the media requiring the least number of deliverables and labeled with the following:
  - a. Case number
  - b. Production date
  - c. Producing party
  - d. Bates range (if applicable)
3. All submissions must be organized by **custodian** unless otherwise instructed.
4. All document family groups, i.e. email attachments, embedded files, etc., should be produced together and children files should follow parent files sequentially in the Bates numbering.
5. All load-ready collections should include only one data load file and one image pointer file.
6. All load-ready text must be produced as separate document-level text files.
7. All load-ready collections should account for custodians in the custodian field.
8. All load-ready collections must provide the extracted contents of any container files to ensure all relevant files are produced as separate records.
9. Audio files should be separated from data files if both are included in the production.
10. Only alphanumeric characters and the underscore character are permitted in file names and folder names. Special characters are not permitted.
11. All electronic productions submitted on media must be produced using industry standard self-extracting encryption software.
12. The SEC uses 7zip to access compressed files. Note that the SEC **cannot** accept files that use AES-256 Jpeg or pkAES-256-Cert Deflate compression methods, even if the files are created with 7zip. If you have any questions or need additional information, please reach out to the requesting SEC staff member.
13. Electronic productions of 20 GB or less are strongly encouraged to be submitted via Secure File Transfer. All Secure File Transfers should be sent to the SEC Centralized Production Unit ([ENF-CPU@sec.gov](mailto:ENF-CPU@sec.gov)) with a CC to the requesting SEC staff member. If you do not have your own Secure File Transfer application, you may reach out to the requesting SEC staff member for a link to the SEC system in order to upload your production. If using the SEC Secure File Transfer system, you will NOT be able to CC individuals outside the SEC on your upload transmission. Note that the SEC **cannot** accept productions made using file sharing sites such as Google Drive, Microsoft Office 365 or Dropbox.
14. Productions containing BSA or SAR material must be delivered on encrypted physical media. The SEC **cannot** accept electronic transmission of BSA or SAR material. Any BSA or SAR material produced should be segregated and appropriately marked as BSA or SAR material, or should be produced separately from other case related material.
15. Passwords for electronic documents, files, compressed archives and encrypted media must be provided separately either via email or in a cover letter apart from the media.
16. All electronic productions should be produced free of computer viruses.
17. Before producing forensically collected images, parties should reach out to the requesting SEC staff member in order to discuss appropriate handling.
18. Before producing unique data sets (large sets of relational data, website reconstruction, chat room data, etc.), parties should reach out to the requesting SEC staff member in order to discuss an appropriate production format.
19. Additional technical descriptions can be found in the addendum to this document.

**\*Please note that productions sent to the SEC via United States Postal Service are subject to Mail Irradiation, and as a result electronic productions may be damaged.\***

## Delivery Formats

### I. Imaged Productions

The SEC prefers that all scanned paper and electronic file collections be produced in a structured format including industry standard load files, Bates numbered image files, native files and searchable document-level text files.

#### 1. Images

- a. Black and white images must be 300 DPI Group IV single-page TIFF files
- b. Color images must be produced in JPEG format
- c. File names cannot contain embedded spaces or special characters (including the comma)
- d. Folder names cannot contain embedded spaces or special characters (including the comma)
- e. All image files must have a unique file name, i.e. Bates number
- f. Images must be endorsed with sequential Bates numbers in the lower right corner of each image
- g. The number of image files per folder should not exceed 2,000 files
- h. Excel spreadsheets should have a placeholder image named by the Bates number of the file
- i. AUTOCAD/photograph files should be produced as a single page JPEG file

#### 2. Image Cross-Reference File

The image cross-reference file (.LOG or .OPT) links the images to the database records. It should be a comma-delimited file consisting of seven fields per line with a line in the cross-reference file for every image in the database with the following format:

*ImageID,VolumeLabel,ImageFilePath,DocumentBreak,FolderBreak,BoxBreak,PageCount*

#### 3. Data File

The data file (.DAT) contains all of the fielded information that will be loaded into the database.

- a. The first line of the .DAT file must be a header row identifying the field names
- b. The .DAT file must use the following *Concordance®* default delimiters:
  - Comma ¶ ASCII character (020)
  - Quote ¢ ASCII character (254)
- c. If the .DAT file is produced in Unicode format it must contain the byte order marker
- d. Date fields should be provided in the format: mm/dd/yyyy
- e. Date and time fields must be two separate fields
- f. The time zone must be included in all time fields
- g. If the production includes imaged emails and attachments, the attachment fields must be included to preserve the parent/child relationship between an email and its attachments
- h. An OCRPATH field must be included to provide the file path and name of the extracted text file on the produced storage media. The text file must be named after the FIRSTBATES. Do not include the text in the .DAT file.
- i. For productions with native files, a LINK field must be included to provide the file path and name of the native file on the produced storage media. The native file must be named after the FIRSTBATES.
- j. BEGATTACH and ENDATTACH fields must be two separate fields
- k. A complete list of metadata fields is available in **Addendum A** to this document

#### 4. Text

Text must be produced as separate document-level text files, not as fields within the .DAT file. The text files must be named per the FIRSTBATES/Image Key and the full path to the text file (OCRPATH) should be included in the .DAT file. Text files may be in either ANSI or Unicode format, however, ALL text files must be in the same format within the same production. Note that productions containing text with foreign characters must produce text files in Unicode format to preserve the foreign characters. Text files must be in a separate folder, and the number of text files per folder should not exceed 2,000 files. There should be no special characters (including commas) in the folder names. For redacted documents, provide the full text for the redacted version.

#### 5. Linked Native Files

Copies of original email and native file documents/attachments must be included for all electronic productions.

- a. Native file documents must be named per the FIRSTBATES number
- b. The full path of the native file must be provided in the .DAT file for the LINK field
- c. The number of native files per folder should not exceed 2,000 files



## II. Native File Production without Load Files

With prior approval, native files may be produced without load files. The native files must be produced as they are maintained in the normal course of business and organized by custodian-named file folders. When approved, native email files (.PST or .MBOX) may be produced. A separate folder should be provided for each custodian.

## III. Adobe PDF File Production

With prior approval, Adobe PDF files may be produced in native file format.

1. All PDFs must be unitized at the document level, i.e., each PDF must represent a discrete document.
2. PDF files should be produced in separate folders named by the custodian. The folders should not contain any special characters (including commas).
3. All PDF files must contain embedded text that includes all discernible words within the document, not selected text or image only. This requires all layers of the PDF to be flattened first.
4. If PDF files are Bates endorsed, the PDF files must be named by the Bates range.

## IV. Audio Files

Audio files from telephone recording systems must be produced in a format that is playable using Microsoft Windows Media Player™. Additionally, the call information (metadata) related to each audio recording **MUST** be provided. The metadata file must be produced in a delimited text format. Field names must be included in the first row of the text file. The metadata must include, at a minimum, the following fields:

- |                        |  |
|------------------------|--|
| 1) Caller Name:        | Caller's name or account/identification number |
| 2) Originating Number: | Caller's phone number                          |
| 3) Called Party Name:  | Called party's name                            |
| 4) Terminating Number: | Called party's phone number                    |
| 5) Date:               | Date of call                                   |
| 6) Time:               | Time of call                                   |
| 7) Filename:           | Filename of audio file                         |

## V. Video Files

Video files must be produced in a format that is playable using Microsoft Windows Media Player™.

## VI. Electronic Trade and Bank Records

When producing electronic trade records, bank records, or financial statements, provide the files in one of the following formats:

1. MS Excel spreadsheet with header information detailing the field structure. If any special codes exist in the dataset, a separate document must be provided that details all such codes. If details of the field structure do not fit in the header, a separate document must be provided that includes such details.
2. Delimited text file with header information detailing the field structure. The preferred delimiter is a vertical bar "|". If any special codes exist in the dataset, a separate document must be provided that details all such codes. If details of the field structure do not fit in the header, a separate document must be provided that includes such details.

## VII. Electronic Phone Records

When producing electronic phone records, provide the files in the following format:

1. MS Excel spreadsheet with header information detailing the field structure. If any special codes exist in the dataset, a separate document must be provided that details all such codes. If details of the field structure do not fit in the header, a separate document must be provided that includes such details. Data must be formatted in its native format (i.e. dates in a date format, numbers in an appropriate numerical format, and numbers with leading zeroes as text).
  - a. The metadata that must be included is outlined in **Addendum B** of this document. Each field of data must be loaded into a separate column. For example, Date and Start\_Time must be produced in separate columns and not combined into a single column containing both pieces of information. Any fields of data that are provided in addition to those listed in **Addendum B** must also be loaded into separate columns.

### **VIII. Audit Workpapers**

The SEC prefers for workpapers to be produced in two formats: (1) With Bates numbers in accordance with the SEC Data Delivery Standards; and (2) in native format or if proprietary software was used, on a standalone laptop with the appropriate software loaded so that the workpapers may be reviewed as they would have been maintained in the ordinary course of business. The laptop must have printing capability, and when possible, the laptop should be configured to enable a Virtual Machine (VM) environment.

### **IX. Mobile Device Data**

Before producing mobile device data (including but not limited to text messages) parties should reach out to the requesting SEC staff member in order to discuss the appropriate production format

## ADDENDUM A

The metadata of electronic document collections should be extracted and provided in a .DAT file using the field definition and formatting described below:

Field Name	Sample Data	Description
FIRSTBATES	EDC0000001	First Bates number of native file document/email
LASTBATES	EDC0000001	Last Bates number of native file document/email **The LASTBATES field should be populated for single page documents/emails.
ATTACHRANGE	EDC0000001 - EDC0000015	Bates number of the first page of the parent document to the Bates number of the last page of the last attachment "child" document
BEGATTACH	EDC0000001	First Bates number of attachment range
ENDATTACH	EDC0000015	Last Bates number of attachment range
PARENT_BATES	EDC0000001	First Bates number of parent document/Email **This PARENT_BATES field should be populated in each record representing an attachment "child" document
CHILD_BATES	EDC0000002; EDC0000014	First Bates number of "child" attachment(s); can be more than one Bates number listed depending on the number of attachments **The CHILD_BATES field should be populated in each record representing a "parent" document
CUSTODIAN	Smith, John	Email: Mailbox where the email resided Native: Name of the individual or department from whose files the document originated
FROM	John Smith	Email: Sender Native: Author(s) of document **semi-colon should be used to separate multiple entries
TO	Coffman, Janice; LeeW [mailto:LeeW@MSN.com]	Recipient(s) **semi-colon should be used to separate multiple entries
CC	Frank Thompson [mailto:frank_Thompson@cdt.com]	Carbon copy recipient(s) **semi-colon should be used to separate multiple entries
BCC	John Cain	Blind carbon copy recipient(s) **semi-colon should be used to separate multiple entries
SUBJECT	Board Meeting Minutes	Email: Subject line of the email Native: Title of document (if available)
FILE_NAME	BoardMeetingMinutes.docx	Native: Name of the original native file, including extension
DATE_SENT	10/12/2010	Email: Date the email was sent Native: (empty)
TIME_SENT/TIME_ZONE	07:05 PM GMT	Email: Time the email was sent/ Time zone in which the emails were standardized during conversion. Native: (empty) **This data must be a separate field and cannot be combined with the DATE_SENT field

TIME_ZONE	GMT	The time zone in which the emails were standardized during conversion. Email: Time zone Native: (empty)
LINK	D:\001\EDC0000001.msg	Hyperlink to the email or native file document **The linked file must be named per the FIRSTBATES number
MIME_TYPE	application/msword	The content type of an email or native file document as identified/extracted from the header
FILE_EXTEN	MSG	The file type extension representing the email or native file document; will vary depending on the format
AUTHOR	John Smith	Email: (empty) Native: Author of the document
LAST_AUTHOR	Jane Doe	Email: (empty) Native: Last Author of the document
DATE_CREATED	10/10/2010	Email: (empty) Native: Date the document was created
TIME_CREATED/TIME_ZONE	10:25 AM GMT	Email: (empty) Native: Time the document was created including time zone **This data must be a separate field and cannot be
DATE_MOD	10/12/2010	Email: (empty) Native: Date the document was last modified
TIME_MOD/TIME_ZONE	07:00 PM GMT	Email: (empty) Native: Time the document was last modified including the time zone **This data must be a separate field and cannot be
DATE_ACCESSD	10/12/2010	Email: (empty) Native: Date the document was last accessed
TIME_ACCESSD/TIME_ZONE	07:00 PM GMT	Email: (empty) Native: Time the document was last accessed including the time zone **This data must be a separate field and cannot be
PRINTED_DATE	10/12/2010	Email: (empty) Native: Date the document was last printed
FILE_SIZE	5,952	Size of native file document/email in KB
PGCOUNT	1	Number of pages in native file document/email
PATH	J:\Shared\SmithJ\October Agenda.doc	Email: (empty) Native: Path where native file document was stored including original file name.
INTFILEPATH	Personal Folders\Deleted Items\Board Meeting Minutes.msg	Email: original location of email including original file name. Native: (empty)
INTMSGID	<000805c2c71b\$75977050\$cb8306d1@MSN>	Email: Unique Message ID Native: (empty)

HEADER	Return-Path: <example_from@dc.edu> X-SpamCatcher-Score:1[X] Received:from[136.167.40.119] (HELO dc.edu) by fe3.dc.edu (CommuniGate Pro SMTP4.1.8) with ESMTP-TLS id 61258719 for example_to@mail.dc.edu; Mon, 23 Aug 2004 11:40:10 - 0400 Message-ID: <4129F3CA.2020509@dc.edu> Date: Mon, 23 Aug 2005 11:40:36 -400 From: Taylor Evans <example_from@dc.edu> User-Agent:Mozilla/5.0 (Windows;U; Windows NT 5.1; en-US;rv:1.0.1) Gecko/20020823 Netscape/7.0 X-Accept-Language:en-us,en MIME-Version:1.0 To: Jon Smith <example_to@mail.dc.edu> Subject:Business Development Meeting Content-Type: text/plain;charset=us-ascii; format=flowed Content-Transfer-Encoding:7bit	Email: The email header information Native: (empty)
MD5HASH	d131dd02c5e6eec4693d9a069 8aff95c 2fcab58712467eab4004583eb 8fb7f89	MD5 Hash value of the document.
OCRPATH	TEXT/001/EDC0000001.txt	Path to extracted text of the native file

Sample Image Cross-Reference File:

```

IMG00000001,,E:\001\IMG00000001.TIF,Y,,,
IMG00000002,,E:\001\IMG00000002.TIF,,,,
IMG00000003,,E:\001\IMG00000003.TIF,,,,
IMG00000004,,E:\001\IMG00000004.TIF,Y,,,
IMG00000005,,E:\001\IMG00000005.TIF,Y,,,
IMG00000006,,E:\001\IMG00000006.TIF,,,,

```

## **ADDENDUM B**

For Electronic Phone Records, include the following fields in separate columns:

For Calls:

- 1) Account Number
- 2) Connection Date – Date the call was received or made
- 3) Connection Time – Time call was received or made
- 4) Seizure Time – Time it took for the call to be placed in seconds
- 5) Originating Number – Phone that placed the call
- 6) Terminating Number – Phone that received the call
- 7) Elapsed Time – The length of time the call lasted, preferably in seconds
- 8) End Time – The time the call ended
- 9) Number Dialed – Actual number dialed
- 10) IMEI Originating – Unique id to phone used to make call
- 11) IMEI Terminating– Unique id to phone used to receive call
- 12) IMSI Originating – Unique id to phone used to make call
- 13) IMSI Terminating- Unique id to phone used to receive call
- 14) Call Codes – Identify call direction or other routing information
- 15) Time Zone – Time Zone in which the call was received or placed, if applicable

For Text messages:

- 1) Account Number
- 2) Connection Date – Date the text was received or made
- 3) Connection Time – Time text was received or made
- 4) Originating Number – Who placed the text
- 5) Terminating Number – Who received the text
- 6) IMEI Originating – Unique id to phone used to make text
- 7) IMEI Terminating– Unique id to phone used to receive text
- 8) IMSI Originating - Unique id to phone used to make text
- 9) IMSI Terminating- Unique id to phone used to receive text
- 10) Text Code – Identify text direction, or other text routing information
- 11) Text Type Code – Type of text message (sent SMS, MMS, or other)
- 12) Time Zone – Time Zone in which the call was received or placed, if applicable

For Mobile Data Usage:

- 1) Account Number
- 2) Connection Date – Date the data was received or made
- 3) Connection Time – Time data was received or made
- 4) Originating number – Number that used data
- 5) IMEI Originating – Unique id of phone that used data
- 6) IMSI Originating - Unique id of phone that used data
- 7) Data or Data codes – Identify data direction, or other data routing information
- 8) Time Zone – Time Zone in which the call was received or placed, if applicable

**SECURITIES AND EXCHANGE COMMISSION**  
**Washington, D.C. 20549**

**Supplemental Information for Persons Requested to Supply  
Information Voluntarily or Directed to Supply Information  
Pursuant to a Commission Subpoena**

**A. False Statements and Documents**

Section 1001 of Title 18 of the United States Code provides that fines and terms of imprisonment may be imposed upon:

[W]hoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully--

- (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;
- (2) makes any materially false, fictitious, or fraudulent statement or representation; or
- (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry.

Section 1519 of Title 18 of the United States Code provides that fines and terms of imprisonment may be imposed upon:

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States . . . , or in relation to or contemplation of any such matter.

**B. Testimony**

If your testimony is taken, you should be aware of the following:

1. *Record.* Your testimony will be transcribed by a reporter. If you desire to go off the record, please indicate this to the Commission employee taking your testimony, who will determine whether to grant your request. The reporter will not go off the record at your, or your counsel's, direction.
2. *Counsel.* You have the right to be accompanied, represented and advised by counsel of your choice. Your counsel may advise you before, during and after your testimony; question you briefly at the conclusion of your testimony to clarify any of the answers you give during testimony; and make summary notes during your testimony solely for your use. If you are accompanied by counsel, you may consult privately.

If you are not accompanied by counsel, please advise the Commission employee taking your testimony if, during the testimony, you desire to be accompanied, represented and advised by counsel. Your testimony will be adjourned once to afford you the opportunity to arrange to be so accompanied, represented or advised.

You may be represented by counsel who also represents other persons involved in the Commission's investigation. This multiple representation, however, presents a potential conflict of interest if one client's interests are or may be adverse to another's. If you are represented by counsel who also represents other persons involved in the investigation, the Commission will assume that you and counsel have discussed and resolved all issues concerning possible conflicts of interest. The choice of counsel, and the responsibility for that choice, is yours.

3. *Transcript Availability.* Rule 6 of the Commission's Rules Relating to Investigations, 17 CFR 203.6, states:

A person who has submitted documentary evidence or testimony in a formal investigative proceeding shall be entitled, upon written request, to procure a copy of his documentary evidence or a transcript of his testimony on payment of the appropriate fees: *Provided, however,* That in a nonpublic formal investigative proceeding the Commission may for good cause deny such request. In any event, any witness, upon proper identification, shall have the right to inspect the official transcript of the witness' own testimony.

If you wish to purchase a copy of the transcript of your testimony, the reporter will provide you with a copy of the appropriate form. Persons requested to supply information voluntarily will be allowed the rights provided by this rule.

4. *Perjury.* Section 1621 of Title 18 of the United States Code provides that fines and terms of imprisonment may be imposed upon:

Whoever--

(1) having taken an oath before a competent tribunal, officer, or person, in any case in which a law of the United States authorizes an oath to be administered, that he will testify, declare, depose, or certify truly, or that any written testimony, declaration, deposition, or certificate by him subscribed, is true, willfully and contrary to such oath states or subscribes any material matter which he does not believe to be true; or

(2) in any declaration, certificate, verification, or statement under penalty of perjury as permitted under section 1746 of title 28, United States Code, willfully subscribes as true any material matter which he does not believe to be true.

5. *Fifth Amendment and Voluntary Testimony.* Information you give may be used against you in any federal, state, local or foreign administrative, civil or criminal proceeding brought by the Commission or any other agency.

You may refuse, in accordance with the rights guaranteed to you by the Fifth Amendment to the Constitution of the United States, to give any information that may tend to incriminate you.

If your testimony is not pursuant to subpoena, your appearance to testify is voluntary, you need not answer any question, and you may leave whenever you wish. Your cooperation is, however, appreciated.

6. *Formal Order Availability.* If the Commission has issued a formal order of investigation, it will be shown to you during your testimony, at your request. If you desire a copy of the formal order, please make your request in writing.

### **C. Submissions and Settlements**

Rule 5(c) of the Commission's Rules on Informal and Other Procedures, 17 CFR 202.5(c), states:

Persons who become involved in . . . investigations may, on their own initiative, submit a written statement to the Commission setting forth their interests and position in regard to the subject matter of the investigation. Upon request, the staff, in its discretion, may advise such persons of the general nature of the investigation, including the indicated violations as they pertain to them, and the amount of time that may be available for preparing and submitting a statement prior to the presentation of a staff recommendation to the Commission for the commencement of an administrative or injunction proceeding. Submissions by interested persons should be forwarded to the appropriate Division Director or Regional Director with a copy to the staff members conducting the investigation and should be clearly referenced to the specific investigation to which they relate. In the event a recommendation for the commencement of an enforcement proceeding is presented by the staff, any submissions by interested persons will be forwarded to the Commission in conjunction with the staff memorandum.

The staff of the Commission routinely seeks to introduce submissions made pursuant to Rule 5(c) as evidence in Commission enforcement proceedings, when the staff deems appropriate.

Rule 5(f) of the Commission's Rules on Informal and Other Procedures, 17 CFR 202.5(f), states:

In the course of the Commission's investigations, civil lawsuits, and administrative proceedings, the staff, with appropriate authorization, may discuss with persons involved the disposition of such matters by consent, by settlement, or in some other manner. It is the policy of the Commission, however, that the disposition of any such matter may not, expressly or impliedly, extend to any criminal charges that have been, or may be, brought against any such person or any recommendation with respect thereto. Accordingly, any person involved in an enforcement matter before the Commission who consents, or agrees to consent, to any judgment or order does so solely for the purpose of resolving the claims against him in that investigative, civil, or administrative matter and not for the purpose of resolving any criminal charges that have been, or might be, brought against him. This policy reflects the fact that neither the Commission nor its staff has the authority or responsibility for instituting, conducting, settling, or otherwise disposing of criminal proceedings. That authority and responsibility are vested in the Attorney General and representatives of the Department of Justice.

### **D. Freedom of Information Act**

The Freedom of Information Act, 5 U.S.C. 552 (the "FOIA"), generally provides for disclosure of information to the public. Rule 83 of the Commission's Rules on Information and Requests, 17 CFR 200.83, provides a procedure by which a person can make a written request that information submitted to the Commission not be disclosed under the FOIA. That rule states that no determination as to the validity of such a request will be made until a request for disclosure of the information under the FOIA is received. Accordingly, no response to a request that information not be disclosed under the FOIA is necessary or will be given until a request for disclosure under the FOIA is received. If you desire an acknowledgment of receipt of your written request that information not be disclosed under the FOIA, please provide a duplicate request, together with a stamped, self-addressed envelope.



## **E. Authority for Solicitation of Information**

*Persons Directed to Supply Information Pursuant to Subpoena.* The authority for requiring production of information is set forth in the subpoena. Disclosure of the information to the Commission is mandatory, subject to the valid assertion of any legal right or privilege you might have.

*Persons Requested to Supply Information Voluntarily.* One or more of the following provisions authorizes the Commission to solicit the information requested: Sections 19 and/or 20 of the Securities Act of 1933; Section 21 of the Securities Exchange Act of 1934; Section 321 of the Trust Indenture Act of 1939; Section 42 of the Investment Company Act of 1940; Section 209 of the Investment Advisers Act of 1940; and 17 CFR 202.5. Disclosure of the requested information to the Commission is voluntary on your part.

## **F. Effect of Not Supplying Information**

*Persons Directed to Supply Information Pursuant to Subpoena.* If you fail to comply with the subpoena, the Commission may seek a court order requiring you to do so. If such an order is obtained and you thereafter fail to supply the information, you may be subject to civil and/or criminal sanctions for contempt of court. In addition, Section 21(c) of the Securities Exchange Act of 1934, Section 42(c) of the Investment Company Act of 1940, and Section 209(c) of the Investment Advisers Act of 1940 provide that fines and terms of imprisonment may be imposed upon any person who shall, without just cause, fail or refuse to attend and testify or to answer any lawful inquiry, or to produce books, papers, correspondence, memoranda, and other records in compliance with the subpoena.

*Persons Requested to Supply Information Voluntarily.* There are no direct sanctions and thus no direct effects for failing to provide all or any part of the requested information.

## **G. Principal Uses of Information**

The Commission's principal purpose in soliciting the information is to gather facts in order to determine whether any person has violated, is violating, or is about to violate any provision of the federal securities laws or rules for which the Commission has enforcement authority, such as rules of securities exchanges and the rules of the Municipal Securities Rulemaking Board. Facts developed may, however, constitute violations of other laws or rules. Information provided may be used in Commission and other agency enforcement proceedings. Unless the Commission or its staff explicitly agrees to the contrary in writing, you should not assume that the Commission or its staff acquiesces in, accedes to, or concurs or agrees with, any position, condition, request, reservation of right, understanding, or any other statement that purports, or may be deemed, to be or to reflect a limitation upon the Commission's receipt, use, disposition, transfer, or retention, in accordance with applicable law, of information provided.

## **H. Routine Uses of Information**

The Commission often makes its files available to other governmental agencies, particularly United States Attorneys and state prosecutors. There is a likelihood that information supplied by you will be made available to such agencies where appropriate. Whether or not the Commission makes its files available to other governmental agencies is, in general, a confidential matter between the Commission and such other governmental agencies.

Set forth below is a list of the routine uses which may be made of the information furnished.

1. To appropriate agencies, entities, and persons when (1) the SEC suspects or has confirmed that there has been a breach of the system of records, (2) the SEC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the SEC (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the SEC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
2. To other Federal, state, local, or foreign law enforcement agencies; securities self-regulatory organizations; and foreign financial regulatory authorities to assist in or coordinate regulatory or law enforcement activities with the SEC.
3. To national securities exchanges and national securities associations that are registered with the SEC, the Municipal Securities Rulemaking Board; the Securities Investor Protection Corporation; the Public Company Accounting Oversight Board; the Federal banking authorities, including, but not limited to, the Board of Governors of the Federal Reserve System, the Comptroller of the Currency, and the Federal Deposit Insurance Corporation; state securities regulatory agencies or organizations; or regulatory authorities of a foreign government in connection with their regulatory or enforcement responsibilities.
4. By SEC personnel for purposes of investigating possible violations of, or to conduct investigations authorized by, the Federal securities laws.
5. In any proceeding where the Federal securities laws are in issue or in which the Commission, or past or present members of its staff, is a party or otherwise involved in an official capacity.

6. In connection with proceedings by the Commission pursuant to Rule 102(e) of its Rules of Practice, 17 CFR 201.102(e).

7. To a bar association, state accountancy board, or other Federal, state, local, or foreign licensing or oversight authority; or professional association or self-regulatory authority to the extent that it performs similar functions (including the Public Company Accounting Oversight Board) for investigations or possible disciplinary action.

8. To a Federal, state, local, tribal, foreign, or international agency, if necessary to obtain information relevant to the SEC's decision concerning the hiring or retention of an employee; the issuance of a security clearance; the letting of a contract; or the issuance of a license, grant, or other benefit.

9. To a Federal, state, local, tribal, foreign, or international agency in response to its request for information concerning the hiring or retention of an employee; the issuance of a security clearance; the reporting of an investigation of an employee; the letting of a contract; or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

10. To produce summary descriptive statistics and analytical studies, as a data source for management information, in support of the function for which the records are collected and maintained or for related personnel management functions or manpower studies; may also be used to respond to general requests for statistical information (without personal identification of individuals) under the Freedom of Information Act.

11. To any trustee, receiver, master, special counsel, or other individual or entity that is appointed by a court of competent jurisdiction, or as a result of an agreement between the parties in connection with litigation or administrative proceedings involving allegations of violations of the Federal securities laws (as defined in section 3(a)(47) of the Securities Exchange Act of 1934, 15 U.S.C. 78c(a)(47)) or pursuant to the Commission's Rules of Practice, 17 CFR 201.100 through 900 or the Commission's Rules of Fair Fund and Disgorgement Plans, 17 CFR 201.1100 through 1106, or otherwise, where such trustee, receiver, master, special counsel, or other individual or entity is specifically designated to perform particular functions with respect to, or as a result of, the pending action or proceeding or in connection with the administration and enforcement by the Commission of the Federal securities laws or the Commission's Rules of Practice or the Rules of Fair Fund and Disgorgement Plans.

12. To any persons during the course of any inquiry, examination, or investigation conducted by the SEC's staff, or in connection with civil litigation, if the staff has reason to believe that the person to whom the record is disclosed may have further information about the matters related therein, and those matters appeared to be relevant at the time to the subject matter of the inquiry.

13. To interns, grantees, experts, contractors, and others who have been engaged by the Commission to assist in the performance of a service related to this system of records and who need access to the records for the purpose of assisting the Commission in the efficient administration of its programs, including by performing clerical, stenographic, or data analysis functions, or by reproduction of records by electronic or other means. Recipients of these records shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

14. In reports published by the Commission pursuant to authority granted in the Federal securities laws (as such term is defined in section 3(a)(47) of the Securities Exchange Act of 1934, 15 U.S.C. 78c(a)(47)), which authority shall include, but not be limited to, section 21(a) of the Securities Exchange Act of 1934, 15 U.S.C. 78u(a)).

15. To members of advisory committees that are created by the Commission or by Congress to render advice and recommendations to the Commission or to Congress, to be used solely in connection with their official designated functions.

16. To any person who is or has agreed to be subject to the Commission's Rules of Conduct, 17 CFR 200.735-1 through 200.735-18, and who assists in the investigation by the Commission of possible violations of the Federal securities laws (as such term is defined in section 3(a)(47) of the Securities Exchange Act of 1934, 15 U.S.C. 78c(a)(47)), in the preparation or conduct of enforcement actions brought by the Commission for such violations, or otherwise in connection with the Commission's enforcement or regulatory functions under the Federal securities laws.

17. To a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.

18. To members of Congress, the press, and the public in response to inquiries relating to particular Registrants and their activities, and other matters under the Commission's jurisdiction.

19. To prepare and publish information relating to violations of the Federal securities laws as provided in 15 U.S.C. 78c(a)(47)), as amended.

20. To respond to subpoenas in any litigation or other proceeding.

21. To a trustee in bankruptcy.

22. To any governmental agency, governmental or private collection agent, consumer reporting agency or commercial reporting agency, governmental or private employer of a debtor, or any other person, for collection, including collection by administrative offset, Federal salary offset, tax refund offset, or administrative wage garnishment, of amounts owed as a result of Commission civil or administrative proceedings.

23. To another Federal agency or Federal entity, when the SEC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

\* \* \* \* \*

*Small Business Owners:* The SEC always welcomes comments on how it can better assist small businesses. If you would like more information, or have questions or comments about federal securities regulations as they affect small businesses, please contact the Office of Small Business Policy, in the SEC's Division of Corporation Finance, at 202-551-3460. If you would prefer to comment to someone outside of the SEC, you can contact the Small Business Regulatory Enforcement Ombudsman at <http://www.sba.gov/ombudsman> or toll free at 888-REG-FAIR. The Ombudsman's office receives comments from small businesses and annually evaluates federal agency enforcement activities for their responsiveness to the special needs of small business.

# **Exhibit B**

**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 is 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.<sup>1</sup>

## **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

---

<sup>1</sup> 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).<sup>2</sup>

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.

---

<sup>2</sup> 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>.

Combating 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.

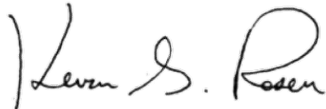
If, however, the Staff has a proposal for narrowing this request so as to limit the burden on Covington, we remain open to considering limitations on information relating to non-clients impacted by the cyberattack.

#### **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](mailto:tboutrous@gibsondunn.com); Kevin Rosen at (213) 229-7635 or [krosen@gibsondunn.com](mailto:krosen@gibsondunn.com); or Richard Grime at (202) 955-8219 or [rgrime@gibsondunn.com](mailto: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.

# **Exhibit C**



DIVISION OF  
ENFORCEMENT

UNITED STATES  
SECURITIES AND EXCHANGE COMMISSION  
WASHINGTON, D.C. 20549

W. Bradley Ney  
Senior Counsel

Telephone: (202) 551-5317  
Email: NeyW@sec.gov

July 14, 2022

VIA EMAIL (tboutrous@gibsondunn.com)

Theodore J. Boutrous, Jr., Esq.  
Gibson Dunn & Crutcher LLP  
1050 Connecticut Ave., N.W.  
Washington, D.C. 20036

Re: In the Matter of Microsoft Hafnium Cyberattack, HO-14224

Dear Mr. Boutrous:

I write in response to your letter dated June 10, 2022, which asserted certain objections to the March 21, 2022 subpoena (the "Subpoena") issued by the U.S. Securities & Exchange Commission (the "Commission") to the law firm Covington & Burling LLP ("Covington"). Specifically, your letter objected to the production of documents in response to Request No. 3 of the Commission's Subpoena relating to the impact of the Microsoft Hafnium cyberattack on Covington's public company clients.<sup>1</sup>

According to Covington, in or around November 2020, threat actors associated with the Microsoft Hafnium cyberattack gained unauthorized access to Covington's computer network and certain individual devices. In connection with the cyberattack, the threat actors were able to access information of certain firm clients, including hundreds of public companies and other companies regulated by the Commission. According to Covington, the firm voluntarily provided information regarding the cyberattack to the FBI. Covington did not voluntarily provide information regarding the cyberattack to the Commission. After learning of the cyberattack, we sent the Subpoena to Covington to ascertain information regarding the impact of the cyberattack on entities regulated by the Commission.

Request No. 3 of the Subpoena seeks specific, targeted information regarding public company clients of Covington whose information was viewed, copied, modified or exfiltrated in connection with the breach. Specifically, Request No. 3 seeks documents sufficient to identify: (1) the name of any impacted public company clients; (2) the nature and extent of the

---

<sup>1</sup> As described in your letter and discussed with Covington, "public company clients" should be understood to reference both: (1) companies with securities (including ADRs) traded on U.S. exchanges and (2) companies that are regulated by the Commission pursuant to the federal securities laws, such as brokers, dealers, exchanges and investment advisors.

unauthorized activity; and (3) any communications with the impacted clients or other impacted parties concerning the suspected unauthorized activity. Contrary to the assertions in your letter, the staff is not seeking privileged communications between Covington and its clients, and has specifically told Covington that it could withhold and produce a privilege log for any privileged documents or communications responsive to the Subpoena.

With respect to your request for a meeting with our Director and Chief Counsel to discuss the issues laid out above, they decline such a meeting at this time. Associate Directors Melissa Hodgman and Carolyn Welshhans are open to a meeting if you so desire.

## **I. The Subpoena Seeks Information in Covington's Sole Possession Necessary to Carry Out The Commission's Mission of Protecting Investors.**

Cybersecurity issues are currently at the forefront of the Commission's agenda, and have been for some time. According to the FBI, cybersecurity incidents cost the American public billions of dollars annually,<sup>2</sup> and by some estimates may cost companies as much as \$10.5 trillion globally by 2025.<sup>3</sup> Threat actors regularly target public companies and financial sector participants regulated by the Commission. To address the increasing cyber-threat to regulated entities, in late 2017, the Division of Enforcement created a new Cyber Unit focusing on cybersecurity-related violations, including trading on non-public information obtained through illegal cyber-activity, failures to disclose material cybersecurity events and risks as required by the Securities Act of 1933 or the Securities Exchange Act of 1934, and violations of other provisions of the federal securities laws, such as Reg. S-P, Reg. SCI, and Reg. S-ID. The last two appointed Commission chairs have devoted significant public speeches and statements to the subject of cybersecurity.<sup>4</sup> So far this year, the Commission proposed multiple new rules relating to cybersecurity controls and disclosure of cyber-incidents, and markedly expanded staffing for the Cyber Unit.<sup>5</sup> The significance and importance of cybersecurity issues to the Commission's three-part mission has never been more apparent than in the last several years, where state actors have targeted public companies and regulated entities with large-scale cyberattacks, often seeking to profit at the expense of investors who the Commission is charged with protecting.

---

<sup>2</sup> See *Internet Crime Report*, Federal Bureau of Investigation (2021) available at [https://www.ic3.gov/Media/PDF/AnnualReport/2021\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf).

<sup>3</sup> Steve Morgan, *Cybercrime to Cost the World \$10.5 Trillion Annually by 2025*, *Cybercrime Mag.* (Nov. 13, 2020), <https://tinyurl.com/czw7bce9>.

<sup>4</sup> See, e.g., *Cyber Security and Securities Laws*, Chair Gary Gensler Speech at Northwestern Pritzker School of Law's Annual Security Regulation Institute (January 24, 2022) available at <https://www.sec.gov/news/speech/gensler-cybersecurity-and-securities-laws-20220124>; *Working on Team Cyber*, Chair Gary Gensler Remarks Before the Joint Meeting of the Financial and Banking Information and Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC) (April 14, 2022) available at <https://www.sec.gov/news/speech/gensler-speech-joint-meeting-041422>; Chair Jay Clayton Speech on *SEC Rule Making, the Past Year, the Year Ahead, and Challenges Caused by Brexit, Libor Transition, and Cybersecurity Risks* (Dec. 6, 2018) available at <https://www.sec.gov/news/speech/speech-clayton-120618>; Chair Jay Clayton Statement on Cybersecurity (Sept. 20, 2017) available at <https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20>.

<sup>5</sup> *SEC Proposes Cybersecurity Risk Management Rules for Registered Investment Advisors and Funds* (February 9, 2022) available at <https://www.sec.gov/news/press-release/2022-20>; *SEC Proposes Rules on Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure by Public Companies* (March 9, 2022) available at <https://www.sec.gov/news/press-release/2022-39>.

As a large law firm with hundreds of public company clients, Covington is regularly in possession of material information, the theft of which puts investors at significant risk. Neither Covington's position as a victim of a cyberattack, nor the fact that it is a law firm, insulate it from the staff's legitimate investigative responsibilities. The staff regularly seeks information from companies that were victims of cyberattacks for a number of reasons, including to (1) understand the nature and scope of the attack, (2) assess and identify trading based on the attack, and (3) determine relevant disclosure obligations for public companies impacted by the attack. The Commission has previously brought cases against threat actors who traded on information obtained through cyberattacks, including cyberattacks on law firms, as well as against companies that failed to disclose the material impact of cyberattacks to investors.<sup>6</sup>

Against this backdrop, the significance of the requested information to the Commission's ongoing mission of investor protection is apparent and the staff's request for specific information regarding regulated entities targeted during a known cyberattack cannot in good faith be described as "speculative." The investigative powers of the Commission are statutory and are analogous to those of a grand jury. *United States v. Morton Salt Co.*, 338 U.S. at 642-43. Like a grand jury, an agency "can investigate merely on suspicion that the law is being violated, or just because it wants assurance that it is not." *Id.* Thus, courts have recognized that the SEC is acting within the scope of its Congressionally-granted authority even where its investigation is based on nothing more than "official curiosity." *See, e.g., Arthur Young & Co.*, 584 F.2d at 1023-24 & n. 45. Indeed, a district court is bound to enforce an administrative subpoena if the information sought "is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant." *Morton Salt*, 338 U.S. 632, 652 (1950). In this instance, the staff has far more basis than "official curiosity" for seeking the requested information. The staff knows that a foreign actor intentionally and maliciously accessed the files of Covington's clients, which include public companies and other entities regulated by the Commission, and it would be an abdication of our official responsibility not to determine whether the malicious activity resulted in violations of the federal securities laws to the detriment of investors.

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

In response to Request No. 3, you raise objections based on D.C. Rule of Professional Conduct 1.6 ("D.C. Rule 1.6"), the attorney-client privilege and work-product doctrine, and various prudential concerns that you claim counsel against the staff seeking this information. These objections mirror the objections that Covington itself – prior to seeking outside counsel – initially raised in response to the Subpoena. After due consideration, we remain unconvinced that any of these objections justifies Covington's blanket refusal to produce information in response to Request No. 3.

---

<sup>6</sup> *See, e.g., Chinese Traders Charged with Trading on Hacked Nonpublic Information Stolen From Two Law Firms* (Dec. 27, 2016) available at <https://www.sec.gov/news/pressrelease/2016-280.html>; *Altaba, Formerly Known as Yahoo!, Charged with Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay \$35 Million* (April 14, 2018) available at <https://www.sec.gov/news/press-release/2018-71>.

As an overall matter, Covington objects to the subpoena based on D.C. Rule 1.6(a)(1), which generally prevents an attorney from “knowingly . . . reveal[ing] a confidence or secret of the lawyer’s client.” However, if issued a subpoena, the recipient must comply notwithstanding Rule 1.6, absent some other valid objection. This is because, as you acknowledge in your letter, Rule 1.6(e)(2)(a) provides an exception to the general rule, and permits the lawyer to “reveal client confidences or secrets” when “required by law or court order.” The U.S. District Court for the District of Columbia has specifically considered the relationship between Rule 1.6(a) and 1.6(e) in the context of a subpoena seeking communications between a law firm and its clients in a civil action, and determined that a subpoena is a court order subject to exception under the Rule. *See In Re: Motion To Compel Compliance With Subpoena Directed To Cooke Legal Group, PLLC*, 333 F.R.D. 291, 296 (D.D.C. 2019) (granting plaintiff’s motion to compel production of the subpoenaed documents). Specifically, the Court in that case held that Rule 1.6 did “not bar [the law firm] from complying with the instant subpoena, but instead specifically permits the firm to do so” because of the application of the Rule 1.6(e) exception. *Id.*

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

In support of your position, you also cite to D.C. Bar Ethics Opinion 214, claiming that it requires the attorney to “resist disclosure until either the consent of the client is obtained or the firm has exhausted available avenues of appeal” with respect to the subpoena. As you know, we previously asked Covington to inquire of its clients whether they consented or objected to Covington providing the requested information. Although the staff did not agree to the particular formulation that Covington intended to use, we understand that Covington did, in fact, reach out to clients to make such a request. However, to date we have not received any update on whether Covington has received such consent from any of its clients, and we would ask that you provide us with an update on that process at your earliest convenience. We want to make clear, however, that even absent such consent, given the application of Rule 1.6(e) by the courts, Covington’s continued objection based on the confidentiality prong of Rule 1.6(a) is unlikely to protect the information from disclosure.

### **III. Covington’s Blanket Privilege Claim is Without Merit, and Any Privileged Items Identified in Response to Request No. 3, Should Be Included on a Privilege Log.**

With respect to Request No. 3(a) of the Subpoena, you also object that the identity of clients impacted by the cyberattack is protected by the work-product doctrine. Specifically, you

claim that Covington prepared a list of impacted clients in anticipation of litigation, and that their identity is therefore protected work product. We disagree with your assertion that the identity of clients impacted by the cyberattack constitutes work product. Initially, documents should only be deemed prepared ‘in anticipation of litigation,’ and thus within the scope of the work product doctrine, if “in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained *because* of the prospect of litigation.” *United States v. Adlman*, 134 F.3d 1194 (2d Cir. 1998)(emphasis in original). Documents are not considered work product if they “would have been created in essentially similar form irrespective of the litigation.” *Id.* In this case, while Covington’s list of impacted clients may have some value in anticipation of potential litigation (although it is unclear to us what that litigation would be), it seems obvious that the firm produced the list with the business intention of reaching out to inform clients that their information had been accessed, as Covington informed the staff it has done.

Moreover, even to the extent the identity of impacted clients could be considered work product, the information would be factual work-product over which the doctrine is not absolute. Rather, the work product privilege can be overcome upon a showing that the party seeking the information: (1) has substantial need for the materials; and (2) cannot, without undue hardship, obtain their substantial equivalent by other means. *See, e.g.*, Fed. R. Civ. P. 26(b)(3)(A). In this case, you indicated that approximately 300 public company clients have had their legal files accessed by a malicious actor, and the Commission is charged with protecting investors from the threat arising from that activity – hence the Commission’s substantial need for the information. In addition, there is literally no other place for the Commission to obtain the relevant information as to which public companies were impacted. That information is uniquely in Covington’s possession as the party whose network was accessed.

With respect to Request No. 3(c), you claim that Covington’s communications with its clients regarding the breach are protected by the attorney-client privilege. In our communications with Covington and with you, we have repeatedly stated that we are not asking for the production of privileged documents, and that we expect any privileged documents responsive to the subpoena would be redacted and/or logged with sufficient information to identify the basis for the privilege. As you know, that is consistent with what the Federal Rules of Civil Procedure would require for any privileged communications.

With respect to Request No. 3(c), your letter describes how Covington initially “contacted those potentially affected clients simply to notify them [that their information had been accessed in the breach] and invited each client to discuss the matter,” following which “most of Covington’s publicly traded clients . . . initiate[d] further substantive discussion.” You then claim that all communications with clients regarding the cyberattack were subject to the attorney-client or work product privilege. Contrary to Covington’s blanket privilege assertion, the application of privilege to any given communication in this context requires a factual analysis of the context for the communication. “The application of the attorney-client privilege is a question of fact, to be determined in the light of the purpose of the privilege and guided by judicial precedents.” *EEOC v. BDO USA, L.L.P.*, 876 F.3d 690, 695 (5th Cir. 2017) (internal quotation marks and citations omitted). Blanket assertions of privilege are generally improper, and instead “[t]he privilege must [generally] be specifically asserted with respect to particular documents.” *Taylor Lohmeyer Law Firm P.L.L.C. v. United States*, 957 F.3d 505, 510 (5th Cir.

2020) (quoting *United States v. El Paso Co.*, 682 F.2d 530, 539 (5th Cir. 1982)) (denying motion to quash IRS John Doe summons seeking identity of law firm clients). At the very least, it seems unlikely that Covington's initial generic communication "simply notifying" impacted clients of the breach and inviting them to discuss the matter would be protected by the privilege. As noted above, if there were subsequent discussions with Covington's clients that contained attorney-client privileged communications, we are not seeking those communications and would expect them to be logged.

#### **IV. Covington's "Burden" Arguments Are Without Merit.**

You also claim that the requested subpoena is unduly burdensome. Contrary to your assertions, the Commission's subpoena is actually extremely limited and seeks information that is already in Covington's unique possession. Furthermore and perhaps more critically, as described in your letter, Covington has already identified – prior to receipt of the Subpoena – the impacted public company clients and the scope of the impact on those clients. As we understand it, the number of impacted public company clients is approximately 300, not nearly the thousands of impacted victims at issue in some other recent cyberattacks. Indeed, Covington has already reached out to the clients on multiple occasions and, according to your letter, had substantive communications with the majority of them regarding the implications of the cyberattack. Your complaint that Covington might have to identify, review and log communications with 300 clients from a finite period of time regarding this singular issue seems a small burden to impose in the interest of protecting investors from unscrupulous traders or companies that fail to disclose a theft of information that could materially impact shareholders' investments.

Your letter also raises a variety of prudential concerns that you claim counsel against requiring the production of the information. Among other things, you claim that the staff should follow the Department of Justice's ("DOJ") approach, which you describe as seeking information from law firms only in the last instance, and not in the first instance. We find this argument unpersuasive. As you know, the Commission and the DOJ operate independently and the Commission has its own rules and investigative guidelines. The fact that DOJ prosecutes criminal offenses counsels for even greater caution around the attorney-client relationship, given the other rights that might be implicated by the provision of such information, such as rights protected under the Fifth Amendment to the U.S. Constitution. In any event, DOJ's guidance does not appear to apply to the situation here – where the firm itself has been a victim of a cyberattack.

The situation here is unique because the Commission is not seeking evidence that came into Covington's possession as part of its representation of the clients – *i.e.*, the information that clients provided to Covington in connection with their representation. Instead, Covington is the sole fact witness to a cyberattack. In that capacity, Covington is uniquely situated to provide the requested information. In other words, the Commission is coming to Covington in the first instance not for some investigative expediency, but because there is no other place to obtain the requested information.

You also assert the Commission should not require such information because it could have a damaging impact on companies' willingness to cooperate with law enforcement in the



future. Your argument attempts to have it both ways. You contend that Covington's desire to cooperate with certain law enforcement agencies on its own terms should somehow militate against requiring it to comply with other law enforcement agencies to which it does not want to provide information. Ultimately, the Commission, DOJ, and Department of Homeland Security all have distinct missions that touch upon cybersecurity events in different ways. Your suggestion that the Commission should stand down from its mission so that firms like Covington will continue to cooperate with other law enforcement agencies would be a disservice to investors and would actually diminish the appropriate and well-balanced law enforcement approach to addressing cyberattacks.

#### **V. To Date, Covington Has Rejected the Staff's Attempts at Compromise.**

Given your position that Covington cannot provide the requested information absent client consent or a court order, there may be limited space for a compromise on this issue short of litigation. At Covington's request, the staff has already made multiple good faith proposals to compromise on the scope of the subpoena. Among other things, we proposed that Covington provide anonymized details regarding the breach in the first instance so that it could determine whether there was a need for additional information. We also proposed that Covington provide only the names of clients whose representation is publicly known, and therefore not a secret. With respect to communications, we proposed that Covington initially produce only a template of the initial letter communicating the fact of the breach to clients, as opposed to individual communications to each client. In each of these instances, Covington rebuffed the staff's proposed attempts to compromise and appears to be instead taking an "all-or-nothing" approach to production of the information sought by Request No. 3.

Nevertheless, the staff remains open to a compromise that would provide the information that the staff needs to conduct its investigation. In order to try to avoid a litigated outcome to this dispute, we propose that Covington produce: (1) all requested information to which Covington's clients consent to production; (2) the names of the impacted public company clients, as defined in footnote 1 above; (3) a description of the scope of the impact on those clients; and (4) the initial letter sent to the impacted clients to "simply notify them" of the attack, without providing a log of other client communications. Such a compromise would provide the key information that the staff needs to move forward with its investigation, while making it easier for Covington to respond to Request No. 3(c) of the subpoena, and should alleviate the concerns that you've raised with respect to potentially privileged communications under Request No. 3(c). Please respond to our proposed resolution no later than Friday, July 29, 2022. In the event we are unable to reach a mutually agreeable resolution by that time, we are prepared to move forward with an action to enforce the subpoena.

Mr. Boutrous, Jr., Esq.  
July 14, 2022  
Page 8

Please let us know if you have any questions or if you wish to discuss this matter in more detail.

Sincerely,

A handwritten signature in blue ink, appearing to read "W. Bradley Ney", is written over a horizontal line.

W. Bradley Ney, Esq.  
Senior Counsel  
Division of Enforcement

Cc: Kevin S. Rosen, Esq.  
Richard W. Grime, Esq.  
Lory Stone, Senior Counsel, Division of Enforcement  
Fred Block, Supervisory Trial Counsel, Division of Enforcement  
Melissa Hodgman, Associate Director, Division of Enforcement  
Carolyn Welshhans, Associate Director, Division of Enforcement