IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SECURITIES AND EXCHANGE COMMISSION, **Applicant,** **v.** **COVINGTON & BURLING LLP,** **Respondent.**	**Case No. 23-mc-00002 (APM)**

AMICUS CURIAE BRIEF OF THE CHAMBER OF COMMERCE OF THE UNITED STATES IN SUPPORT OF THE RESPONDENT

February 21, 2023

Megan L. Brown
Kevin Muhlendorf
Boyd Garriott
Tyler Bridegan
WILEY REIN LLP
2050 M Street NW
Washington, D.C. 20036
Telephone: (202) 719-7000
Facsimile: (202) 719-7049
mbrown@wiley.law
kmuhlendorf@wiley.law
bgarriott@wiley.law
tbridegan@wiley.law

Counsel for Amicus Curiae Chamber of Commerce of the United States of America

LCVR 7(O)(5) & FRAP 29(A)(4)(E) STATEMENT

Pursuant to LCvR 7(o)(5), *amicus curiae* Chamber of Commerce of the United States of America hereby certifies that it is a not-for-profit corporation. It has no parent corporation, and no publicly held corporation owns 10% or more of its stock.

Counsel for amicus curiae certify that no counsel for a party authored any part of this brief. No entity or person, other than amicus curiae, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of this brief.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Regulations

Agency Materials

Other Authorities

INTEREST OF AMICUS CURIAE

The Chamber of Commerce of the United States of America ("Chamber") is the world's largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files amicus curiae briefs in cases, like this one, that raise issues of concern to the nation's business community.

The Chamber has identified this action as particularly troubling. The Chamber's members are regular targets of cybersecurity threats, and the Chamber has been involved in every major legislative and regulatory proceeding on cybersecurity risk management for more than a decade, building partnerships through its Cybersecurity Leadership Council and other efforts. Many of the Chamber's members are subject to the direct oversight of, or investigation by, the Securities and Exchange Commission ("SEC" or "Commission").

The Chamber submits this brief to apprise the Court of the damage the SEC's subpoena, if enforced, would have on the business community, which has been pioneering key partnerships with federal agencies that the SEC's Subpoena now threatens, and on the nation's cybersecurity priorities, given the chilling effect the SEC's actions will have on federal cybersecurity policy.

INTRODUCTION

Every day, an American business faces a cyberattack. The Securities and Exchange Commission ("SEC" or "Commission"), using unnecessarily aggressive and unprecedented tactics, is re-victimizing those businesses, and enforcement of the SEC's underlying subpoena ("Subpoena") would impose an unlawful and unreasonable burden. Indeed, the Subpoena represents a twisted irony. After the Hafnium[1] attackers—criminals with ties to hostile nation states—were able to rifle through Covington & Burling's ("Covington") systems and client files, the SEC now seeks to do the same. If allowed, the SEC's blatant fishing expedition will distort incentives for collaborative responses to cyberattacks.

The SEC has not shown a need for this information. The SEC has a panoply of tools it can rely on to investigate whether there has been problematic activity, and need not resort to the Subpoena. Of note, the SEC holds itself out as an expert in data analysis, has touted its ability to investigate without the need to identify specific issuers, and has access to high-powered, less intrusive investigatory tools. Access to Covington's files might make the SEC's job marginally easier, but that does not justify the damage that will be caused by enforcing this Subpoena. Not only is this a fishing expedition, but the SEC is fishing in restricted waters without a valid license.

[1] According to the SEC's Application, it "is investigating potential violations of the federal securities laws arising out of the Microsoft Hafnium cyberattack (the 'Cyberattack'), which began in or around November 2020 and continued into at least March 2021. Specifically, the Commission is investigating the impact of the Cyberattack on public companies and regulated entities in order to (a) understand the nature and scope of the attack, (b) assess and identify potential illegal trading based on information gathered during the attack, and (c) determine relevant disclosure obligations for public companies impacted by the attack." SEC Appl. for Order to Show Cause, Dkt. 1, ¶ 2 ("Application"). "As part of the Cyberattack, threat actors gained unauthorized access to Covington's computer network and certain individual devices, and accessed legal files for approximately 300 of its clients." *Id.* ¶ 3.

Enforcement of the Subpoena would undermine the confidential trust relationship between attorneys and clients, without any clear benefit to the SEC given the host of analytical tools designed to aid the SEC in protecting markets. The SEC's invasive approach instead threatens to chill relationships businesses have with their trusted partners. The SEC's course of action injects tremendous uncertainty into the lawyer-client relationship, including aspects of confidentiality and privilege.

Lastly, the SEC's approach flouts norms of cybersecurity policy, chills voluntary cooperation on cyber incidents, and fragments federal cybersecurity regulation. Specifically, cybersecurity policy—and the agencies that traditionally set cybersecurity policy—have historically protected victims, respected privilege, and limited the downstream uses of information shared with the government. The Federal Bureau of Investigation ("FBI") has long sought to encourage businesses that fall victim to cyberattacks, to cooperate with law enforcement to investigate such attacks. Such communications are essential and are only possible when businesses know that the communications will remain confidential. These priorities appear in myriad settings and have been championed by Congress, the Department of Homeland Security ("DHS"), and the FBI. This Court should not allow the SEC to act as an agent of cybersecurity chaos.

For these reasons, the Court should hold that the SEC has not met its burden to show that its Subpoena is reasonable or warrants overriding the extraordinary burden imposed on a victim of a cyberattack. To the contrary, this Subpoena will undermine the attorney-client privilege, flout norms of cybersecurity policy, chill voluntary cooperation on cyber incidents, and fragment federal cybersecurity regulation.

ARGUMENT

I. THE SEC DOES NOT NEED THIS SUBPOENA TO VINDICATE ITS CLAIMED INTERESTS IN LIGHT OF ITS DATA ANALYTIC TOOLS AND EFFECTIVE INVESTIGATIVE METHODS.

The SEC cites two types of potential securities violations for which it claims it *must* have the client information from Covington – potential illicit trading utilizing material non-public information (insider trading) about Covington's clients, and potential disclosure violations by Covington's public company clients themselves.

The SEC has ample tools at its disposal to fulfill its mission. It should not conscript hacking victims, whether law firms or other trusted third parties, like security firms, to ease its work. Specifically, as to insider trading, the Commission admits that it "has proprietary tools to survey the market for potential illicit trading in the stock of all publicly traded companies." Mem. P. & A., Dkt. 1-1at 10−11. In the SEC's own words, the roster would merely help it narrow its investigation by allowing it to conduct a "targeted analysis" and "increas[e] the likelihood that the Commission would identify any potential illegal trading." *Id.* at 11. Put simply, the SEC concedes that the roster is not necessary.

The Commission's public statements touting its data analysis capabilities confirm that the Victim-Client roster is not needed to investigate insider trading. As explained in a litigation release cited by the SEC,[2] the agency's "use of innovative analytical tools to find suspicious trading patterns and expose misconduct demonstrates that *no trading scheme is beyond our ability to unwind*." Press Release, SEC Charges 32 Defendants in Scheme to Trade on Hacked News Releases (Aug. 11, 2015) https://www.sec.gov/news/press-release/2015-163 (emphasis added). This statement is one of many. Similar claims litter SEC litigation releases from the last

[2] *See* Mem. P. & A., Dkt. 1-1 at 3 n.1.

decade. The Division of Enforcement has boasted about its ability to use technology to bring "significant trading-related cases that may not have been possible without our ability to analyze voluminous amounts of data, including trading data and communications metadata." SEC Division of Enforcement 2019 Annual Report at 13 (Nov. 6, 2019), https://www.sec.gov/enforcement-annual-report-2019.pdf. The SEC has highlighted the staff's ability to perform "analysis of numerous events," use "complex analytic tools," and complete "statistical analyses" to investigate and prosecute insider trading. *Id.*

The SEC's request for the Victim-Client roster is also inconsistent with its "trader-based" approach to insider trading, under which the SEC "looks for traders who collectively exhibit unusual trading patterns across different securities, and then tries to find common sources of information or relationship[s] that link them together." Michael A. Perino, *Real Insider Trading*, 77 Wash. & Lee L. Rev. 1647, 1702–03 (2020) (citing Todd Ehret, *SEC's Advanced Data Analytics Helps Detect Even the Smallest Illicit Market Activity*, Reuters (June 30, 2017) https://perma.cc/PB99-QXQD). SEC leadership has touted "new technological tools and investigative approaches that allow [the SEC] not only to pinpoint suspicious trading across multiple securities but also to identify relationships among traders." Mary Jo White, Chair, SEC, Remarks at a Press Conference Announcing Enforcement Charges Involving an International Hacking Trading Scheme (Aug. 11, 2015), https://www.sec.gov/news/statement/press-conference-remarks-massive-hacking-trading-scheme. Thus, given the starting point for SEC investigations can be the trader, not the security issuer, access to Covington's client list is not necessary.

Instead of demanding the Victim-Client information, the SEC could check its trading database (ARTEMIS) for anomalous trading in the relevant time period and have made inquiries

with any identified issuers. *See* Michael S. Piwowar, Commissioner, SEC, Remarks at the 2018 RegTech Data Summit - Old Fields, New Corn: Innovation in Technology and Law (Mar. 7, 2018), https://www.sec.gov/news/speech/piwowar-old-fields-new-corn-innovation-technology-law ("[ARTEMIS] is just one of many advanced technologies, both internally developed and in partnerships with the private sector, that we are deploying in our efforts to root out fraud in the securities markets and protect investors."). The SEC also could review FINCEN Suspicious Activity Reports for anomalous activity following the Hafnium attack and seek information about account owners and associated trades. The SEC also could obtain the hacker's IP addresses from the FBI, with whom Covington cooperated, and query regulated broker-dealers to see if trades were made from those IP addresses. *See, e.g.*, Complaint, *SEC v. Kliushin*, 1:21-cv-12088 (D. Mass. Dec. 20, 2021), https://www.sec.gov/litigation/complaints/2021/comp-pr2021-265.pdf; SEC Enforcement Division 2019 Annual Report at 13 (referencing Complaint, *SEC v. Ieremenko*, 19-cv-00505 (D. N.J. Jan. 15, 2019), https://www.sec.gov/litigation/ https://www.sec.gov/litigation/complaints/2019/comp-pr2019-1.pdf) ("Staff also analyzed IP addresses that accessed various communications and other systems to help establish the connections among seemingly unrelated participants in the alleged scheme.").

The Commission's desire to investigate disclosure violations is a similarly unpersuasive reason to revictimize Covington and its clients or undermine their relationship of trust and confidence. Instead of having any articulable (or articulated) reason to believe there was a disclosure failure related to the breach, the SEC wants to instead force Covington to reveal its affected clients to the SEC to give the Commission staff a "head start" in investigating those very same clients. But making the Commission's job marginally easier on no more than an imagined

violation cannot possibly overcome the burden on Covington and its clients, given the ample other tools the Commission has to investigate.

The SEC has an entire group in the Enforcement Division devoted to uncovering disclosure violations – the Financial Reporting and Audit (FRAud) Group – without resort to confidential information. *See* SEC, *Spotlight on Financial Reporting and Audit (FRAud) Group* (Feb. 10, 2020), https://www.sec.gov/spotlight/financial-reporting-and-audit-task-force. The FRAud Group utilizes "ongoing review of financial statements and revisions, an analysis of performance trends by industry, and the use of technology-based tools." *Id.* The FRAud group specifically welcomes "corporate insiders" to submit tips to help it uncover "issuer reporting and disclosure" violations. *Id.* To that end, the SEC's Office of the Whistleblower reported that for FY 2022, it received 1,554 tips related to "Corporate Disclosures and Financials."[3] SEC, *SEC Whistleblower Office Announces Results for FY 2022* at 5–6 (Nov. 15, 2022), https://www.sec.gov/files/2022_ow_ar.pdf. The Covington client list is simply not necessary for the SEC to do its job – which it has done for years without threatening to weaponize trusted business service providers.

At bottom, the SEC's attempts to justify this extreme intrusion into the relationship of trust between attorneys and their clients fails under the weight of the Commission's own bravado about its investigative skills for both insider trading and disclosure violations.

II. JUDICIAL ENDORSEMENT OF THE SEC'S TACTICS BY ENFORCING THE SUBPOENA WILL UNDERMINE RELIANCE ON COUNSEL AND THE ATTORNEY-CLIENT RELATIONSHIP, AND BURDEN U.S. BUSINESS.

Subpoena Request No. 3 ("Request 3"), at the heart of this matter and the sole outstanding request, is of substantial concern to the United States business community. Request

[3] The SEC also reported 396 insider trading tips in FY 2022.

3 would compel the production of 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" including Victim-Client names. *See* W. Bradley Ney's Decl., Dkt. 1-2, Ex. A at 17 of 66.

This assault on the attorney-client relationship and confidential communications is unduly burdensome and therefore is not justified. Dragging law firms into investigations will inject significant uncertainty into the attorney-client relationship, and "[a]n uncertain privilege," of course, "is little better than no privilege at all." *Upjohn Co. v. United States*, 449 U.S. 383, 393 (1981). Indeed, businesses will be less likely to seek legal counsel in the wake of a cyberattack for fear that doing so will leave them *more* exposed because the SEC can seek information from their counsel. Compounding this predicament, companies whose law firms or other trusted third parties are weaponized by the SEC may need separate counsel to evaluate and manage the consequences of such weaponization. Chilling businesses in the throes of a cyber crisis from seeking the help they need will fundamentally weaken the business community's cyber resilience.

U.S. businesses of all sizes rely on the attorney-client relationship and privilege, which is foundational to the practice of law and administration of justice. *Upjohn*, 449 U.S. at 389–90 (citing 8 J. Wigmore, Evidence § 2290 (McNaughton rev. ed. 1961)). The attorney-client privilege developed at common law to encourage "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice." *Id.* at 389. It promotes candor between lawyer and client. Candor, in turn, ensures informed, effective representation. *See Hunt v. Blackburn*, 128 U.S. 464, 470 (1888).

Victims of cyberattacks, including Chamber members, work with counsel in many ways that may be jeopardized by the SEC tactics at issue here. Companies often rely on legal counsel (and other trusted third parties) to address their exposure and proper response in a cyber incident and more generally as trusted counselors. DHS's Cybersecurity and Infrastructure Security Agency ("CISA") has recognized that "outside counsel . . . wield significant influence as company advisors on cybersecurity." CISA, *Resources for Lawyers*, https://www.cisa.gov/resources-lawyers. Given the complex regulatory and litigation risks associated with corporate security programs, government and third-party audits, and incident management, companies prudently work with trusted counsel. In a cyber incident, lawyers advise on the incident itself, contractual and customer reporting, regulatory obligations (including under securities laws), cooperation with government agencies (like the FBI and DHS), litigation and liability risk, and myriad compliance considerations. The SEC's justifications for its approach here would reach law firms and other trusted outside counsel.

The stakes of this Subpoena are high for all businesses. If the SEC can force outside lawyers and other trusted third parties to disclose information about clients that are cybercrime victims, with no articulable suspicion of a securities law violation, it grievously jeopardizes the privilege and distorts incentives.

Victims may be less willing to seek counsel, may rely more on in-house lawyers, and may be more guarded in seeking legal advice.

> The mere fact that [an] attorney has been subpoenaed, even if the subpoena is ultimately quashed, may encourage that client, or others, to hold back critical information for fear that a future subpoena might be enforced. . . . In short, the mere issuance of subpoenas to attorneys inevitably has a chilling effect on the attorney-client relationship.

David S. Rudolph & Thomas K. Maher, *The Attorney Subpoena: You Are Hereby Commanded to Betray Your Client*, 1 Crim. Just. 15, 16 (1986). Self-censorship by clients guts the privilege.

"The lawyer-client privilege rests on the need for the advocate and counselor to know all that relates to the client's reasons for seeking representation if the professional mission is to be carried out." *Trammel v. United States*, 445 U.S. 40, 51 (1980).

The threat posed to the role of counsel as trusted advisors is particularly acute here, where the Victim-Clients experienced a breach of their confidential information due to a criminal attack on their trusted counsel, Covington. The SEC has publicized this breach and its effects, increasing risk to Covington and its clients of follow-on cyberattacks, as is frequently observed when malicious actors take advantage of victims.[4] And it effectively seeks to turn Covington, the initial victim of Hafnium, into a witness against its clients who were also victimized by Hafnium.

The SEC is also placing Covington in the potential chain of prosecution of its clients. In order to bring a civil enforcement action against a Covington client for failing to disclose a material fact about the breach, the SEC would have to demonstrate that the client failed to disclose material information about the impacts of the Hafnium attack on it—which the client could only know from a communication with Covington. Indeed, such communication from Covington may have been blended with legal advice on the need for disclosure under SEC guidance and rules and other legal duties arising from the data breach, making this inquiry especially perilous. Because a willful violation of federal securities laws can be a criminal violation, requiring Covington to disclose affected clients could place its communications at the center of both a potential civil *and* criminal matter against the client. *See* 15 U.S.C. § 78ff(a) (criminalizing conduct). Even if those communications ultimately remain privileged and

[4] *See e.g.*, Alexander Applegate, *Repeat Offenders Target Prior Ransomware Insurance Victims for Fun and Profit*, ZeroFox (July 9, 2021), https://www.zerofox.com/blog/ransomware-insurance-victims/ ("repeat attacks against victims definitely appear to be on the rise").

undisclosed, the SEC's intrusive tactics targeting lawyers create tremendous uncertainty about the durability of the privilege undermining confidential relationships and making Victim-Clients likely to need additional counsel to advise on their relationship with their lawyers and how to protect their interests. "An uncertain privilege . . . is little better than no privilege at all." *Upjohn*, 449 U.S. at 393.

The SEC's approach is particularly puzzling given the traditional sensitive respect for attorney-client relationships by federal agencies—including the SEC. The SEC Enforcement Manual provides, "[a]s a matter of public policy, the SEC wants to encourage individuals, corporate officers and employees to consult counsel about the requirements and potential violations of the securities laws." SEC Enforcement Manual at 75–76 (Nov. 17, 2018), https://www.sec.gov/divisions/enforce/enforcementmanual.pdf. For its part, the Department of Justice ("DOJ") will only subpoena attorneys upon special senior approval and as a last resort, recognizing "the potential effects upon an attorney-client relationship that may result from the issuance of a subpoena to an attorney for information relating to the attorney's representation of a client." *See* U.S. Dep't of Just., Just. Manual § 9-13.410(A) (2018). As underscored by the DOJ's policy, interfering with the attorney-client relationship should not be approached lightly; it certainly should not be encroached on using an overbroad Subpoena where the information sought could be derived using other tools. By pursuing such an overreaching Subpoena, the SEC unduly burdens the attorney-client relationship.

III. THE SEC'S SHIFTING APPROACH TO CYBERSECURITY-RELATED INVESTIGATIONS UNDERMINES FEDERAL CYBERSECURITY POLICY, THREATENS TO CHILL COLLABORATION, AND RISKS FRAGMENTATION OF CYBERSECURITY REPORTING AND OVERSIGHT.

The SEC's approach undermines federal cybersecurity policy in several ways, confirming the heavy burden the agency faces to justify its tactics. The SEC's public, punitive approach is

incongruous with policy choices by Congress and other agencies to protect victims. The SEC's approach may discourage voluntary collaboration with the FBI. And the SEC's subpoena enforcement action will fragment the complex cybersecurity regulatory landscape, which Congress has been actively working to harmonize. The Court should consider all of these consequences as it evaluates the burden imposed by the SEC's Subpoena.

A. Information sharing and reporting regimes consistently prioritize victim confidentiality, protect attorney-client privilege, and restrict regulatory and enforcement use of shared information.

The SEC's approach appears to ignore bedrock elements of federal cybersecurity policy, which protect victims, respect privilege, and limit the downstream uses of information shared with the government. These priorities appear in myriad settings and have been championed by Congress, DHS, and the FBI. DHS has been leading the charge for incident reporting to enhance the government's ability to anticipate and respond to attacks and to help victims. Congress and the President have provided DHS authority and direction to manage information sharing and encourage voluntary cyber incident reporting. This work, like the FBI's work with companies that experience an attack, protects victims and the security of information shared with the government. Even as voluntary incident reporting will be augmented by forthcoming mandates regarding critical infrastructure under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), protecting victims remains a touchstone. Unsurprisingly, when the SEC proposed onerous public disclosure rules relating to material cybersecurity incidents,[5] the agency heard an outcry that the rapid public disclosure of cyber incidents was out of step with decades of work to protect victims.

[5] *See* SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22 (Mar. 9, 2022).

A bit of history puts this concern in context. In 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which called for "a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing . . . ." In 2015, Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing*, sought to further promote voluntary information sharing between the private sector and the government, emphasizing that "[s]uch information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, ***that preserves business confidentiality***, ***that safeguards the information being shared***, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats . . . ." (emphasis added).

Congress enacted the landmark Cybersecurity Information Sharing Act of 2015 ("CISA 2015") to enhance cooperation by creating new authorities for private companies to voluntarily share cybersecurity threat indicators and other information with DHS and by marrying those authorities with clear protection of information for the shared information from public disclosure under FOIA or state law. 6 U.S.C. § 1504(d)(2)-(3). Notably, Congress in CISA 2015 protected the attorney-client privilege from risk of waiver by sharing information. S*ee id.* § 1504(d)(1). Congress also prohibited the government from using shared information for regulatory purposes, including enforcement actions. *Id.* § 1504(d)(5)(D)(i). These protections were vital to establish the trust needed for meaningful cooperation.

In the intervening years, those protections fostered increasing trust among companies, industries, information sharing and analysis centers (ISACs), information sharing and analysis organizations (ISAOs) and government, principally DHS and the FBI. The Chamber and its members have led many efforts, working collaboratively on threats, best practices, and incident

response, including events like the Colonial Pipeline incident and Log4J vulnerability, as well partnering with government on increased cyber risk from the Russian invasion of Ukraine.

In 2022, Congress addressed incident reporting, reiterating the importance of protecting victims. CIRCIA directed DHS to create new reporting mandates for certain incidents affecting critical infrastructure. Key elements of CIRCIA and the rules to be developed by DHS will be confidential treatment of information, protection from public disclosure, a prohibition on the use of "information about a covered cyber incident or ransom payment . . . to regulate, including through an enforcement action" the activities of the reporting entity, and a clear preservation of attorney-client privilege. *See* 6 U.S.C. § 681e(a)(5)(A).

Other agencies maintain reporting regimes that emphasize confidentiality and limitations on use. For example, the Transportation Security Administration ("TSA") now requires reporting by pipeline and rail operators to CISA and TSA of certain cybersecurity incidents on a confidential basis. *See, e.g.*, TSA, Security Directive 1580-21-01, Enhancing Rail Cybersecurity (Dec. 31, 2021), https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf. The Department of Defense ("DoD") requires reporting under the Defense Federal Acquisition Regulation Supplement Section 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, on a confidential basis. 48 C.F.R. § 232.204-7012. DoD may share information with law enforcement but "voluntary reporting can only be shared with law enforcement with consent from the Partner." Defense Industrial Base (DIB) Cybersecurity Portal, *Frequently Asked Questions*, https://dibnet-fls.boozallencsn.com/dibnet/#faq. These are just a few examples of how agencies protect information shared with the government, particularly in circumstances like those here, where a victim does the right thing to proactively work with the FBI.

Confidentiality protects victims of cyberattacks. Absent protections, victims become attractive targets for revictimization by the same or copycat malicious actors; companies and their customers, once publicly identified, are highlighted for exploitation as bad actors are on notice that individuals or businesses are at risk and look to exploit vulnerabilities. Ongoing law enforcement investigations may be compromised, and victims' internal investigations and remedial measures may be disrupted. Finally, incomplete or inaccurate information may be prematurely distributed to the public or third parties. The Chamber explained these and other risks in comments on the SEC's proposed public disclosure rule, which would undermine federal policy and incentives to voluntarily work with the government. *See, e.g.*, Letter from U.S. Chamber of Commerce to Vanessa A. Countryman, Secretary, SEC, Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (File Number S7-09-22) at 2–3, 5, 8–9, 16 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128398-291304.pdf (discussing risks).

B. The SEC ignores these critical norms by seeking the confidential client list and publicly shaming Covington, the victim of a cyberattack.

Several aspects of the SEC's approach flout norms established by Congress and other agencies in dealing with cyber incident reporting by victims. As an initial matter, the Court cannot overlook that the SEC initially requested information about the clients' files that may have been illegally accessed by the cybercriminal, as well as the firm's communications with clients about that access. American businesses are deeply troubled by the notion that the SEC ever thought it reasonable to try to obtain investigative information through third parties, especially outside counsel, in this manner. Remarkably, the agency initially even sought attorney-client communications and other confidential information, only limiting its demands

after Covington fought back. Although the agency has since backed away from those invasive demands, its tactics continue to be abusive.

The SEC's use of a public subpoena enforcement action appears to be an attempt to punish Covington by exposing the extent of the breach, and by creating an *in terrorem* effect on Covington's clients, other law firms, or companies with access to confidential client data, and the entire private sector that relies on legal counsel for advice about cyber risk management and incidents. Tellingly, the SEC's filing could have been done under seal. Instead, the agency chose to target Covington and its clients publicly, sending a signal to the entire business community. *See* LCvR 5.1(h) (outlining rules for filing sealed documents). Exacerbating this harm, the SEC made public Covington's white paper, which contained sensitive details about the breach, despite Covington asking for confidential treatment under FOIA, as expressly permitted by the SEC's rules. *See* Application Ex. B, Dkt. 1-2, at 1, 20–21; 17 C.F.R. § 200.83 (providing rules for requesting confidential treatment); SEC, *Securities and Exchange Commission Confidential Treatment Procedure Under Rule 83*, https://www.sec.gov/foia/conftreat (describing requirements of Rule 83). Recent cyber legislation described above makes clear the importance to Congress of protecting sensitive information from public release.

The SEC's tactics are unnecessarily punitive to Covington, and fundamentally at odds with the goal and tenor of federal cyber policy which is to protect victims and encourage voluntary cooperation. The SEC's tactics are damaging to cybersecurity best practices and fundamentally at odds with the consensus approach, in which the government avoids revictimizing the victims of cyberattacks. Covington and its clients were the victims of a cyberattack, and Covington is limited (by prudence and legal ethics) in what it can say to defend itself without worsening reputational damage wrought by the SEC's approach.

The SEC's attempt to use Covington to identify third parties to be targeted for further investigation opens the door to future and broader abuses and threatens to chill consultation with external expertise when it is most needed. What would stop the SEC from using its subpoena power to troll through the confidential business records of cyber incident response companies, third party auditors, ISPs, and potentially any other professional service provider just on the mere chance that they might find some reason to investigate one of their clients? Any company reaching out for external expertise, whether they be a victim of a cyberattack needing incident response services or merely one in need of advice on a complex business transaction is rightly uneasy about the SEC's tactics in this case and would need to strongly consider using service providers beyond the reach of the SEC. This cannot be a mistake by the SEC, and this Court should reject its heavy-handed attempt to strike unease into the private sector's use of external expertise.

C. The SEC's tactics sow doubt in the promise of confidential treatment of reported cybersecurity incidents by the FBI and other agencies.

The FBI is tasked with responding to and investigating cyberattacks and, in partnership with the private sector, has had notable successes in pursuing criminal actors and illicit funds. Unfortunately, this Subpoena threatens years of work by the FBI and the private sector to cultivate trust in the business community. The FBI frequently makes public pleas for victims to report cyberattacks and recognizes that voluntary cooperation is vital to the government's interests.[6] While the FBI has repeatedly assured the business community that it will protect

[6] Christopher Wray, Director, FBI, Partnering with the Private Sector to Counter the Cyber Threat (Mar. 22, 2022), https://www.fbi.gov/news/speeches/fbi-partnering-with-private-sector-to-counter-the-cyber-threat-032222 ("But we also need what the private sector sees to protect companies, schools, universities, of all kinds. 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 to stop the next attack, whether that's another against you or a new attack on one of

victims in order to encourage prompt voluntary cooperation, the Subpoena appears to be a clear attempt by the SEC to weaponize information voluntarily reported to the government. This chills not only other law firms, but the entire business community that is called on by the FBI and DHS to increase voluntary cooperation. If the SEC is permitted to enforce this Subpoena, businesses will rethink their cooperation with the federal government out of fear that cooperation will be used against them.

There are substantial benefits to voluntary reporting. The FBI Director has asked companies to "please report the compromise by contacting your local field office immediately—the more quickly we get involved, the more we can do to help."[7] The government has told companies that "[w]hen you engage with the FBI, we can leverage our capabilities and expertise to mitigate damage done by malicious cyber actors, or even to prevent malicious activity from occurring at all. . . . [and] you are working to help prevent these bad actors from victimizing others, and potentially from re-victimizing you."[8] The FBI Director has committed to treating hacked companies as victims, noting that "[w]e don't view it as our responsibility when

---

your partners. We like to say that the best way to protect one business is to hear from others, and the best way to protect others is to hear from that one."); *see* Christopher Wray, Director, FBI, Digital Transformation: Using Innovation to Combat the Cyber Threat (Mar. 7, 2018), https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat ("At the FBI, we treat victim companies as victims.").

[7] Christopher Wray, Director, FBI, Director's Remarks to the Boston Conference on Cyber Security 2022 (June 1, 2022), https://www.fbi.gov/news/speeches/directors-remarks-to-boston-conference-on-cyber-security-2022.

[8] Joe Bonavolonta, Special Agent in Charge, FBI, Remarks Prepared for Delivery at 6th Annual Boston Conference on Cyber Security (June 1, 2022), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/remarks-prepared-for-delivery-by-fbi-boston-division-special-agent-in-charge-joe-bonavolonta-at-6th-annual-boston-conference-on-cyber-security.

companies share information with us to turn around and share that information with some of th[e] other [regulatory] agencies."[9]

The FBI works discreetly with reporting entities and protects their identities in judicial processes to go after bad actors. *See, e.g.*, Press Release, FBI, Partners Disarm Emotet Malware: Global law enforcement and private sector take down a major cyber crime tool (Feb. 1, 2021) https://www.fbi.gov/news/stories/emotet-malware-disrupted-020121 (emphasizing the importance of protecting victim identities); Press Release, DOJ, U.S. Department of Justice Disrupts Hive Ransomware Variant (Jan. 26, 2023) https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant (withholding victim identities). These measures by the FBI confirm the importance of protecting victims. The FBI gains invaluable information about criminals' tactics and operations from victim reporting, and so the agency takes pains, even when seeking judicial orders, to avoid identifying victims. *See, e.g.*, Aff. of FBI Special Agent Tim Callanan, ¶¶ 11–13, Case No. 2:23-mj-00281 (C.D. Cal. Jan 23, 2023), https://www.justice.gov/opa/press-release/file/1564286/download (describing, among others, "a hospital located in the Midwestern United States," "a technology company in New Jersey," and "a heavy machinery company in central Florida," but not identifying victims).

It is not clear how the SEC learned of the Hafnium attack on Covington or any impacts on Victim-Clients. However, any possible use by the SEC of information provided to the FBI to pursue additional information about third-party victims would be troubling. At a minimum, the SEC's hypothetical use of information voluntarily provided to the FBI risks chilling future

[9] Alison Noon, *FBI Director Vows To Treat Hacked Companies as 'Victims'*, Law360 (Mar. 7, 2018), https://www.law360.com/articles/1019414. *See also* Nate Raymond, *FBI chief: Corporate hack victims can trust we won't share info*, Reuters (Mar. 7, 2018) https://www.reuters.com/article/us-usa-fbi-wray/fbi-chief-corporate-hack-victims-can-trust-we-wont-share-info-idUSKCN1GJ2QS.

interactions by victims—law firms or other trusted third parties—with the FBI and other agencies that want and benefit from receiving early, voluntary cooperation.

As part of its law-enforcement mission, the FBI works with the SEC to investigate potential securities law violations. But enforcement of the Subpoena here may breed suspicion that the close working relationship can be exploited to enable regulatory access to information that businesses have been assured would be confidential. Such a result would harm the country's cybersecurity goals. Both the FBI and SEC have highlighted how closely they work – publicizing the FBI-SEC "embed program." In 2017, the SEC noted that:

> The Division [of Enforcement] also collaborates with the Federal Bureau of Investigation (FBI) on individual matters and through a Memorandum of Understanding to embed several Agents and Intelligence Analysts from the FBI's Economic Crimes Unit into the Division's Office of Market Intelligence (OMI) for the purpose of information sharing and combatting securities fraud by leveraging each other's resources and expertise.

SEC, Major Management Priorities, Challenges and Risks, at 129 (2017) https://www.sec.gov/about/reports/sec-fy2017-other-information.pdf. An FBI Director noted:

> [T]he FBI recognizes the need for increased cooperation with our regulatory counterparts. Currently, we have embedded agents and analysts at the Securities and Exchange Commission . . . , which allows the FBI to work hand in hand with U.S. regulators to mitigate the corporate and securities fraud threat. Furthermore, these relationships enable the FBI to identify fraud trends more quickly, and to work with our operational and intelligence counterparts in the field to begin criminal investigations when deemed appropriate.

James B. Comey, Director, FBI, Oversight of the FBI (May 21, 2014), https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-5.

That close relationship has previously raised concern about possible inappropriate sharing of information between the two agencies. As one commentator who analyzed information sharing arrangements after interviewing FBI and SEC sources wrote, "the[se] [embed] programs

raise due process questions that have not yet been addressed." Anthony O'Rourke, *Parallel Enforcement and Agency Interdependence*, 77 Md. L. Rev. 985, 992 (2018). The program also

> [G]ive[s] civil regulators access to FBI information that they are formally unable to possess under rules governing sensitive criminal evidence. As a former senior officer at the SEC explained, one of the agency's goals in designing the embedded agent program was to ensure that, in certain circumstances and through the FBI embeds, the SEC can access information from the FBI databases. This access appears to be circumscribed by "law enforcement protocols prohibiting prosecutors and the FBI from sharing investigative materials, such as wiretapped conversations, with securities regulators," . . . [yet] enforcement staff appear to be able to review materials that remain under the formal custodial control of the FBI embedded agents.

Id. at 1058.[10]

Declining to enforce the Subpoena will help protect the voluntary reporting paradigm the FBI has worked hard to create by reinforcing confidentiality and making the SEC meet its burden to justify its actions. It will bolster the view that voluntarily providing cyberbreach information to the FBI will not subject a victim to investigation by other government agencies and will help assuage concerns that the SEC is bending the rules to use those same protected materials.

D. The SEC's approach will undermine and fragment federal cybersecurity policy.

Fragmentation is anathema to current federal cybersecurity policy because it siloes information, creates inconsistent and duplicative requirements, and burdens both government and the private sector. The imperative to harmonize is reflected in the recent creation by Congress of the Office of the National Cyber Director to "[e]nsur[e] federal coherence,"[11] and in CIRCIA's

[10] The embed program also allows civil regulators to review FBI 302s (reports of interviews) "while [still] truthfully asserting that the documents have not left the custody of criminal investigators" and are therefore not subject to civil discovery demands – denying defendants in SEC enforcement actions access to those materials. *Id*. at 1059–1060.

[11] The White House, *Office of the National Cyber Director*, https://www.whitehouse.gov/oncd/.

new Cyber Incident Reporting Council. Congress, through CIRCIA, directed DHS to lead "an intergovernmental Cyber Incident Reporting Council, in consultation with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, Sector Risk Management Agencies, and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations." 6 U.S.C. § 681f(a). Another federal group, the Cybersecurity Forum of Independent and Executive Branch Regulators, has a similar mission. Its leader remarked, "[r]ight now, there's a lot of fragmentation across sectors and jurisdictions in what information gets reported, when and how it is reported, and how that information can be used." Jessica Rosenworcel, Chairwoman, FCC, Remarks To The Cybersecurity Forum Of Independent And Executive Branch Regulators (Apr. 8, 2022), https://docs.fcc.gov/public/attachments/DOC-382215A1.pdf.

By unnecessarily attempting to insert itself as a regulator overseeing private companies' cybersecurity incidents, the SEC flies in the face of the government's goal of harmonization. This will further strain private companies' resources, overlap with expert agencies' work, and impose all the aforementioned risks and inconsistencies in treatment. These fragmentation concerns are not limited to this SEC investigation but are raised by the SEC's other overly aggressive moves into cybersecurity regulation. One of the authors of CIRCIA, Senator Rob Portman, took the SEC to task about its proposed public disclosure rule because, among other things, it was out of step with Congressional and Executive Branch policy by demanding public disclosure, duplicating other cyber regulatory efforts, and failing to protect confidentiality. *See* Letter from Sen. Rob Portman, Ranking Member, Comm. on Homeland Sec., to Vanessa Countryman, Secretary, SEC, RE: SEC Proposed Rule on Cybersecurity Risk Management,

Strategy, Governance, and Incident Disclosure, File No. S7-09-22 (May 9, 2022), https://www.sec.gov/comments/s7-09-22/s70922-20128391-291294.pdf (criticizing the SEC's proposed rule as out of step with consensus federal policy and the newly enacted CIRCIA).

Despite these concerns, the SEC's treatment of Covington suggests that the agency intends to insert itself ever more aggressively into private sector cybersecurity, which is not at the core of its Congressional mandate or expertise. The SEC's mission is "[t]o protect investors[,] maintain fair, orderly, and efficient markets[,] and facilitate capital formation." SEC, *About the SEC* (Nov. 22, 2016), https://www.sec.gov/about. Certainly, SEC leadership has provided guidance about material cyber risks and the need for regulated entities to consider cyber as part of their enterprise risk management. But the SEC's most recent Strategic Plan, describing the agency's responsibilities, expertise and goals, (SEC, Strategic Plan Fiscal Years 2022–2026 (2022), https://www.sec.gov/files/sec_strategic_plan_fy22-fy26.pdf), mentions cyber merely three times and nowhere previews the broad authorities claimed in defense of its Subpoena here. It states that to address some kinds of systemic issues, "the SEC must pursue new authorities from Congress where needed." *Id.* at 11. Cybersecurity and incident reporting are two such issues. Until that time, and in the midst of "continuing cybersecurity workforce challenges," the agency can add little value, if any, to investigation of cyber incidents like the attack on Covington. *See generally*, GAO-23-106415 Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight (2023), https://www.gao.gov/assets/gao-23-106415.pdf.

The SEC is institutionally not suited to be a primary actor in the oversight of cybersecurity risk management, much less in investigating incidents and attacks. This relatively limited expertise and the absence of a Congressionally directed role should have led the agency

to be more measured in its approach to Covington in the wake of the Hafnium attack. It should rely on its ample existing tools to investigate insider training and disclosure practices, without using abusive tactics that raise novel and sensitive issues that intrude on lawyer-client confidentiality, privacy rights, and agency authorities.

CONCLUSION

For the foregoing reasons, the Court should deny the SEC's Application.

February 21, 2023

Respectfully submitted,

/s/ Megan L Brown
Megan L. Brown, Bar ID: 490842
Kevin Muhlendorf, Bar ID: 469596
Boyd Garriott, Bar ID: 1617468
Tyler Bridegan
WILEY REIN LLP
2050 M Street NW
Washington, D.C. 20036
Telephone: (202) 719-7000
Facsimile: (202) 719-7049
mbrown@wiley.law
kmuhlendorf@wiley.law
bgarriott@wiley.law
tbridegan@wiley.law

Counsel for Amicus Curiae Chamber of Commerce of the United States of America

CERTIFICATE OF COMPLIANCE

I hereby certify that the filing complies with the Local Civil Rules relating to formatting and page limits, being double-spaced, prepared in 12-point font, and not exceeding the allotted page or word limits.

/s/ Megan L. Brown
Megan L. Brown (Bar ID: 490842)

CERTIFICATE OF SERVICE

I hereby certify that on February 21, 2023, I caused a true and correct copy of the foregoing document to be served upon all counsel of record registered with the Court's ECF system, by electronic service via the Court's ECF transmission facilities.

/s/ Megan L. Brown
Megan L. Brown (Bar ID: 490842)