IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

DEMOCRATIC NATIONAL COMMITTEE, Plaintiff, v. THE RUSSIAN FEDERATION et al., Defendants.	)	Civil Action No. 1:18-cv-03501-JGK

PLAINTIFF'S OMNIBUS MEMORANDUM OF LAW IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS AND RUSSIA'S STATEMENT OF IMMUNITY

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

Plaintiff the Democratic National Committee ("Plaintiff" or "DNC") hereby submits this Omnibus Memorandum of Law in Opposition to the Motions to Dismiss the Second Amended Complaint (ECF No. 217) ("Complaint") filed by Defendants Donald J. Trump for President, Inc. (the "Trump Campaign" or the "Campaign") (ECF No. 227) ("Campaign Br."); Aras Iskenerovich Agalarov ("Aras Agalarov") and Emin Araz Agalarov ("Emin Agalarov") (together, the "Agalarovs") (ECF No. 230) ("Agalarov Br."); Jared Kushner ("Kushner") (ECF No. 222) ("Kushner Br."); George Papadopoulos ("Papadopoulos") (ECF No. 234) ("Papadopoulos Br."); Roger J. Stone, Jr. ("Stone") (ECF No. 232) ("Stone Br.")[1]; WikiLeaks (ECF Nos. 208, 225) ("WikiLeaks 1st Br." and "WikiLeaks 2nd Br.", respectively) (collectively, the "Motions to Dismiss").[2] This Memorandum also responds to the "Statement of Immunity of the Russian Federation" (ECF No. 186) ("Statement of Immunity") filed by the Russian Federation ("Russia").

I. INTRODUCTION

In the run-up to the 2016 election, Defendants mounted a brazen attack on American democracy. The Trump Campaign, Trump's closest advisors, WikiLeaks, and Russia participated in a common scheme to hack into the DNC's computer system, steal its trade secrets and other private documents, and then strategically disseminate those materials to the public to improve

[1] Because Stone's brief does not contain page numbers, citations to his brief reference ECF pagination.

[2] Defendants Paul J. Manafort, Jr. ("Manafort"), Donald J. Trump, Jr. ("Trump, Jr."), and Julian Assange ("Assange") did not move to dismiss the Complaint, and thus concede it adequately alleges the claims asserted against them. Defendant Joseph Mifsud, whose whereabouts are unknown, has not been served, and he has not moved to dismiss the Complaint. In his motion to dismiss, (ECF No. 223), Richard W. Gates III ("Gates") states only that he incorporates each and every argument of every Defendant, "insofar as it applies to him." Because Gates does not raise any original arguments, the DNC does not cite Gates's motion in the remainder of this memorandum. Nevertheless, all references to "Defendants" include Gates, unless otherwise specified.

Trump's chances of winning the election. After securing Trump's grip on power, Defendants worked tirelessly to keep it, lying to the American public, Congress, the Justice Department, and the FBI to conceal any misconduct that jeopardized Trump's presidency.

Over the course of nearly 100 pages, the Complaint marshals compelling evidence of Defendants' coordinated efforts to damage the DNC and benefit Trump, including forensic analyses of the DNC's computers, documented conversations and meetings, and government reports. As described in the Complaint, these sources reveal that:

- After a Russian agent met with a foreign policy advisor to the Trump Campaign, a team of Russian intelligence officers hacked into the DNC's computer system and stole sensitive documents, including trade secrets. They also stole confidential materials from other Democratic Party targets.

- Before disseminating any of these materials to the public, the Russian government offered Trump, Jr.—who was a close political advisor to his father during throughout his presidential campaign—"sensitive" documents and other information damaging to the Democratic Party as "part of Russia and its government's support for Mr. Trump." Rather than reporting this overture to U.S. authorities, Trump, Jr. responded: "If it's what you say, I love it," and then arranged a meeting for members of the Trump Campaign to discuss the documents with Russian agents in Trump Tower.

- The day after the Trump Tower meeting, Russia hacked into a DNC backup server.

- Just a few days later, Russia began posting stolen DNC documents online.

- After seeing the stolen documents, WikiLeaks contacted Russia and explained that, if Russia agreed to release new stolen materials through WikiLeaks, it would have a much "greater impact" on the election. WikiLeaks further recommended releasing stolen documents on the eve of the Democratic National Convention to prevent Democrats from rallying around their nominee.

- WikiLeaks gave Trump, Jr. a stolen password that he used to gain unlawful access to an anti-Trump website.

- Stone, who advised Trump during his campaign, asked an associate to contact WikiLeaks and request that it publish specific stolen Democratic documents.

- Trump's campaign manager, Paul Manafort, shared internal Trump Campaign polling data with a known Russian spy.

- Several Defendants have repeatedly lied to the public and federal investigators, committed criminal obstruction of justice, and intimidated witnesses to conceal their meetings and their ties to each other and to Russia.

In the face of these weighty allegations, Defendants attempt to rewrite black letter conspiracy law. Throughout their briefs, Defendants assert that, because they did not personally commit certain offenses (such as hacking into the DNC's servers), they cannot be liable for the damage caused by those offenses. Not so. Each Defendant joined an ongoing conspiracy to steal the DNC's data and use it to support Trump's candidacy. Courts have long recognized that, if a defendant joined a conspiracy, he is liable for all crimes that his co-conspirators committed to further their shared goals, regardless of whether those crimes occurred "before [or] after" the defendant "became a member" of the conspiracy. *United States v. Santos*, 541 F.3d 63, 73 (2d Cir. 2008). As a matter of law, therefore, all Defendants are responsible for the hacking of the DNC's servers and the dissemination of stolen documents to the public.

Defendants also attempt to compartmentalize the Complaint's allegations, arguing that specific events—considered in isolation—are not particularly incriminating. Once again, however, Defendants are sailing into the wind. The Supreme Court has instructed that the "character and effect of a conspiracy are not to be judged by dismembering it and viewing its separate parts, but only by looking at it as a whole." *Cont'l Ore Co. v. Union Carbide & Carbon Corp.*, 370 U.S. 690, 699 (1962). Accordingly, conspiracies are regularly established by piecing together a series of clues. That is precisely what the DNC has done here: When all the evidence in the Complaint is considered as a whole, it raises a plausible inference that the Defendants implemented an unlawful agreement.

Nor can Defendants hide behind the First Amendment. The Complaint presents clear evidence that all Defendants—including WikiLeaks—participated in a criminal conspiracy to steal the DNC's information and use it to support Russia's preferred presidential candidate. The First

Amendment affords no protection for information thieves or foreign actors working to influence the outcome of American elections. Thus, when the Trump Campaign presented its First Amendment theory to a federal court in Virginia, the court rejected it out of hand.

Russia can also be held accountable for its role in the conspiracy. The Foreign Sovereign Immunities Act ("FSIA") does not confer immunity on Russia for torts committed in the United States, such as trespassing onto the DNC's servers or converting the DNC's property. The FSIA also gives the DNC the right to sue Russia for commercial activity, such as theft of the DNC's trade secrets.

The Motions to Dismiss should therefore be denied and the Russian Federation's Statement of Immunity should be rejected.

II. FACTS

When all of the allegations in the Complaint are construed in the light most favorable to the DNC, they paint a portrait of previously unimaginable treachery: a presidential campaign and its associates conspiring with a hostile foreign power to secure Trump's grip on the presidency. Near the end of 2015, Felix Sater, a longtime business partner of Trump, ¶ 87,[3] told Michael Cohen ("Cohen"), Trump's personal attorney: "I will get Putin on this program and we will get Donald elected . . . . I know how to play it and we will get this done. Buddy our boy can become President of the USA and we can engineer it. I will get all of Putins [sic] team to buy in on this, I will." ¶ 88.

In early 2016, as the Trump Campaign was gathering steam, Campaign leaders set the stage for a cooperative relationship with Russia. ¶¶ 10, 89. In February of that year, the Campaign recruited Lt. Gen. Michael T. Flynn ("Flynn") to serve as an informal foreign policy advisor. ¶ 90.

[3] Citations to "¶ __" refer to paragraphs of the Complaint.

Flynn had recently delivered a paid speech to a Russian government-funded propaganda outlet and dined with Putin. *Id.*

In March 2016, the Trump Campaign hired Manafort, who had spent the previous decade working to advance Kremlin interests in Ukraine. ¶ 91. At the time, Manafort was millions of dollars in debt to Oleg Deripaska ("Deripaska"), a Putin-tied Russian oligarch. While Manafort had no money to pay back this debt, he agreed to work for the Trump Campaign for free. *Id.* Manafort told Deripaska that he wanted to use campaign-related "media coverage" to settle his debts, and offered Deripaska private briefings on the campaign. ¶¶ 91, 152. In other words, Manafort expressed hope that, in lieu of payment from the Trump Campaign, he could receive debt relief from a Russian oligarch closely connected to Putin. In addition to proposing this troubling financial arrangement, Manafort maintained regular contact with Konstantin Kilimnik ("Kilimnik"), who was once known around Manafort's office as "the guy from the GRU [Russia's military intelligence agency]." ¶ 67.

Papadopoulos, a foreign policy adviser to the Trump Campaign, also began to cultivate relationships with Russian operatives in March 2016. ¶¶ 93-100. In March and April, Papadapoulos repeatedly met with Mifsud, who helped connect him to "official and unofficial" Russian sources. ¶ 95. Papadapoulos later told his Russian sources about signals they could hear in Trump's speeches. *See* ¶ 98. For example, after Trump gave his first major foreign policy address, where he spoke about "improved relations with Russia," Papadopoulos told one of his Russian contacts "that's the signal to meet." *See id.* Confirming the illicit nature of his activities, Papadopoulos lied to the FBI to conceal his contacts with Mifsud and other Russians. ¶ 223.

On April 18, 2016, the same day that Papadopoulos met with Mifsud and an individual with connections to the Russian Ministry of Foreign Affairs, Russian intelligence operatives

launched a months-long cyberattack against the DNC. During that attack, Russia stole DNC documents and data—including trade secrets—and placed malware known as X-Agent on DNC computers, so that Russian spies could monitor messages and data going to and from those computers in realtime. ¶¶ 94, 101.

Before disseminating a single page stolen from the DNC, Russia reached out to the Trump Associates[4] to tell them about the trove of documents it had stolen to further their criminal plan. On April 26, 2016, Papadopoulos again met with Mifsud, who told him that the Russians had "thousands of emails" that could harm Secretary Clinton's presidential campaign. ¶ 94. Rather than reporting this troubling message to American law enforcement authorities, Papadopoulos simply reported back to his superiors at the Trump Campaign. ¶¶ 96-97.

On June 3, 2016, Aras and Emin Agalarov, two more Kremlin-connected oligarchs, contacted Donald Trump, Jr. with an offer from the Russian Crown Prosecutor: Russia wanted to give the Trump Campaign "very high level and sensitive information" and "documents" concerning the Democratic presidential nominee. Trump, Jr. gleefully accepted, exclaiming, "if it's what you say I love it, especially later in the summer" ¶¶ 133-34. Trump, Jr. then called Emin Agalarov to arrange a "meeting at which Russians would provide the Trump Campaign with [the] damaging information about the Democratic nominee." ¶ 135. On June 6 and 7, the two men held more phone calls to discuss the upcoming meeting, presumably setting a rough agenda. *Id.* Trump, Jr. also discussed the upcoming meeting with senior members of the Trump Campaign, including Manafort, Gates, and Kushner. ¶ 219. The carefully planned meeting took place two days later, on June 9, 2016, in Trump Tower. ¶ 137. "The Trump Campaign was represented by Trump's inner-circle: Trump, Jr., Kushner, and Manafort. Representing Russia's interests were Agalarov publicist

[4] Capitalized terms are as defined in the Complaint unless otherwise noted.

Rob Goldstone ["Goldstone"], Kremlin-connected Russian lawyer Natalia Veselnitskaya ("Veselnitskaya"), Agalarov business associate Irakyl Kaveladze, lobbyist Rinat Akhmestshin, and a translator." *Id.* Notably, the individuals who attended the Trump Tower meeting lied about it, either to the American public or to congressional investigators.

Within days of the Trump Tower meeting, two things happened. First, Russia renewed its hacking efforts by breaking into a DNC backup server. ¶¶ 143-44. Second, Russia began disseminating the documents it stole from the DNC, including trade secrets, through a fictitious online persona called Guccifer 2.0. ¶ 148.

On June 22, 2016—the day after Guccifer 2.0 disseminated its second batch of stolen DNC documents—WikiLeaks reached out to Guccifer 2.0 and asked it to "[s]end any new material [stolen from the DNC] here for us to review and it will have a much higher impact than what you are doing." ¶ 149. In subsequent exchanges, WikiLeaks explained that Trump had a "25 percent chance" of defeating the Democratic presidential nominee and suggested that his odds might improve if WikiLeaks could disseminate stolen documents that would create conflict among Democrats during the upcoming Democratic National Convention. ¶ 150.

Between July 14, 2016 and July 18, 2016, Russian intelligence operatives transmitted stolen DNC documents—including trade secrets—to WikiLeaks; as promised, WikiLeaks disseminated them on the eve of the Democratic National Convention. ¶¶ 154-56. The result was chaos—the DNC had to change its anticipated speakers, and DNC employees were flooded with so many threatening phone calls and emails that it was difficult to use their phones to carry out Convention plans. ¶ 20.

Throughout the summer and fall of 2016, during the height of the presidential campaign, the Trump Associates and other individuals affiliated with the Trump Campaign regularly

communicated with Russian agents and WikiLeaks as they strategically disseminated information at moments when it would be most helpful to the Trump Campaign. *See* ¶¶ 159-176. At one point, Manafort, who served as chairman of the Trump Campaign, even gave Kilimnik "polling data . . . related to Trump's 2016 Campaign," that could have helped Russia gauge the effects of publishing DNC documents; Manafort later concealed that interaction from the Special Counsel. ¶ 231. Trump, Jr. and WikiLeaks also worked together to hack into an anti-Trump political action committee website, which could have informed their shared election interference strategy. ¶ 173.

Even Trump himself supported the GRU and WikiLeaks's information theft and dissemination. "At a press conference on July 27, 2016, after commenting extensively on . . . materials that were stolen from the DNC['s] servers" (including trade secrets), Trump urged Russia to steal additional documents from Secretary Clinton's personal email server, calling out: 'Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing.'" ¶ 158. That same day, the GRU "attempted—for the first time—to hack email accounts used by Secretary Clinton's personal office." *Id.*

In August 2016, Stone revealed information that he could not have had unless he were communicating with WikiLeaks, Russian operatives, or both about their hacking operations in the United States. For instance, in August of 2016, nobody in the public sphere knew that Russia had stolen emails from John Podesta, the chairman of Secretary Hillary Clinton's presidential campaign. Nevertheless, on August 21, 2016, Stone forecasted that damaging information about Podesta would be released, tweeting "it will soon [be] the Podesta's [sic] time in the barrel." ¶ 170. Weeks later, WikiLeaks began releasing batches of Podesta's emails on a near-daily basis until Election Day—as Stone had said. ¶ 175. Similarly, in mid-September 2016, Stone said that he expected "Julian Assange and the WikiLeaks people to drop a payload of new documents on

Hillary [Clinton] on a weekly basis fairly soon." ¶ 172. And, beginning on October 7, 2016, WikiLeaks began releasing stolen emails at least once a week—as Stone had predicted. ¶ 175.

Around the same time, Stone requested that WikiLeaks disseminate specific stolen documents that, from Stone's perspective, would be particularly damaging to Democrats. ¶ 171. WikiLeaks, for its part, suggested that Trump call public attention to certain batches of stolen documents on the WikiLeaks website. ¶ 173.

On September 9, 2016, GRU operatives contacted Stone, writing him "please tell me if I can help u anyhow[,]" and adding "it would be a great pleasure to me." ¶ 179. The operatives then asked Stone for his reaction to a stolen "turnout model for the Democrats' entire presidential campaign." *Id.* Stone replied, "[p]retty standard." *See id.*

Throughout September 2016, Russian intelligence agents illegally gained access to DNC computers hosted on a third-party cloud computing service, stole large amounts of the DNC's private data and proprietary computer code, and exfiltrated the stolen materials to their own cloud-based accounts registered with same service. ¶ 180.

On November 9, 2016, Trump won the Presidency of the United States. ¶ 204. The reaction in Russia was jubilation, with a member of Russia's parliament telling his fellow legislators: "I congratulate you all on this." ¶ 205. The same day, WikiLeaks sent a private message to Stone on Twitter: "Happy? We are now more free to communicate." ¶ 207.

Despite Trump's victory, Defendants recognized that his grip on political power would be jeopardized if the American public discovered the illegal coordination between Russia and the Trump Campaign. The Defendants therefore dedicated their criminal enterprise to concealing their collusion, sometimes by lying to the American public, and other times through criminal obstruction of justice. ¶ 206. For example, just two days after the 2016 election, Trump Campaign

spokesperson Hope Hicks falsely told the Associated Press that the Trump Campaign had no communications with any "foreign entity" during the campaign: "Never happened. There was no communication between the campaign and any foreign entity during the campaign." ¶ 208.

Moreover, Stone, Kushner, Trump, Jr., Corsi, and Manafort lied to or misled the Special Counsel, the FBI, and Congressional committees tasked with investigating Russian interference in the American election. On January 18, 2017, Kushner failed to disclose in his security clearance form that he met with Veselnitskaya and other Russian government representatives at the Trump Tower meeting. ¶ 213. Similarly, on July 24, 2017, Kushner provided a written statement to Congress stating that he did not know what the Trump Tower meeting was going to be about, despite the fact the House Intelligence Committee Majority's report concluded that Kushner, Trump, Jr. and Manafort all attended a preparatory meeting before gathering in Trump Tower. ¶ 219 Kushner also falsely denied attempting to create a "secret backchannel" with the Russian government. ¶ 220.

In September 2017, Stone falsely told the House Intelligence Committee that he never had any communications with any Russians in connection with the 2016 presidential election. ¶ 214. He also falsely told the Committee he spoke to Assange only through Credico, despite the fact that he communicated with Assange through Corsi and he exchanged Twitter direct messages with WikiLeaks in 2016. ¶ 225. To bolster this narrative, Stone directed Corsi to delete incriminating emails. ¶ 215. When the House Intelligence Committee subpoenaed Credico, on November 30, 2017, Stone asked Corsi to write publicly about Credico, presumably to discredit or influence his testimony. ¶ 226. Credico stated that, around the time Stone was interviewed by the House Intelligence Committee, Stone told him to "just go along with" Stone's story. Credico later asserted his Fifth Amendment rights and declined to talk to the Committee. ¶ 226. When, in early 2018,

Credico began to dispute Stone's story, Stone sent Credico a barrage of communications to attempt to convince Credico to stick with Stone's false narrative. After Credico nevertheless indicated he would dispute the narrative, Stone threatened Credico: "I am so ready. Let's get it on. Prepare to die cock sucker." ¶ 228.

On July 8 and 9, 2017, Trump, Jr. made highly misleading statements about the Trump Tower meeting, falsely stating the meeting was to discuss "the adoption of Russian children . . . ." ¶ 217. On September 7, 2017, he testified before the Senate Judiciary Committee that no attendee of the Trump Tower meeting requested additional meetings or communications with members of the Trump Campaign, but this testimony was flatly contradicted by subsequently released emails in which Goldstone (a Trump Tower meeting attendee), sought a second meeting between Veselnitskaya (another Trump Tower meeting attendee) and the Trump transition team shortly after the election. ¶ 222.

On October 5, 2017, Papadopoulos pleaded guilty to lying to the FBI about his contacts with Mifsud and other Russian agents during a January 27, 2017 interview. He also admitted that he deleted his Facebook account, scrubbed other social media accounts, and changed his cell phone number to try to hide those contacts. ¶ 223.

On September 6, 2018, Corsi lied to the Special Counsel's office and FBI special agents, falsely telling them he declined Stone's request to contact WikiLeaks, and that he never provided Stone with any information regarding WikiLeaks, what materials WikiLeaks possessed, or what WikiLeaks intended to do with those materials. ¶ 230.

These illegal concealment efforts dovetailed with Russia's work to undermine Mueller's investigation. Soon after Mueller's appointment in 2017, using fake social media accounts, Russia engaged in an influence campaign aimed at painting Mueller as corrupt and discrediting allegations

of Russian interference in the 2016 election. ¶ 212. As the *Washington Post* put it, "[h]aving worked to help Trump into the White House, [Russia] now worked to neutralize the biggest threat to his staying there." *Id.*

Like Russia, Assange and WikiLeaks also worked to undermine the Special Counsel's investigation. On July 29, 2017, for instance, WikiLeaks tweeted: "Will Special Prosecutor Robert Mueller Fabricate The Results Of His Investigation Like He Did With Iraq?" ¶ 221. Moreover, on October 11, 2018, WikiLeaks released a proprietary AWS document which analysts noted would be incredibly valuable for those trying to compromise AWS servers like the ones that house the DNC's documents and data—*i.e.* Russia. ¶ 235.

Both Stone and Russia have maintained contact with Assange and worked to protect him and his ability to operate WikiLeaks to support the goals of the enterprise. Stone has engaged in a vigorous effort to secure a pardon for Assange. ¶ 229. In late 2017, Russian diplomats met secretly with a close confidante of Assange to devise a plan to smuggle him out of Ecuador's London embassy in a diplomatic vehicle. ¶ 69. However, the plan was abandoned after it was deemed too risky. *Id.*

Meanwhile, Russia committed fresh cybercrimes in the run-up to the 2018 midterm elections geared toward protecting the enterprise and advancing its goals. For instance, in August 2017, Russia attempted to hack into the Senate computer network of a Democratic Senator—a longtime critic of Trump, Russia, and WikiLeaks—and the networks of two other midterm candidates. ¶¶ 232-33. In November 2018, dozens of DNC email addresses were targeted in a spear-phishing campaign, although there is no evidence that the attack was successful. The content of these emails and their timestamps were consistent with a spear-phishing campaign that leading

cybersecurity experts have tied to Russian intelligence. Therefore, it is probable that Russian intelligence again attempted to unlawfully infiltrate DNC computers in November 2018. ¶ 236.

Since the 2016 election, U.S. intelligence and law enforcement agencies have repeatedly emphasized the continuing nature of the threat of Russian interference in U.S. elections. For example, in August 2018, senior U.S. national security and intelligence officials announced that Russia was continuing its illicit interference in domestic politics, including through social media disinformation campaigns, attempts to hack political targets, and infiltrate the country's electoral infrastructure. ¶ 234. Director of National Intelligence Dan Coats characterized the threat of continued Russian interference as "real" and "continuing," and FBI Director Chris Wray added that "[t]his threat is not going away." *Id.*

III. LEGAL STANDARDS

A. Standard of Review on a Motion to Dismiss Pursuant to Federal Rule of Civil Procedure 12(b)(6)

Rule 8 of the Federal Rules of Civil Procedure provides that a complaint "must contain . . . a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). To survive a motion to dismiss pursuant to Rule 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*. (citing *Twombly*, 550 U.S. at 556); *see Arista Records, LLC v. Doe 3*, 604 F.3d 110, 119 (2d Cir. 2010) (rejecting "notion that *Twombly* imposed a heightened standard that requires a complaint to include specific evidence" of each allegation). In considering a motion to dismiss, the court accepts as true all factual allegations in the complaint and draws all reasonable inferences

in the plaintiff's favor. *See Goldstein v. Pataki*, 516 F.3d 50, 56 (2d Cir. 2008). And "it is well-settled that a complaint must be read as a whole, not parsed piece by piece to determine whether each allegation, in isolation, is plausible." *Pension Ben. Guar. Corp. ex rel. St. Vincent Catholic Med. Ctrs. Ret. Plan v. Morgan Stanley Inv. Mgmt. Inc.*, 712 F.3d 705, 732 (2d Cir. 2013) (quotation marks and citation omitted).

"[A] given set of [allegations] may well be subject to diverging interpretations, each of which is plausible." *Anderson News, L.L.C. v. Am. Media, Inc.*, 680 F.3d 162, 184 (2d Cir. 2012) (citing *Anderson v. Bessemer* City, 470 U.S. 564, 575 (1985)). In such a case, "[t]he choice between two plausible inferences that may be drawn from factual allegations is not a choice to be made by the court on a Rule 12(b)(6) motion." *Id.* at 185. Indeed, "[a] court ruling on such a motion may not properly dismiss a complaint that states a plausible version of the events merely because the court finds a different version more plausible." *Id.*; *see also Twombly*, 550 U.S. at 556 ("[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of the facts alleged is improbable, and that recovery is very remote and unlikely." (internal quotation marks omitted)).

Thus, in the conspiracy context, "[t]o present a plausible claim at the pleading stage, the plaintiff need not show that its allegations suggesting an agreement are more likely than not true or that they rule out the possibility of independent action[.]" *Anderson News, L.L.C.*, 680 F.3d at 184. "Asking for plausible grounds to infer an agreement *does not impose a probability requirement at the pleading stage*; it simply calls for enough fact to raise *a reasonable expectation* that *discovery* will reveal evidence of illegal agreement." *Id.* (quoting *Twombly*, 550 U.S. at 556).

B. Scope of Material Properly Before the Court on a Rule 12(b)(6) Motion

At the motion to dismiss stage, a court cannot consider evidence outside the four corners of the complaint, even if that evidence purports to cast doubt on the plaintiff's version of events.

See Goel v. Bunge, Ltd., 820 F.3d 554, 558-59 (2d Cir. 2016). There are only two narrow exceptions to this rule. First, a court may consider documents that are "incorporated by reference [in] or otherwise integral to the complaint." *Concord Assocs., L.P. v. Entm't Props. Tr.*, 817 F.3d 46, 51 n.2 (2d Cir. 2016). Second, a court may consider judicially noticeable documents if the plaintiff "rel[ied] on the documents in drafting the [c]omplaint." *Id.*

A document is only "integral" to the complaint if the complaint "relies heavily upon its terms and effect." *See Goel*, 820 F.3d at 559 (quoting *Chambers v. Time Warner Inc.*, 282 F.3d 147, 153 (2d Cir. 2002)). A document will not satisfy this standard simply because a plaintiff has quoted it in the complaint. *Id.* Nor is it enough for a complaint to cite a document "for the purpose of indicating that evidence existed to support the complaint's assertions." *Sahu v. Union Carbide Corp.*, 548 F.3d 59, 68 (2d Cir. 2008) (citing *Twombly*, 550 U.S. at 544). Rather, in "most instances" where the court finds that a document is "integral" to a complaint, the document "is a contract or other legal document containing obligations upon which the plaintiff's complaint stands or falls . . . " *Glob. Network Commc'ns, Inc. v. City of New York*, 458 F.3d 150, 157 (2d Cir. 2006); *accord Goel*, 820 F.3d at 559.

A court can only take judicial notice of a "fact that is not subject to reasonable dispute because it (1) is generally known within the trial court's territorial jurisdiction; or (2) can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201. This may include "the fact of" public documents and filings, but not "the truth of the matters asserted" in those filings. *Int'l Star Class Yacht Racing Ass'n v. Tommy Hilfiger U.S.A., Inc.*, 146 F.3d 66, 70 (2d Cir. 1998) (quotation marks omitted); *accord Staehr v. Hartford Fin. Servs. Grp., Inc.*, 547 F.3d 406, 425 (2d Cir. 2008) (same rule applies to "press coverage, prior lawsuits, or regulatory filings").

IV. ARGUMENT

A. The Complaint Adequately Alleges Substantive RICO Violations (Responding to: Agalarov Br. 6-14, Campaign Br. 12-37, Kushner Br. 3-10, Papadopoulos Br. 7-20, Stone Br. 20-23, WikiLeaks 1st Br. 12-16, WikiLeaks 2nd Br. 3-6)

RICO is an "aggressive initiative" for fighting crime, which should be "read broadly." *Sedima, S.P.R.L. v. Imrex Co.*, 473 U.S. 479, 497-98 (1985). "This is the lesson not only of Congress' self-consciously expansive language and overall approach [to the statute], but also of its express admonition that RICO is to 'be liberally construed to effectuate its remedial purposes.'" *Id.* (internal citation omitted) (quoting Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 904(a), 84 Stat. 947). Congress counted on the American public to enforce RICO's robust criminal prohibitions: The statute includes a private right of action that allows individuals injured by racketeering activity to serve as "private attorneys general," supplementing the government's efforts to hold defendants accountable for complex criminal schemes, *Holmes v. Sec. Inv'r Prot. Corp.*, 503 U.S. 258, 283 (1992), particularly in cases where the government chooses not to prosecute defendants criminally, *see Sedima, S.P.R.L.*, 473 U.S. at 493 (explaining that "[p]rivate attorney general provisions such as § 1964(c) are in part designed to fill prosecutorial gaps" that arise when the government declines to press criminal charges against a "guilty party"). The DNC uses the critical tools Congress provided in the RICO statute to hold Defendants accountable for their wrongdoing.

As required by RICO, the DNC has plausibly alleged that Defendants (1) conducted the affairs of (2) an enterprise affecting interstate or foreign commerce (3) through a pattern of racketeering activity, 18 U.S.C. § 1962(c), and that (4) the DNC suffered an injury to its business or property that (5) was proximately caused by the Defendants' RICO violation, 18 U.S.C. § 1964(c). *D'Addario v. D'Addario*, 901 F.3d 80, 96 (2d Cir. 2018); *see also World Wrestling*

Entm't, Inc. v. Jakks Pac., Inc., 530 F. Supp. 2d 486, 496 (S.D.N.Y. 2007) (A RICO plaintiff need only satisfy Rule 8's plausibility standard).[5]

1. *Conducting the Affairs (Responding to: Agalarov Br. 9-10, Campaign Br. 24-26, Kushner Br. 8-10, Papadopoulos Br. 16-17, Stone Br. 20-21, WikiLeaks 1st Br. 13-14)*

Each of the Defendants "conduct[ed] or participat[ed], directly or indirectly," in the RICO enterprise's affairs. 18 U.S.C. § 1962(c). To determine whether a defendant's conduct satisfies this requirement, courts ask whether the defendant participated in the "operation *or* management" of the enterprise. *Reves v. Ernst & Young*, 507 U.S. 170, 179 (1993) (emphasis added). This inquiry "presents a 'relatively low hurdle for plaintiffs to clear, . . . especially at the pleading stage.'" *D'Addario*, 901 F.3d at 103 (quoting *First Capital Asset Mgmt., Inc. v. Satinwood, Inc.*, 385 F.3d

[5] The Agalarovs ask the Court to dismiss the Complaint with prejudice, suggesting that the Court has an "obligation" to dismiss frivolous RICO claims early in litigation. Agalarov Br. 24-25. The Trump Campaign similarly argues that the Court must look with "particular scrutiny" at RICO claims. Campaign Br. 13. Essentially, these Defendants suggest that RICO claims are inherently suspect and ask the Court to regard the DNC's allegations with suspicion. But the U.S. Supreme Court has consistently recognized the importance of private civil RICO actions. *See, e.g., Rotella v. Wood*, 528 U.S. 549, 557 (2000) (recognizing RICO's "congressional objective of encouraging civil litigation to supplement Government efforts to deter and penalize [its] prohibited practices. The object of civil RICO is thus not merely to compensate victims but to turn them into prosecutors, 'private attorneys general,' dedicated to eliminating racketeering activity."). And civil RICO actions are not subject to any heightened pleading requirement, *World Wrestling Entm't, Inc.*, 530 F. Supp. 2d at 496, unless, unlike here, a defendant's predicate acts involve fraud. *Weizmann Inst. Of Sci. v. Neschis*, 229 F. Supp. 2d 234, 245 (S.D.N.Y. 2002). Instead, as with any action subject to the Rule 8 pleading standard, the Court should accept as true all factual allegations in the Complaint and draw all reasonable inferences in the DNC's favor. *See Cruz v. FXDirectDealer, LLC,* 720 F.3d 115, 118 (2d Cir. 2013) (applying the *Iqbal* standard in a RICO case).

159, 176 (2d Cir. 2004)). Contrary to Papadopoulos's and Stone's suggestion, a plaintiff need not show that a defendant had "primary responsibility for the enterprise's affairs," or even a "a formal position in the enterprise." *Reves*, 507 U.S. at 179; *see* Papadopoulos Br. 17; Stone Br. 20-21. Nor is a plaintiff required to show that a defendant participated in "all of the enterprise's affairs." *In re Express Scripts/Anthem ERISA Litig.*, 285 F. Supp. 3d 655, 685 (S.D.N.Y. 2018). A plaintiff need only allege that a defendant played "*some* part" in directing a portion of the enterprise's activities. *Reves*, 507 U.S. at 179; *In re Express Scripts/Anthem ERISA Litig.*, 285 F. Supp. 3d at 685. This burden can be satisfied by alleging that a defendant "actively assisted" the leaders of an association-in-fact enterprise ("AIF enterprise")[6] as they engaged in racketeering activity. *D'Addario*, 901 F.3d at 104.

Applying these principles, the Complaint adequately alleges that Defendants participated in the "operation or management" of the two alternative enterprises described in the Complaint: the AIF Enterprise and the Trump Campaign.

Aras Agalarov. The facts alleged in the Complaint suggest that Aras Agalarov helped make important decisions on behalf of the AIF Enterprise. On June 3, 2016, Aras Agalarov met with the Crown Prosecutor of Russia and discussed how Russia could use "official documents" and "high level and sensitive information" to bolster Trump's candidacy. ¶ 133. It is reasonable to infer that the Crown Prosecutor discussed those sensitive matters with Aras because he believed that Aras could help him decide what information to share or how to deliver sensitive documents—such as stolen Democratic materials—to the Trump Campaign.

[6] As explained in detail below at Section IV.A.2, an AIF enterprise is "any union or group of individuals associated in fact although not a legal entity." 18 U.S.C. § 1961(4).

The Complaint also alleges that Aras "actively assisted" the leaders of the AIF Enterprise and the Trump Campaign by serving as a trusted go-between, funneling information and offers of assistance from the Russian government to senior members of the Trump Campaign, including Trump, Jr. *D'Addario*, 901 F.3d at 104; *see* ¶¶ 133, 222. By brokering relationships and facilitating communications between Russia and the Trump Campaign, Aras "directly" affected the way that the AIF Enterprise and the Trump Campaign conducted business. *D'Addario*, 901 F.3d at 104.

Emin Agalarov. Like his father, Emin Agalarov served as a trusted go-between for Russia and senior members of the Trump Campaign. *See* ¶ 133. He also collaborated with Trump, Jr. on the agenda for the Trump Tower meeting. *See* ¶ 135. In helping to decide what topics would be discussed, Emin helped shape the partnership between Russia and the Trump Campaign. Thus, he had ample "control and discretion" over the enterprise's affairs. *City of New York v. Fedex Ground Package Sys., Inc.*, 175 F. Supp. 3d 351, 372 (S.D.N.Y. 2016).

Kushner. Kushner was a "senior advisor" to the Campaign and made important strategic decisions on its behalf, including decisions about its "data-driven efforts." ¶ 59. As the leader of these efforts, *id.*, Kushner met with senior Campaign officials to prepare for the Trump Tower meeting, ¶ 219, and then participated in the Trump Tower meeting (where the Defendants likely discussed data stolen from the DNC, and how that data could be of use to the Campaign), ¶ 137. Attendance at the Trump Tower meeting was limited to the most senior members of the Campaign, who convened for the express purpose of discussing "very high level and sensitive information." ¶ 133. It is therefore reasonable to infer that Kushner directed the affairs of both enterprises.

Papadopoulos. As a foreign policy advisor to the Trump Campaign, Papadopoulos repeatedly met with Russian officials, who told him about stolen Democratic emails. ¶¶ 92-94.

Papadopoulos exercised "discretion" in delivering information he learned during these meetings to his superiors at the Trump Campaign. *Fedex*, 175 F. Supp. 3d at 372; *see* ¶ 97. By exercising a measure of control over the communications between Russia and the Trump Campaign, Papadopoulos directed the affairs of the Trump Campaign and the AIF Enterprise.[7] Moreover, Papadopoulos's attempts to broker a meeting between senior Trump Campaign officials and the Russian government establish Papadopoulos's active assistance to the leaders of the AIF Enterprise. *D'Addario*, 901 F.3d at 104; *see* ¶¶ 98, 100. Papadopoulos also went to great lengths to conceal these communications from the FBI so Defendants could continue to use illegal means to secure Trump's grip on power. ¶ 223.

WikiLeaks. WikiLeaks played a leadership role in the AIF Enterprise, and developed its "own methods and practices to determine how and when" to disseminate the DNC's information. *City of New York v. LaserShip, Inc.*, 33 F. Supp. 3d 303, 310 (S.D.N.Y. 2014). WikiLeaks was the architect of the plan to release stolen information on the eve of the Democratic National Convention, ¶¶ 149-51, and also instructed members of the Trump Campaign to call attention to specific leaked documents, ¶ 173.

Stone. Stone directed the affairs of both enterprises by discussing the release of DNC documents with WikiLeaks, Russian officers using the screen name Guccifer 2.0, and senior members of the Trump Campaign, helping them coordinate the timing of these releases to bolster

[7] Papadopoulos argues that his only participation in the enterprise consisted of "emailing the Trump Campaign that there were 'interesting messages coming in from Moscow about a trip when the time is right.'" Papadopoulos Br. 16. But the Complaint contains many detailed factual allegations regarding Papadopoulos' management of his contacts with ties to Russia, as well as his efforts to coordinate communication between Russia and the Trump Campaign. *See, e.g.*, ¶¶ 92-100.

Trump's electoral prospects. ¶¶ 161, 163, 167, 171-72, 174-76. Stone also went to great lengths to conceal these efforts from Congress, so that the Defendants could continue to use illegal means to secure Trump's grip on power. ¶¶ 224-26, 228.

Trump Campaign. The Trump Campaign also played a leadership role in the AIF Enterprise. Acting though its employees and other agents, the Trump Campaign repeatedly communicated with Russian agents (including the Russian agents at the Trump Tower meeting and Kilimnik) to obtain information about stolen DNC documents and determine how to use those documents to Trump's advantage during the 2016 election. *See, e.g.* ¶¶ 133-40, 159-76; *U1it4less, Inc. v. Fedex Corp.*, 871 F.3d 199, 205 (2d Cir. 2017) (noting that, in the RICO context (as in other contexts), a corporate entity can "act only though its employees, subsidiaries, or agents.").

2. *Enterprise Affecting Interstate and Foreign Commerce (Responding to: Agalarov Br. 14, Campaign Br. 13-24, Kushner Br. 8, Papadopoulos Br. 18, WikiLeaks 1st Br. 15)*

An enterprise" is "any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity." 18 U.S.C. § 1961(4). Plaintiff alleges the existence of two different enterprises: (1) the Trump Campaign itself; or, in the alternative, and at the very least, (2) an Association-in-Fact Enterprise ("AIF Enterprise").

a. Defendants Concede the Complaint Adequately Alleges the Trump Campaign is a RICO Enterprise (Responding to: Campaign Br. 13)

First, Plaintiff alleges that the Trump Campaign, a legal entity, is a racketeering enterprise as defined in 18 U.S.C. § 1961(4), and that each Defendant other than the Trump Campaign participated in the operation or management of the enterprise. ¶ 269. The Second Circuit has held that "*any* legal entity may qualify as a RICO enterprise." *First Capital Asset Mgmt., Inc.*, 385 F.3d at 173 (emphasis added); *see also D'Addario*, 901 F.3d at 102 ("[S]ection 1961(4) provides that

any 'legal entity' may qualify as a RICO enterprise . . . ."). Here, the Trump Campaign "is an American not-for-profit corporation," ¶ 55, and is thus "an 'enterprise' within the meaning of RICO." *D. Penguin Bros. Ltd. v. City Nat. Bank*, 587 F. App'x 663, 667 (2d Cir. 2014) (finding not-for-profit corporation was a RICO enterprise). Defendants do not contest, and thus concede, that the Complaint adequately alleges the Trump Campaign was a RICO enterprise, and that each Defendant other than the Trump Campaign itself is distinct from this enterprise.[8] None of the arguments discussed below at Section IV.A.2.b. has *any* bearing on whether the Complaint adequately alleges the Trump Campaign is a racketeering enterprise.

b. In the Alternative, the Complaint Also Adequately Alleges Defendants Were Part of an AIF Enterprise (Responding to: Campaign Br. 14-24)

In the alternative, Plaintiff alleges that the Trump Campaign was a member of an AIF Enterprise comprising Russia, WikiLeaks, Assange, the Trump Campaign, Aras and Emin Agalarov, Mifsud, the Trump Associates, Corsi, the Defendants' employees and agents, and additional entities and individuals known and unknown. ¶¶ 267, 272.

An AIF Enterprise is "any union or group of individuals associated in fact although not a legal entity." 18 U.S.C. § 1961(4). "The term 'any' ensures that the definition has a wide reach, and the very concept of an association in fact is expansive." *Boyle v. United States*, 556 U.S. 938, 944 (2009) (internal citation omitted). "The Supreme Court has . . . further instructed that, in accordance with the law's purposes, the RICO statute is to be 'liberally construed,' giving a broad and flexible reach to the term 'association-in-fact.'" *D'Addario*, 901 F.3d at 100 (quoting *Boyle*, 556 U.S. at 944). "In line with this general approach, the Supreme Court has rejected attempts to

[8] The Trump Campaign notes only that, as the enterprise itself, it cannot also be a member of the enterprise, Campaign Br. 13, a point that is not in dispute, *see* ¶ 269.

graft onto the statute formal strictures that would tend to exclude amorphous or disorganized groups of individuals from being treated as RICO 'enterprises.'" *Id.*

Thus, an AIF Enterprise requires only three structural features: "(1) a shared purpose, (2) relationships among the associates, and (3) 'longevity sufficient to permit these associates to pursue the enterprise's purpose.'" *Id.* (quoting *Boyle*, 556 U.S. at 946). The Complaint adequately pleads each of these elements.

(1) Common Purpose (Responding to: Campaign Br. 14-21, Kushner Br. 8, Papadopoulos Br. 18, WikiLeaks 1st Br. 15)

Several Defendants argue that the alleged AIF Enterprise lacked a common purpose. "Courts interpret the phrase 'common purpose' according to its plain meaning." *In re Nat. W. Life Ins. Deferred Annuities Litig.*, 635 F. Supp. 2d 1170, 1174 (S.D. Cal. 2009) (collecting cases). "The common purpose element . . . does not require the enterprise participants to share all of their purposes in common." *Id.* (citing *Odom v. Microsoft Corp.*, 486 F.3d 541, 552 (9th Cir. 2007)).

Here, the Complaint alleges that Defendants' "common purpose" was "to secure Trump's grip on the Presidency through illegal means." ¶ 70. The Trump Campaign does not meaningfully contest that Defendants shared this common purpose; rather, it notes that several Defendants had different motivations for pursuing their common goal. But that is of no moment. Individuals can join an enterprise for different reasons, but still work toward the enterprise's common objectives. *See United States v. Granton*, 704 F. App'x 1, 6 (2d Cir. 2017) ("[Defendants] can act with personal motivation while being part of—and acting in furtherance of—an enterprise"); *see also Dickson v. Microsoft Corp.*, 309 F.3d 193, 205 (4th Cir. 2002) ("'Where, as here, the defendants were knowing participants in a scheme . . . , the fact that their motives were different from or even in conflict with those of the other conspirators is immaterial.'" (alterations adopted) (quoting *Duplan Corp. v. Deering Milliken Inc.*, 594 F.2d 979, 982 (4th Cir. 1979))); 2 Scott Martin &

Irving Scher, *Antitrust Adviser* § 11:32 (5th ed. 2015) ("[A] participant in a conspiracy is still a conspirator, regardless of the participant's reason for joining the conspiracy."). For example, one individual might join a drug cartel to boost his reputation, while his friend joins to protect his physical safety, but the two can still work together to accomplish the cartel's goals, such as gaining territory, selling drugs, and competing against rival cartels. It is no different here, where Defendants wanted to secure Trump's grip on power for different reasons, but they all worked toward that shared goal. *See* ¶¶ 71-80.

The Trump Campaign argues that Russia's motivations were "complex and evolving, but centered on that nation's overarching geopolitical objectives," and then lists a litany of various incentives for Russia's conduct. Campaign Br. 16. The Campaign impermissibly relies on material outside of the Complaint to build this narrative. Even aside from this defect, however, the Trump Campaign fails to explain how Russia's purported incentives are at odds with its work in securing Trump's grip on the Presidency, an outcome Putin has admitted he preferred, ¶ 76. For instance, the Trump Campaign argues that Russia's aims included damaging American confidence and undermining a future Clinton presidency. Campaign Br. 16. But there is no contradiction in working to secure Trump's grip on power and in damaging American confidence and undermining the Western alliances in the process. To the contrary, Trump repeatedly made statements denigrating Western alliances, ¶ 75, and it is more than plausible that, to serve its interests, Russia would—and did—go to extraordinary lengths to help elect Trump.[9]

[9] That Russia's hacking, as the Campaign claims, began before Trump became the Republican front-runner is irrelevant: The Complaint alleges the AIF Enterprise began by March or June 2016, ¶ 272, and Russia's illegal activity before this time is irrelevant to the question of whether Russia worked to aid Trump's election as part of the AIF Enterprise alleged.

The Trump Campaign's arguments regarding WikiLeaks's motivations fare no better. First, the Trump Campaign claims Assange's and WikiLeaks's only goal was to undermine Secretary Clinton based on personal vendettas, and the Campaign concludes that these vendettas do not line up with Russia's objective to "undermin[e] the US-led liberal democratic order." Campaign Br. 17; *see also* WikiLeaks 1st Br. 15. But this again conflates an individual defendant's personal motivation for entering into the AIF Enterprise with the common purpose of that Enterprise. The Trump Campaign ignores the numerous allegations of Assange's and WikiLeaks's contacts and coordination with Trump Associates and Russia in aid of Trump's election. *See, e.g.*, ¶¶ 149-151, 161-65, 170-76. For instance, on July 6, 2016, WikiLeaks instructed Guccifer 2.0 to send additional hacked material because "we think trump has only a 25% chance of winning against hillary . . . so conflict between bernie and hillary is interesting." ¶ 150. This alone suffices to plausibly allege Assange and WikiLeaks worked to secure Trump's grip on power.

The remainder of the Trump Campaign's arguments suffer from similar defects, and should be rejected. The Campaign concedes that its own stated goal was to elect Trump in 2016 and 2020, but the Campaign dismisses this as the purpose of every political campaign. Campaign Br. 18. Of course, that the Trump Campaign's purpose may be routine does nothing to diminish that it did, in fact, have this purpose. The Campaign claims that the Agalarovs' personal motivation of "curr[ying] favor with Russian officials" was not shared by other Defendants, *id.*, while ignoring allegations that this motivation led the Agalarovs to arrange the Trump Tower meeting to provide incriminating "documents and information" that "would be very useful to [Trump.]" ¶ 133. Similarly, Mifsud's desire to advance Russia's interests led him to meet with Papadopoulos to try to set up a meeting between Russian officials and the Trump Campaign to share "thousands of emails" to aid the Campaign. ¶¶ 94-95.

The Campaign then correctly notes that the Complaint alleges "the Trump Associates . . . stood to benefit financially and professionally from a Trump Presidency," ¶ 80, and concedes that "it is hardly surprising that the Defendants who worked for or are related to President Trump would desire his election." Campaign Br. 18-19. That it is "hardly surprising" that the Trump Associates worked to secure Trump's grip on power only bolsters its plausibly. And that the Trump Associates had "an inherently personal" motivation or that these Defendants' personal motivations did not line up with those of other Defendants, Campaign Br. 19, is irrelevant.[10]

Finally, several Defendants also contend that an enterprise's common purpose must be "unlawful," and that there is nothing unlawful about seeking to secure Trump's grip on power. Campaign Br. 19-21; Papadopoulos Br. 18. This argument rests on outdated case law. In 2009, the Supreme Court in *Boyle* held that "an association-in-fact enterprise is simply a continuing unit that functions with a common purpose." 556 U.S. at 948. After *Boyle*, the Second Circuit clarified that members of an AIF Enterprise can associate together for a *lawful* purpose. In *D'Addario*, for instance, the Second Circuit found that individuals associated with an Estate were an association-in-fact, and had "a shared purpose" that was not only lawful, but "*prescribed by law*: settling the Estate by paying off its debts and distributing its assets among the heirs." 901 F.3d at 103 (emphasis added). In any event, the Complaint alleges that Defendants' overarching aim was to "us[e] illegal means to secure Trump's grip on the Presidency," an inherently unlawful goal. ¶ 272.

[10] Corsi's effort to aid Stone, Trump's long-time confidant and partner, ¶ 58, in obtaining information from WikiLeaks, ¶ 162, and his subsequent effort to conceal this aid, ¶¶ 170, 215, support an inference that Corsi shared the conspirators' common goal of securing Trump's grip on power.

(2) Relationships (Responding to: Agalarov Br. 14, Campaign Br. 21-23, Papadopoulos Br. 18)

The Trump Campaign and Papadopoulos claim that the Complaint fails to allege relationships amongst the Defendants sufficient to establish an AIF Enterprise. Campaign Br. 21-23; Papadopoulos Br. 18-19. Relationships may be inferred from individuals' "repeated and overlapping participation in the pattern of racketeering activity." *United States v. Veliz*, 623 F. App'x 538, 542 (2d Cir. 2015); *see also Boyle*, 556 U.S. at 946 (AIF enterprise may be "inferred from the evidence showing that persons associated with the enterprise engaged in a pattern of racketeering activity," or, in other words, "the evidence used to prove the pattern of racketeering activity and the evidence establishing an enterprise 'may in particular cases coalesce'" (citation omitted)). "[T]here is no need for a [RICO] plaintiff to prove that each conspirator had contact with all other members." *Schwartz v. Lawyers Title Ins. Co.*, 970 F. Supp. 2d 395, 404-05 (E.D. Pa. 2013).

The large bulk of the Complaint shows the Defendants' extensive relationships with one another, including their repeated communications and meetings, their repeated and overlapping participation in a pattern of racketeering activity, and their willingness to work together to commit non-predicate crimes that furthered their racketeering goals. *See, e.g.*, ¶¶ 93-95 (Papadopoulos, on behalf of the Campaign, met repeatedly with Mifsud to obtain damaging information regarding Clinton and to set up a meeting between Russian officials and the Trump Campaign); ¶¶ 132-138 (Trump Tower meeting, which was set up by Agalarovs on behalf of Russia to share damaging information regarding Clinton, was attended by Kremlin-linked individuals and multiple Trump Associates); ¶¶ 149-151 (WikiLeaks requested additional stolen information from Russia); ¶¶ 159-176 (Trump Associates secretly communicated with Russian agents and WikiLeaks as they strategically released stolen DNC documents); ¶ 173 (WikiLeaks and Trump, Jr. committed a non-

predicate crime by hacking into an anti-Trump political action committee website). The Complaint further alleges continued communications and joint efforts amongst Trump Associates, agents of the Russian government, and WikiLeaks after the 2016 election, including efforts geared toward protecting one another and Trump's grip on power. *See, e.g.*, ¶¶ 69, 206-36 (Agalarovs maintained frequent contact with Trump, Jr. and tried to set up a second meeting between Russian agent and Trump transition team; Kushner attempted to establish secret backchannel to the Russian government; Stone continued communicating with WikiLeaks; Trump Associates communicated with one another, obstructed justice, and otherwise covered up their contacts; Russia continued hacking computer networks of Trump critics; WikiLeaks released Amazon document compromising security of DNC's AWS servers; etc.). It is difficult to square these allegations of consistent, repeated, and overlapping contacts and coordination amongst the Defendants with the Trump Campaign's assertion that the Complaint alleges only "a series of isolated connections" and "isolated interactions." Campaign Br. 22.

The Campaign next claims that the AIF Enterprise analysis requires Plaintiff to establish that the enterprise had a "framework" or "structure" and to allege the details of that "framework" or "structure." Campaign Br. 21-22; *see also* WikiLeaks 1st Br. 14. The Supreme Court has made clear that "an association-in-fact enterprise is simply a continuing unit that functions with a common purpose." *Boyle*, 556 U.S. at 948. An AIF Enterprise need not have "a leader or hierarchy," nor does it require that its "participants ever formulate[] any long-term master plan or agreement." *Id.* at 941; *see also United States v. Burden*, 600 F.3d 204, 215 (2d Cir. 2010) ("We are mindful that 'the existence of an association-in-fact is oftentimes more readily proven by what it does, rather than by abstract analysis of its structure.'" (quoting *United States v. Coonan*, 938 F.2d 1553, 1559 (2d Cir. 1991))); *Equinox Gallery Ltd. v. Dorfman*, 306 F. Supp. 3d 560, 571

(S.D.N.Y. 2018) (a complaint need not "allege that a particularly organized structure existed" and "the existence of an enterprise may be inferred from evidence showing that persons associated with the enterprise engaged in a pattern of racketeering activity"). Further, "[m]embers of the group need not have fixed roles; different members may perform different roles at different times," "[t]he group need not have a name [or] regular meetings[,]" and "nothing in RICO exempts an enterprise whose associates engage in spurts of activity punctuated by periods of quiescence." *Boyle*, 556 U.S. at 948.

Here, the Complaint alleges a loose organizational structure with general roles for different Defendants: as a general matter, Russia's role in the enterprise was to use its military infrastructure to conduct hacking activity, WikiLeaks's and Assange's role in the enterprise primarily was to use WikiLeaks's platform to disseminate the hacked materials and provide advice about the best materials to steal and the optimal timing for the thefts, and the Trump Associates' and Agalarovs' role in the enterprise primarily consisted of coordinating with both Russia and WikiLeaks to time the disseminations, amplify their effect, and solicit and encourage additional hacking to aid the common purpose of securing Trump's grip on power. *Cf. Equinox*, 306 F.3d at 571 (nature of relationships in AIF Enterprise sufficiently alleged where complaint described how a defendant's name, reputation, and resources were key to the enterprise's success). This loose structure is more than sufficient under the expansive standard set forth by the Supreme Court.

The Campaign next claims that some of the Complaint's allegations "rely on unsupported assertions that certain individuals were 'agents'" of the Russian government, and that additional facts are required to establish "an agency relationship." Campaign Br. 22-23. Papadopoulos offers a similar protest. Papadopoulos Br. 19. There are several problems with this line of reasoning. First, neither the Campaign nor Papadopoulos provides any authority suggesting that a formal

agency relationship between Russia and any Russian individuals is required to support Plaintiff's RICO allegations; in fact, common sense suggests it would be sufficient if the Russian actors were formal agents *or* separate co-conspirators who were willing to do Russia's bidding.[11] Second, it cannot be disputed that, at the very least, the GRU Operatives (who are Russian military officers) are actual agents of the Russian government. ¶ 49, 114. Finally, the allegations that Mifsud, the Agalarovs, Veselnitskaya, Deripaska, Kilimnik, and others were either acting on behalf of or coordinating with Russia are robust and supported by extensive citations, including the determinations of U.S. intelligence agencies. *See, e.g.*, ¶ 94 (Mifsud met with high-ranking Russian officials who, through him, transmitted information regarding hacked Clinton emails to Papadopoulos); ¶ 133 (Agalarovs explicitly set up the Trump Tower meeting as "part of Russia and its government's support for Mr. Trump—helped along by Aras and Emin [Agalarov]") ¶¶ 137-38 (Veselnitskaya represented Russia's interests at the Trump Tower meeting, later calling herself an "informant" for the Russian government); ¶ 67 (FBI determined Kilimnik maintained ties with Russian intelligence during 2016 campaign); ¶¶ 66, 152 (Deripaska is a Putin-allied Russian oligarch). These allegations are more than sufficient either to show that these individuals were Russia's co-conspirators or to raise an "inference that some sort of agency relationship

[11] The authority the Campaign relies on applied the agency concept in contexts that are not even arguably analogous to those here. *See RSM Prod. Corp. v. Fridman*, 643 F. Supp. 2d 382, 401-02 (S.D.N.Y. 2009) (discussing agency requirement to exercise personal jurisdiction under N.Y.C.P.L.R. § 302(a)); *Cannon v. Douglas Elliman, LLC*, 2007 WL 4358456, at *5 (S.D.N.Y. Dec. 10. 2007) (finding labor law and breach of contract claims inadequately pled because plaintiffs failed to allege defendants were their employers). Even in these inapplicable cases, the court stated that "Plaintiffs are *not* required to establish the existence of a formal agency relationship." *RSM*, 643 F. Supp. 2d at 401 (emphasis added) (quotation marks and citation omitted).

existed." *Amusement Indus., Inc. v. Stern*, 693 F. Supp. 2d 327, 344 (S.D.N.Y. 2010) (quotation marks omitted).

(3) Longevity (Responding to: Campaign Br. 23)

The Trump Campaign contends that the AIF Enterprise lacks sufficient longevity.[12] Campaign Br. 23. Not so. An AIF Enterprise only has to exist for sufficient time "to permit the[] associates to pursue the enterprise's purpose." *Boyle*, 556 U.S. at 946; Campaign Br. 23. Thus, "there is no hard-and-fast time period for satisfaction of the longevity prong." *United States v. Pierce*, 785 F.3d 832, 838 (2d Cir. 2015). The Campaign argues that the AIF Enterprise "did not exist long enough to play any role in the conduct that facilitated *every* theft and *every* disclosure at issue here." Campaign Br. 23. This argument simply ignores large portions of the Complaint alleging that Defendants committed predicates—including information theft and disclosure—from March 2016 until September 2018, which helped secure Trump's grip on power both before and after the election. *See* ¶¶ 277-304. Moreover, it is irrelevant that some of the Defendants may have committed hacking-related crimes before the enterprise formed. The key point is that, *after* the enterprise formed, it persisted for a period of time sufficient to permit Defendants to pursue their goal of securing Trump's grip on power though a pattern of racketeering activity.

(4) Separateness (Responding to: Campaign Br. 24)

Finally, the Trump Campaign claims that the Complaint fails to allege an AIF Enterprise that is separate from the pattern of racketeering activity alleged. The Supreme Court has held that an enterprise is "an entity separate and apart from the pattern of activity in which it engages." *United States v. Turkette*, 452 U.S. 576, 583 (1981). In other words, the "enterprise must also have

[12] The AIF Enterprise requirement of "longevity" is distinct from the "continuity" element required to show a "pattern" of racketeering activity. *See infra* Section IV.A.3.c.

some element of existence beyond the predicate acts committed." *Hemmerdinger Corp. v. Ruocco*, 976 F. Supp. 2d 401, 413 (E.D.N.Y. 2013) (quotation marks and citation omitted).

Here, the Complaint alleges that Defendants were part of a group that worked together to engage in both predicate *and* non-predicate acts to further their goal of securing Trump's grip on power. For instance, in September 2016, WikiLeaks gave Trump, Jr. a password to an anti-Trump political action committee website, which Trump, Jr. later used. ¶ 173. Additionally, while he was on the campaign trail, Manafort gave internal Trump Campaign polling data to Kilimnik. ¶ 91. After the election, WikiLeaks sent tweets undermining the Special Counsel's investigation, ¶ 221, while Russia used multiple fake social media accounts to paint Mueller as corrupt, ¶ 212, and the Trump Campaign denied any contact with Russians, ¶¶ 208-209. *See Equinox Gallery Ltd.*, 306 F. Supp. 3d at 573 (concealing a scheme to "ensure the enterprise's survival" supports the existence of an AIF Enterprise). These coordinated actions and communications—which are independent of the pattern of racketeering activity—show that the AIF Enterprise had "some element of existence beyond the predicate acts committed." *City of New York v. Chavez*, 944 F. Supp. 2d 260, 270 (S.D.N.Y. 2013).

3. *Pattern of Racketeering Activity (Responding to Campaign Br. 26-33, Papadopoulos Br. 9-11, 12-14, 15-16)*

A "pattern of racketeering activity" requires "at least two acts of racketeering activity, one of which occurred after the effective date of [the RICO statute] and the last of which occurred within ten years (excluding any period of imprisonment) after the commission of a prior act of racketeering activity." 18 U.S.C. § 1961(5). "[A]cts of racketeering activity" include "any act which is indictable under any of the [enumerated statutory provisions]." 18 U.S.C. § 1961(1). These "acts of racketeering activity" are also called "predicate acts," or simply "predicates." *H.J. Inc. v. Nw. Bell Tel. Co.*, 492 U.S. 229, 236 (1989). Defendants committed four types of predicates:

economic espionage (18 U.S.C. § 1831), theft of trade secrets (18 U.S.C. § 1832), obstruction of justice (18 U.S.C. § 1503), and tampering with a witness, victim, informant, or piece of evidence (18 U.S.C. § 1512).

To show that the racketeering activity constitutes a "pattern," the allegations must also show (1) that the racketeering predicates are related, and (2) that they amount to or pose a threat of continued criminal activity. *H.J. Inc.*, 492 U.S. at 239. "For analytic purposes these two constituents of RICO's pattern requirement must be stated separately, though in practice their proof will often overlap." *Id.*

a. Predicates (Responding to: Agalarov Br. 6-9, Campaign Br. 26-31, Kushner Br. 5-8, Papadopoulos Br. 9-11, 12-14, Stone Br. 21-23, WikiLeaks 1st Br. 15-16)

(1) Trade Secret Statutes (Responding to: Campaign Br. 26-31)

Title I of the Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839, prohibits the theft of trade secrets in two main contexts: theft for the benefit of a foreign government, § 1831, and theft for pecuniary gain, § 1832. These two subsections are RICO predicate offenses. *See* 18 U.S.C. § 1961(1). As explained in detail in Section IV.D, below, the DNC possessed trade secrets within the meaning of the Economic Espionage Act, § 1839, which were stolen by Russia pursuant to a conspiracy with the other Defendants. Defendants also conspired to disseminate the DNC's trade secrets. Through these theft and dissemination conspiracies, Defendants committed offenses under both § 1831 and § 1832 as part of their pattern of racketeering activity.

(a) 18 U.S.C. § 1831 (Responding to: Campaign Br. 26-30, Papadopoulos Br. 9-11, Stone Br. 22,)

Each Defendant committed economic espionage in violation of 18 U.S.C. § 1831(a)(5). Section 1831 "prohibits the theft of trade secrets by individuals with the knowledge and intent that the theft will benefit 'any foreign government, foreign instrumentality, or foreign agent.'" *United*

States v. Aleynikov, 737 F. Supp. 2d 173, 180 (S.D.N.Y. 2010) (quoting 18 U.S.C. § 1831(a)). In addition to penalizing one who "steals," or "appropriates, takes, carries away" a trade secret, the statute also penalizes anyone who "transmits, delivers, sends, mails, communicates, or conveys a trade secret," §§ 1831(a)(1)-(2), or anyone who conspires to do the same. § 1831(a)(5). The DNC alleges that Defendants violated this conspiracy provision by conspiring to steal the DNC's trade secrets, and by conspiring to "transmit, deliver, send, communicate, or convey" them to the public, knowing that Defendants' conduct would benefit Russia, a foreign government (a conclusion that was readily apparent to all of the conspirators in light of the Russian government's extensive and sustained involvement in these illegal activities).

The key issue before the Court is whether those conspiracy allegations are plausible. *Twombly*, 550 U.S. at 556, 549, 557. A plaintiff can plead a plausible conspiracy through direct or "*circumstantial* evidence." *Anderson News, L.L.C.*, 680 F.3d at 183-84 (internal quotation marks omitted). The Complaint contains both.

(i) Evidence Against the Trump Campaign, the Trump Associates, and the Agalarovs (Responding to: Campaign Br. 26-30, Papadopoulos Br. 9-11, Stone Br. 22)

The Complaint presents a wealth of evidence that the Trump Campaign, Trump Associates, and the Agalarovs conspired with Russia to steal and disseminate the DNC's trade secrets in violation of § 1831(a)(5). In the run-up to the 2016 election, the Trump Associates were in frequent contact with Russian agents, meeting repeatedly in person and following up with phone calls, texts, emails, tweets, and Skype sessions. The individuals representing Russia in these conversations were not diplomats making formal presentations about Russian policy objectives; they were intelligence agents, oligarchs, and other "unofficial sources." ¶ 95. *See Gelboim v. Bank of Am. Corp.*, 823 F.3d 759, 781 (2d Cir. 2016) (frequent communications between individuals who do

not ordinarily have a reason to talk to one another is probative of a conspiracy). Members of the Trump Campaign knew that their Russian contacts were spies and other intermediaries acting on behalf of Russia, but continued to engage and work with them to achieve the goals of the conspiracy. *See, e.g.*, ¶¶ 67, 91 (describing Manafort and Gates's extensive contacts with Kilimnik, whom they knew as "the guy from the GRU"); ¶¶ 161-67 (describing Stone's frequent contacts with Guccifer 2.0, the online persona who publicly claimed responsibility for hacking the DNC's systems, after the DNC publicly announced that hackers were Russian intelligence officers). There is no obvious, lawful explanation for those interactions. *See Twombly*, 550 U.S. 544, 567 (considering whether there was an "obvious" lawful explanation for alleged conspirators' conduct).

The Trump Associates' discussions with Russian agents are particularly probative of a conspiracy because they were shrouded in secrecy: As explained in more detail below, several members of the Trump Campaign went to elaborate and illegal lengths to conceal the existence or nature of their communications with Russian officers, including false statements, destruction of evidence, and witness intimidation. *See United States v. Apple Inc.*, 952 F. Supp. 2d 638, 693 n.59 (S.D.N.Y. 2013), *aff'd*, 791 F.3d 290 (2d Cir. 2015) (defendants' denials that they spoke to one another, "in the face of overwhelming evidence to the contrary, strongly supports a finding of consciousness of guilt"); *In re Ethylene Propylene Diene Monomer (EPDM) Antitrust Litig.*, 681 F. Supp. 2d 141, 176 (D. Conn. 2009) ("[E]vidence of the frequent and friendly communications between the defendants and the secrecy of their meetings is sufficient to allow a reasonable jury to infer that the defendants participated in an unlawful . . . conspiracy.").

Over the course of the Trump Associates' conversations with Russian agents, Defendants forged an agreement to steal the DNC's intellectual property, including trade secrets, and use it to

support Trump's candidacy. On April 18, 2016, Papadopoulos met with Mifsud and an individual connected to the Russian Ministry of Foreign Affairs. ¶ 94. That same day, Russia launched "a pervasive cyberattack on DNC servers," which included a large-scale theft of trade secrets. ¶¶ 101-06. Less than a week later, Mifsud met Papadopoulos in London and delivered a message from the Russian government: Russia had secured "'thousands of emails' that could harm Hillary Clinton's presidential campaign." ¶ 94. Taken together, these interactions suggest that Russia was reporting on the progress of its cybercrimes to Papadopoulos, apprising him of stolen materials that could be helpful to the Trump Campaign, and giving him an opportunity to tell them whether the Campaign wanted more. In May 2016, Papadopoulos happily told an Australian diplomat about the stolen materials. ¶ 99. And, more importantly, Russia continued stealing documents—including trade secrets—from the DNC.

By early June, Russia had stolen a trove of DNC materials. Before disseminating a single page, however, Russia and the Agalarovs reached out to Trump, Jr. with a message: the Russian government wanted to provide "sensitive information" and "documents" to the "Trump [C]ampaign," as just one "part of" Russia's larger efforts to "support . . . Mr. Trump"; Trump, Jr. gleefully accepted Russia's help, exclaiming, "if it's what you say I love it." ¶¶ 133-34. Trump, Jr. received Russia's message while he was "on the road," but he followed up with Emin Agalarov to arrange a "meeting at which Russians would provide the Trump Campaign with damaging information about the Democratic nominee." ¶ 135. On June 6 and 7, the two men had several phone calls to discuss the upcoming meeting, presumably setting a rough agenda. *Id.* Trump, Jr. also discussed the upcoming meeting with senior members of the Trump Campaign, including Manafort, Gates, and Kushner. ¶ 219. The carefully planned meeting took place two days later, on June 9, 2016, in Trump Tower. ¶ 137. "The Trump Campaign was represented by Trump's inner-

circle: Trump, Jr., Kushner, and Manafort. Representing Russia's interests were Agalarov publicist Rob Goldstone, Kremlin-connected Russian lawyer Natalia Veselnitskaya[], Agalarov business associate Irakyl Kaveladze, lobbyist Rinat Akhmestshin, and a translator." *Id.*

Just as Papadopoulos's meeting with Russian contacts was immediately followed by hacking activity, the Trump Tower meeting was followed the very next day by Russia hacking into a DNC server nicknamed "Raider," which backed up other DNC servers (including those storing trade secrets). ¶¶ 143-44. And less than a week after the Trump Tower meeting, Russia began disseminating the documents it stole from the DNC, including trade secrets. ¶ 148. *See Speakes v. Taro Pharm. Indus., Ltd.*, No. 16-cv-08318 (ALC), 2018 WL 4572987, at *2 (S.D.N.Y. Sept. 24, 2018) (inferring the existence of a conspiracy from suspicious conduct that occurred "[r]ight after" the defendants met).

Because there is evidence that the agenda at the Trump Tower meeting included a discussion of sensitive documents and data in Russia's possession, the attendees prepared for the meeting extensively (as they would for an important strategy discussion), the meeting occurred after Russia had stolen a wide array of documents but before it disseminated any of them, and the meeting was immediately followed by renewed hacking and the dissemination of DNC documents, it is reasonable to infer that: (a) Russia used the meeting to tell members of the Trump Campaign about the documents it had stolen from the DNC, including trade secrets; and (b) members of the Campaign blessed a plan in which Russia would continue stealing similar documents and disseminate the documents it already had to the public. *Cf. United States v. Martin*, 228 F.3d 1, 12 (1st Cir. 2000) (a jury could infer that the Defendants agreed to steal trade secrets where one defendant sent trade secrets to a second defendant, and the second defendant encouraged her to continue).

These inferences are bolstered by several other events described in the Complaint. For example, "[a]t a press conference on July 27, 2016, after commenting extensively on . . . materials that were stolen from the DNC['s] servers" (including trade secrets), Trump urged Russia to steal additional documents from Secretary Clinton's personal email server, calling out: 'Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing.'" ¶ 158. That same day, the GRU "attempted—for the first time—to hack email accounts used by Secretary Clinton's personal office[,]" *id.*, that is, the precise accounts that Trump had urged them to find.

In addition, Manafort, who served as chairman of the Trump Campaign, gave Kilimnik "polling data . . . related to Trump's 2016 Campaign," and then concealed that transaction from the Special Counsel. ¶ 231. It is difficult to see why a high-ranking member of the Trump Campaign would give campaign polling data to a known Russian spy unless the Campaign wanted to help Russia gauge the effectiveness of its plan to interfere in the 2016 election.

Moreover, GRU officers using the screenname Guccifer 2.0 stayed in close contact with Stone, asking for feedback on how they could be most helpful, *after* Russia had been publicly linked to the theft of Democratic documents. *See* ¶¶ 167, 177-79. In September 2016, the GRU operatives asked Stone for his reaction to a "turnout model" that the GRU had stolen from another Democratic Party target. ¶ 179. After Stone suggested that he was not impressed, *see id.*, Russia took snapshots of the virtual servers that housed key pieces of the DNC's analytics infrastructure—its "most, important, valuable, and highly confidential tools," which could have "provided the GRU with the ability to see how the DNC was evaluating and processing data critical to its principal goal of winning elections," ¶ 180. This was not the only time Stone provided help or encouragement to the GRU: On another occasion, GRU officers using the screenname Guccifer

2.0 sent Stone a thank-you note after disseminating a collection of stolen Democratic documents. ¶ 165.

Finally, both during and after the election, members of the Trump Campaign repeatedly acted to cover up Russia's responsibility for stealing and disseminating the DNC's trade secrets. As the Second Circuit has explained, a defendant's "concealment of a conspiracy" can "support an inference" that the defendant was one of the conspirators. *See United States v. Freeman*, 498 F.2d 569, 576 (2d Cir. 1974). That inference is especially appropriate here, where the allegations of concealment are bolstered by specific allegations of meetings, communications, support and encouragement, and other indicia of conspiracy.

The cumulative weight of all this evidence (and the other evidence presented in the Complaint) is more than enough to raise a plausible inference that Defendants agreed to steal Democratic Party materials—including the DNC's trade secrets—and use them to secure Trump's grip on power. *Cf. Uni-Sys., LLC v. United States Tennis Ass'n, Inc.*, 350 F. Supp. 3d 143, 177 (E.D.N.Y. 2018) (holding that a plaintiff adequately pleaded a conspiracy to steal trade secrets by alleging that one of the defendants "'orchestrated' and 'encouraged and facilitated' the acquisition of [specific] trade secrets"). It is also sufficient to raise an inference that Defendants knew their conduct would benefit Russia's objectives, as required by 18 U.S.C. § 1831(a)(5). *See United States v. Liew*, 856 F.3d 585, 597 (9th Cir. 2017) (explaining that "any manner of benefit" to a foreign nation is sufficient to trigger liability under 18 U.S.C. § 1831) (internal quotation marks omitted).[13] To hold otherwise would impose an unreasonable investigative burden on plaintiffs,

[13] Because Defendants conspired with Russia to steal the DNC's trade secrets, they clearly knew that the conspirators' conduct would give a foreign government access to information. *See* Campaign Br. 30.

who can rarely find smoking-gun evidence of a conspiracy before discovery. *See generally Anderson News, L.L.C.*, 680 F.3d at 170.

Rather than contesting the existence of a conspiracy to steal and disseminate trade secrets, several of the Trump Associates and the Agalarovs argue that the DNC has not plausibly alleged that they participated in the conspiracy. Not so. Even in the summary judgment context (which places a significantly higher evidentiary burden on plaintiffs), "once a conspiracy is shown, only slight evidence is needed to link another defendant with it." *Apex Oil Co. v. DiMauro*, 822 F.2d 246, 257 (2d Cir. 1987) (quoting *United States v. Wilkinson*, 754 F.2d 1427, 1436 (2d Cir. 1985)). "The defendant's participation in a single transaction can, on an appropriate record, suffice to sustain a charge of knowing participation in an existing conspiracy." *Santos*, 541 F.3d at 73-74. Alternatively, the defendant's participation can "be inferred from circumstantial evidence of the defendant's status in [a criminal] enterprise or knowledge of the wrongdoing." *New York Dist. Council of Carpenters Pension Fund v. Forde*, 939 F. Supp. 2d 268, 282 (S.D.N.Y. 2013) (internal citations and quotation marks omitted).

The Agalarovs and the Trump Associates all participated in at least one transaction that connects them to the conspiracies to steal and disseminate the DNC's trade secrets. The Agalarovs helped arrange the Trump Tower meeting and sent Trump, Jr. a message that they wanted to "help[] along" Russia's efforts to support the Trump Campaign. ¶ 133. Similarly, Kushner was heavily involved in the Trump Tower meeting, attending both a preparation session with other high-ranking members of the Campaign and the Trump Tower meeting itself. It is also plausible to infer—based on Kushner's "status" as the director of the Campaign's data-driven efforts—that he knew about the efforts to steal and disseminate trade secrets. *New York Dist. Council of Carpenters Pension Fund*, 939 F. Supp. 2d at 282; *see also Glob. Imaging Acquisitions Grp., LLC v.*

Rubenstein, No. 14-C-0635, 2015 WL 5618803, at *2 (E.D. Wis. Sept. 24, 2015) (finding it plausible that a company's "principals" knew about and approved of an employee's plan to steal trade secrets).[14] At the same time, as explained in detail above, Papadopoulos was responsible for coordinating with Russian operatives before and during the April 2016 hacks on the DNC's computer systems. *See* Papadopoulos Br. 9-11; ¶¶ 94-99, 101-06. And Stone coordinated with Russian agents before and during the September hacks.

Stone further argues that his conduct allegedly pertained to the theft of Podesta's emails, which he insists were not taken from DNC servers. Stone Br. 6, 8-13, 22. But it is reasonable to infer that Stone was part of a broader conspiracy to steal and disseminate Democratic information. Stone communicated with and assisted GRU agents posing as Guccifer 2.0 during the same periods of time when the GRU was working to attack the DNC's computer networks. For instance, the Complaint alleges that on August 14, 2016, Stone began communicating with GRU operatives posing as Guccifer 2.0. ¶ 167. Similarly, on September 9, 2016, Stone communicated with GRU operatives about further hacking endeavors. ¶ 179. Less than two weeks later, CrowdStrike, a cybersecurity firm working with the DNC, discovered that the GRU had accessed the DNC's cloud-computing service. ¶ 180. This is the type of suspicious timing that courts have found to be probative of a conspiracy. *See Speakes*, No. 16-cv-08318 (ALC), 2018 WL 4572987, at *2.

---

[14] Kushner and Papadopoulos argue that they could not commit a predicate offense by aiding and abetting the theft of trade secrets. Kushner Br. 5, Papadopoulos Br. 11-12. See also Campaign Br. 26-27. While they are wrong on this front, *Stochastic Decisions, Inc. v. DiDomenico*, 995 F.2d 1158, 1168 (2d Cir. 1993) (recognizing that a Defendant can commit a predicate by aiding and abetting); *4 K & D Corp. v. Concierge Auctions, LLC*, 2 F. Supp. 3d 525, 537 (S.D.N.Y. 2014) (Koeltl, J.) (same), the DNC does not allege that Kushner or Papadopoulos were liable for aiding and abetting the theft of trade secrets; rather, it alleges that they conspired to steal trade secrets, in violation of the plain text of 18 U.S.C. § 1831(a)(5) and § 1832(a)(5).

Thus, at this stage in the litigation, there is ample evidence that each Defendant joined both the conspiracy to steal and the conspiracy to disseminate the DNC's trade secrets. In other words, there is ample evidence that each Defendant committed multiple counts of economic espionage. *See* 18 U.S.C. § 1831(a)(5).

(ii) Evidence against WikiLeaks

The Complaint presents both direct and circumstantial evidence that WikiLeaks joined the Defendants' conspiracy to steal and disseminate the DNC's trade secrets by June 2016. *See Mayor & City Council of Baltimore, Md. v. Citigroup, Inc.*, 709 F.3d 129, 136 (2d Cir. 2013) (direct evidence of a conspiracy includes recorded conversations in which defendants agree to a course of conduct). On June 22, 2016—eight days after the DNC announced that Russian intelligence agents hacked their systems and one day after agents using the screenname Guccifer 2.0 posted a batch of stolen DNC trade secrets online—WikiLeaks asked Guccifer 2.0 to "[s]end any new material [stolen from the DNC] here for us to review and it will have a much higher impact than what you are doing." ¶¶ 148-49. Construed in the light most favorable to the DNC, this was a request for known Russian intelligence agents to steal additional trade secrets from the DNC, and then give them to WikiLeaks to disseminate, because WikiLeaks had a keener understanding of the best way to use stolen materials to boost Trump's electoral prospects. Guccifer 2.0 apparently accepted the offer, and attempted to send stolen DNC documents to WikiLeaks in late June 2016. *Id.*

WikiLeaks's next interaction with Guccifer 2.0 confirms this interpretation of events. On July 6, 2016, WikiLeaks instructed Guccifer 2.0 to send "anything [H]illary related" in the next two days because the Democratic National Convention was approaching, and the convention would give Secretary Clinton an opportunity to "solidify [B]ernie supporters behind her." ¶ 150. WikiLeaks suggested that it could improve Trump's "25% chance of winning" by using materials from Guccifer 2.0 to sow "conflict between [B]ernie and [H]illary." Guccifer 2.0 responded

"ok . . . I see," ¶ 150, and then implemented WikiLeaks's plan, transmitting a large cache of stolen DNC trade secrets so that WikiLeaks could disseminate them on the eve of the Democratic National Convention, ¶¶ 154, 156.

On September 20, 2016, WikiLeaks gave Trump, Jr. a password to access an anti-Trump political action committee website. ¶ 173. By giving Trump, Jr. a password (to an opposition website) that he had no right to use, WikiLeaks demonstrated its willingness to work directly with members of the Trump Campaign as they used stolen information to secure Trump's grip on power.

Additionally, in the summer and fall of 2016, WikiLeaks regularly spoke with Trump. Jr. and Stone. ¶¶ 167, 170-76. In some of those conversations, Stone requested that WikiLeaks release particular stolen Democratic documents. ¶ 171. And following many of the conversations, Stone correctly forecasted WikiLeaks's releases of stolen Democratic documents. ¶¶ 170, 172-75. To round out this picture of guilt, Stone worked hard to conceal his contacts with WikiLeaks, going so far as to destroy email evidence and lie to Congress. *See infra* Section IV.A.3.a.(2). Taken together, this evidence strongly suggests that WikiLeaks coordinated with the Trump Associates to determine the best time to release stolen DNC documents, including trade secrets, to the public.

The Complaint also alleges enough facts to suggest that WikiLeaks knew its conduct would benefit Russia. On June 14, 2016, the DNC publicly announced that Russian intelligence agencies had hacked into its computer systems. ¶ 146. Thus, when Guccifer 2.0 began disseminating materials stolen from those computer systems, WikiLeaks was on notice that Guccifer 2.0 was affiliated with Russian intelligence. Nevertheless, WikiLeaks advised Guccifer 2.0 on the best way to achieve their mutual goals.

(b) 18 U.S.C. § 1832 (Responding to: Campaign Br. 26-31, Papadopoulos Br. 11)

The Complaint also alleges that each Defendant committed theft of trade secrets in violation of 18 U.S.C. § 1832(a)(5). As relevant here, section 1832, which prohibits the theft of trade secrets generally, penalizes "whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret" knowingly "steals," or "appropriates, takes, carries away," or "transmits, delivers, sends, mails, communicates, or conveys a trade secret," or conspires to do the same. 18 U.S.C. § 1832(a)(1), (2), (5).

As noted above, the DNC adequately alleges that Defendants conspired to steal and disseminate the DNC's trade secrets. And, as will be explained further below, Defendants knew that the DNC's trade secrets were "related to a product or service used in or intended for use in interstate or foreign commerce." *See infra* Section IV.D. They also knew that their conduct would economically benefit both themselves and Russia, to the DNC's detriment, as it saved the Defendants the time and expense of conducting costly opposition research. Consequently, the DNC has properly alleged a conspiracy to steal trade secrets, in violation of 18 U.S.C. § 1832(a)(5).[15]

[15] Citing cases from 1998 and 2010, Kushner and Papadopoulos contend that violations of 18 U.S.C. §§ 1831-32 are not RICO predicates. Their authority, however, is outdated. Sections 1831 and 1832 were added to the list of RICO predicates on May 11, 2016. *See* Defend Trade Secrets Act of 2016 (DTSA), Pub. L. No. 114-153, 130 Stat 376 (May 11, 2016) (codified at 18 U.S.C. § 1836, et seq.). Because Defendants stole and disseminated trade secrets at least once after that date, Plaintiff can hold them liable for all of the thefts and disseminations they committed (both before and after May 11, 2016). *See* 18 U.S.C. § 1961(5) ("[A] 'pattern of racketeering activity' requires at least two acts of

(2) Obstruction of Justice Statutes (Responding to Papadopoulos Br. 12-14)

The RICO enterprise did not end when Trump won the 2016 election. ¶ 206. Instead, the Defendants actively worked to conceal their illegal coordination to ensure that Trump maintained his grip on power. *Id.* As the House of Representatives, the Senate, the FBI, and the Justice Department all began investigating Russia's involvement in the 2016 election, the co-conspirators attempted to thwart these proceedings by, among other things, criminal obstruction of justice and witness tampering. ¶¶ 206, 211. In doing so, various Defendants violated two predicate statutes: 18 U.S.C. § 1503 (influencing or injuring officer or juror generally) and 18 U.S.C. § 1512 (tampering with a witness, victim, or an informant).

Papadopoulos argues that 18 U.S.C. §§ 1503 and 1512 do not qualify as RICO predicates because neither statute provides a private cause of action. Papadopoulos Br. 12. This peculiar argument is belied by the plain text of the RICO statute, which lists both 18 U.S.C. §§ 1503 and 1512 as predicate offenses. 18 U.S.C. § 1961(1); *see also European Cmty. v. RJR Nabisco, Inc.*, 764 F.3d 129, 137 (2d Cir. 2014) (recognizing 18 U.S.C. § 1512 as a predicate offense in a civil RICO case) *rev'd and remanded on other grounds*, 136 S. Ct. 2090, 195 L. Ed. 2d 476 (2016);

racketeering activity, *one of which occurred after the effective date of this chapter . . . .*" (emphasis added)); *Snowden v. Lexmark Int'l, Inc.*, 237 F.3d 620, 624-25 (6th Cir. 2001) (suggesting that a defendant can be liable for a substantive RICO offense if he violates a newly added predicate statute at least *once* after the RICO statute has been updated). Defendants have forfeited any argument to the contrary. In any event, many of the most damaging thefts and disclosures of DNC documents (as well as the meetings to orchestrate those thefts and disclosures) happened after May 11, 2016. *See, e.g.*, ¶¶ 123-29, 132-95. Those acts—and the conspiracies to commit them—unquestionably qualify as predicates.

Kim v. Kimm, 884 F.3d 98, 103 (2d Cir. 2018) (recognizing 18 U.S.C. § 1503 as a predicate offense in a civil RICO case).

(a) 18 U.S.C. § 1503 (Responding to: Papadopoulos 12-14, Stone Br. 22-23)

Under 18 U.S.C. § 1503, it is unlawful to interfere with an officer or juror, or otherwise "endeavor[] to influence, obstruct, or impede[] the due administration of justice," either "corruptly or by threats of force." This last provision—known as the "Omnibus Clause"—"serves as a catchall," providing broad protection to judicial proceedings. *United States v. Aguilar*, 515 U.S. 593, 598 (1995). "In order to convict for obstruction of justice under the [O]mnibus [C]lause . . . , the government must establish (1) that there is a pending judicial or grand jury proceeding constituting the administration of justice, (2) that the defendant knew or had notice of the proceeding, and (3) that the defendant acted with the wrongful intent or improper purpose to influence the judicial or grand jury proceeding, whether or not the defendant is successful in doing so—that is, that the defendant corruptly intended to impede the administration of that judicial proceeding." *United States v. Quattrone*, 441 F.3d 153, 170 (2d Cir. 2006) (internal quotation marks and citation omitted). "[A] defendant's actions need not be successful to violate § 1503; it is enough that a defendant 'endeavors' to influence the due administration of justice." *United States v. Baum*, 32 F. Supp. 2d 642, 648 (S.D.N.Y. 1999); *United States v. Martinez*, 862 F.3d 223, 238 (2d Cir. 2017), *cert. denied sub nom. Fiorentino v. United States*, 138 S. Ct. 489, 199 L. Ed. 2d 370 (2017), *and reh'g denied sub nom. United States v. Rodriguez*, 888 F.3d 26 (2d Cir. 2018) (quoting § 1503(a)).

Moreover, "while the statutory term 'corruptly endeavors' requires intent, such intent may be inferred from proof that defendant had knowledge or notice that his corrupt actions would obstruct justice then actually being administered." *United States v. Buffalano*, 727 F.2d 50, 54 (2d

Cir. 1984). The defendant's conduct must also have a "nexus" to the proceeding at issue, which in this Circuit requires that the defendant's conduct must "only have the 'natural and probable effect of interfering with the due administration of justice.'" *United States v. Kumar*, 617 F.3d 612, 621 (2d Cir. 2010) (quoting *Aguilar*, 515 at 599). As the Supreme Court explained, "the act must have a relationship in time, causation, or logic with the judicial proceedings." *Aguilar*, 515 U.S. at 599.

The Omnibus Clause is interpreted expansively. "Courts in [the Second Circuit] have . . . given § 1503's omnibus clause a generally non-restrictive reading." *Kumar*, 617 F.3d at 620 (citing *United States v. Rosner*, 352 F. Supp. 915, 919 (S.D.N.Y. 1972) (noting that the omnibus clause "embraces the widest variety of conduct that impedes the judicial process"); *United States v. Solow*, 138 F. Supp. 812, 814 (S.D.N.Y.1956) (characterizing the omnibus provision as "all-embracing")). Thus, the Second Circuit has recognized that, where a judicial proceeding is likely to result from an agency investigation, the act of lying to the SEC or FBI in the course of an investigation can be encompassed by § 1503. *Kumar*, 617 F.3d at 621 n.8.

The DNC alleges that several Defendants violated the Omnibus Clause in their attempts to conceal their unlawful activities that occurred prior to the election, and to continue to secure Trump's grip on power. ¶¶ 291-294.

Papadopoulos. The DNC alleges that Papadopoulos endeavored to obstruct and impede the due administration of justice by lying to the FBI about his contacts with Mifsud and other Russian agents during a January 27, 2017 interview. ¶ 223. The DNC further alleges that he compounded these lies to the FBI on February 17, 2017 by deleting his Facebook account and scrubbing his other social media accounts, and on February 23, 2017 by changing his cell phone number in an attempt to hide his contacts. ¶ 223.

These allegations are sufficient to state a claim under 18 U.S.C. § 1503. First, Papadopoulos lied to the FBI during the course of an investigation that was likely to result in judicial proceedings, and was aware of that proceeding. At the time of Papadopoulos's January 27, 2017 interview, both the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence had already announced that they planned to investigate Russian attempts to interfere in the 2016 election. ¶ 211. The FBI questioned Papadopoulos about the same subject matter. Given the intense public scrutiny of the issue and his own guilt in collaborating with Russian agents, Papadopoulos should have expected that prosecutors would initiate formal judicial proceedings. This is sufficient to trigger § 1503's application under *Kumar*. 617 F.3d at 621 n.8 (§ 1503 applied where the defendant lied to the SEC in the course of an investigation and "knew that 'formal judicial proceedings' were not only possible or likely, but that the government intended to bring them," creating an inference that the defendant's statements would be presented to a grand jury).

Moreover, it is clear that Papadopoulos acted with "wrongful intent or improper purpose to influence" the proceeding. By deleting his Facebook account, scrubbing his social media accounts of connections to Mifsud and Russian agents, and changing his cell phone number, he took active steps to ensure that his lies to the FBI would not be undermined by his online activity. Thus, his wrongful intent can be inferred. *Cf. United States v. Sun Myung Moon*, 718 F.2d 1210, 1236 (2d Cir. 1983) (producing false documents to grand jury can be sufficient to show corrupt intent under § 1503).

Finally, Papadopoulos's lies to the FBI had the "natural and probable effect of interfering with the due administration of justice" because there was a clear connection in time and in logic with the judicial proceedings. *Aguilar*, 515 U.S. at 599. Where the FBI and both chambers of

Congress were all investigating the same unlawful conduct at the time of Papadopoulos' interview, a grand jury investigation was logically soon to follow.

Stone. The DNC alleges that Stone endeavored to obstruct justice by lying to the House Intelligence Committee and working to discredit Credico's testimony to the House Intelligence Committee. Stone spoke to the House Intelligence Committee on September 25, 2017. At this point, Special Counsel Robert Mueller had empaneled a grand jury. ¶ 211. In his testimony, Stone claimed he "never had any communications with any Russians or individuals fronting for Russians[] in connection with the 2016 presidential election," even though he later acknowledged that he met with a Russian national in May 2016 to obtain disparaging information about Secretary Clinton. ¶¶ 214, 224, 225. Stone also told the Committee he spoke to Assange only through Credico, despite the fact that: (a) he communicated with Assange through Corsi; and (b) he exchanged Twitter direct messages with WikiLeaks in 2016, when Assange was the only user of the WikiLeaks Twitter handle. ¶ 225. The DNC further alleges that Stone lied to the House Intelligence Committee about the identity of his backchannel to Assange, claiming that it was Credico, rather than Corsi. ¶¶ 215, 225.

After Stone told the House Intelligence Committee that he used Credico as his intermediary, the Committee subpoenaed Credico. ¶ 226. Fearing Credico would undermine his narrative, on November 30, 2017, Stone asked Corsi to write publicly about Credico to discredit or influence his testimony. *Id.* Credico stated that, around the time Stone was interviewed by the House Intelligence Committee, Stone told him to "just go along with" Stone's story. *Id.* Later, in early 2018, Credico began to dispute Stone's claim that he was an intermediary between Stone and WikiLeaks. ¶ 228. In response, Stone sent Credico a barrage of communications, including an offer to help pay Credico's legal expenses, in an attempt to convince Credico to stick to Stone's

narrative. *Id.* When Credico nevertheless threatened to dispute Stone's narrative, Stone threatened him, using explicit language. *Id.*

Here too, the DNC has adequately alleged a violation of § 1503. First, there was a grand jury proceeding pending, "constituting the administration of justice." *See, e.g., Quattrone*, 441 F.3d at 170; *United States v. Schwarz*, 283 F.3d 76, 105 (2d Cir. 2002). Stone was doubtless aware of the grand jury proceeding, as the acting Attorney General of the United States had publicly announced Mueller's appointment to serve as Special Counsel for the Department of Justice, with the authority to investigate whether Russia meddled in the 2016 U.S. presidential elections, and whether the Trump Campaign was involved in that meddling, and both Mueller's investigation and the empaneling of the grand jury were widely known. *See* ¶ 211 (describing Mueller's appointment and citing contemporaneous news articles in the New York Times and Wall Street Journal discussing the investigation and the grand jury). Stone's "wrongful intent or improper purpose to influence" the proceeding can be inferred from his clear knowledge that his story to Congress was false and likely to be probed. Specifically, once the House Intelligence Committee subpoenaed Credico, Stone took active measures to ensure that Credico would not contradict his testimony. ¶ 226. Further, and even more tellingly, Stone told Credico to "just go along with" his story to Congress. *Id.* These efforts to keep his lies to Congress intact clearly reflect his knowledge that these lies were likely to obstruct justice. Additionally, Stone worked actively to discredit Credico's testimony, creating a further obstruction to justice. ¶¶ 226, 228.

There is also a nexus between Stone's efforts to deceive Congress and the grand jury proceedings. At the time Stone began to lie to Congress, there were already at least four publicly known investigations of Russia's and the Trump Campaign's collaboration in the 2016 election, conducted by: the FBI, the House Intelligence Committee, the Senate Intelligence Committee, and

the Special Counsel. Because these were all proceeding at the same time and covering the same subject matter, it followed both logically and temporally that providing false testimony to one body would have the "natural and probable effect" of interfering with another body's investigation. Both by lying to Congress himself and by attempting to interfere with Credico's testimony, Stone endeavored to thwart the due administration of justice. *See United States v. Sampson,* 898 F.3d 287, 303 (2d Cir. 2018) (§ 1503 applies to an "inchoate endeavor to witness tamper").

Manafort. The DNC alleges that, on September 14, 2018, Manafort lied to Special Counsel Robert Mueller, telling Mueller that he would cooperate with the Special Counsel's investigation. ¶ 231. At this point, Mueller had empaneled a grand jury. ¶ 211. However, the DNC alleges, while pretending to tell Mueller everything he knew about Russian meddling in the 2016 election, Manafort in fact used the meetings with Mueller's team to funnel information about the investigation to Trump and to present false information to mislead the Special Counsel. ¶ 231. The DNC further alleges that Manafort lied about his repeated interactions with Kilimnik, which continued through at least April 2018, and that in particular, Manafort lied about sharing polling data related to Trump's campaign with Kilimnik in 2016. *Id.* The DNC further alleges that Manafort lied to the Special Counsel by saying that he did not have any communications with officials in the Trump administration, when in fact he communicated with Administration officials until May 26, 2018, if not later.

Here, there was a grand jury proceeding pending, "constituting the administration of justice." *See, e.g., Quattrone*, 441 F.3d at 170; *United States v. Schwarz*, 283 F.3d 76, 105 (2d Cir. 2002). Manafort knew about the grand jury proceeding, as he had already been indicted. *See* ¶ 231. And it is clear that Manafort acted with the intent to influence the grand jury proceeding. Manafort not only provided false testimony to Mueller with the knowledge that his testimony would obstruct

the grand jury's proceeding, but he also actively worked to share information about the investigation with Trump and his co-conspirators. Given Manafort's persistent lies to the Special Counsel, it is reasonable to infer that he was passing information to his co-conspirators with corrupt intent to help them align their stories. *See United States v. Langella*, 776 F.2d 1078, 1081 (2d Cir. 1985) (charges of false testimony to the grand jury and concealment of evidence support a conviction for obstruction of justice under § 1503). These allegations clearly support the conclusion that Manafort deliberately worked to conceal information from the grand jury. This also establishes the clear nexus between his conduct and the grand jury proceedings.

(b) 18 U.S.C. § 1512 (Responding to: Kushner Br. 5-6, Papadopoulos Br. 12-14, Stone Br. 22-23)

The DNC has also alleged that various Defendants violated provisions of 18 U.S.C. § 1512, "[t]ampering with a witness, victim, or an informant." Specifically, the DNC alleges that Stone influenced testimony in an "official proceeding" in violation of 18 U.S.C. § 1512(b)(1); that Corsi and Papadopoulos obstructed official proceedings in violation of 18 U.S.C. § 1512(c)(1); that Papadopoulos, Kushner, Stone, Trump, Jr., and Manafort obstructed official proceedings in violation of 18 U.S.C. § 1512(c)(2); and that Corsi and Stone conspired to obstruct official proceedings in violation of 18 U.S.C. § 1512(k).

"As used in section[] 1512," the term "official proceeding" encompasses— "(A) a proceeding before a judge or court of the United States…; (B) a proceeding before the Congress; [or] (C) a proceeding before a Federal Government agency which is authorized by law[.]" 18 U.S.C. § 1515(a)(1)(A)-(C). While "an official proceeding need not be pending or about to be instituted at the time of the offense," it still must be shown "that such a proceeding was reasonably foreseeable to the defendant." *Martinez*, 862 F.3d at 237 (quoting 18 U.S.C. § 1512(f)(1)).

(i) 18 U.S.C. § 1512(b)(1)

As relevant here, 18 U.S.C. § 1512(b)(1) prohibits "intimidat[ing]," "threaten[ing]," or "corruptly pursuad[ing] another person" so as to influence that person's official testimony. *United States v. Price*, 443 F. App'x 576, 581 (2d Cir. 2011). The Second Circuit "has defined 'corrupt persuasion' as persuasion that is 'motivated by an improper purpose.'" *Id.* (quoting *United States v. Gotti*, 459 F.3d 296, 343 (2d Cir. 2006)).

Stone. As explained in Section IV.A.3.a.(2)(a), above, the DNC alleges that, on September 25, 2017, Stone lied to the House Intelligence Committee. Stone claimed he "never had any communications with any Russians or individuals fronting for Russians[] in connection with the 2016 presidential election," even though he later acknowledged that he met with a Russian national in May 2016 to obtain dirt on Secretary Clinton. ¶¶ 214, 224, 225. Stone also told the Committee he spoke to Assange only through Credico, when in fact he communicated with Assange through Corsi and through the WikiLeaks Twitter handle. ¶ 225, *see also* ¶ 215. As further explained above, after Corsi threatened to reveal Stone's lies, Stone tried to incentivize Corsi to stick with his false narrative and then, when Corsi refused, Stone threatened Corsi.

Through these acts, the DNC alleges, Stone knowingly used intimidation, threats, and other corrupt methods to influence, delay, or prevent Credico's testimony in an official proceeding, in violation of 18 U.S.C. § 1512(b)(1). ¶ 300. Specifically, the DNC alleges that Stone knowingly attempted to use intimidation (threatening Credico using explicit language) with the intent to induce Credico to withhold testimony (urging Credico to lie to Congress to make sure that Credico's narrative did not contradict Stone's own false testimony) from an official proceeding (the House Intelligence Committee's investigation).

(ii) 18 U.S.C. § 1512(c)(1)

By contrast, 18 U.S.C. § 1512(c)(1) prohibits a defendant from "corruptly alter[ing], destroy [ing], mutilat[ing], or conceal[ing] a record, document, or other object, or attempt[ing] to do so, with the intent to impair the object's integrity or availability for use in an official proceeding." *United States v. Jahedi*, 681 F. Supp. 2d 430, 434 (S.D.N.Y. 2009) (quoting 18 U.S.C. § 1512(c)(1)). Section 1512(c)(1) also has a "nexus" requirement: "In order to establish a nexus, there must be a relationship between the defendant's actions and the official proceeding. In other words, an offender "must believe that his actions are likely to affect a particular, existing or foreseeable proceeding." *United States v. Persico*, 645 F.3d 85, 107 (2d Cir. 2011) (quoting *United States v. Kaplan*, 490 F.3d 110, 125 (2d Cir. 2007)). However, a plaintiff need not show "that a defendant's conduct is 'likely to affect' the official proceeding, or correspondingly, that the defendant have knowledge that his conduct is 'likely to affect' the official proceeding, in order to [state a claim] under 18 U.S.C. § 1512(c)(1)." *United States v. Ortiz*, 367 F. Supp. 2d 536, 542 (S.D.N.Y. 2005). Instead, the defendant only needs to engage in the prohibited conduct with the requisite intent.

Corsi. The DNC alleges that Defendant Stone told the House Intelligence Committee that his backchannel to Assange was Credico, rather than Corsi. ¶ 215. To maintain that story, Corsi deleted all of his incriminating email correspondence that predated October 11, 2016. Corsi deleted these incriminating emails between January 13, 2017 (the date that the House Intelligence Committee announced its investigation) and March 1, 2017. *Id.*

Through these acts, Corsi corruptly altered, destroyed, mutilated, or concealed a record, document, or other object with the intent to impair the object's integrity or availability for use in an official proceeding, in violation of 18 U.S.C. § 1512(c)(1). ¶ 296. Specifically, Corsi destroyed documents and records by deleting emails, and did so with the intent to make those documents

unavailable for use in the House Intelligence Committee's investigation—an "official proceeding" under 18 U.S.C. § 1515(a)(1)(B). *See United States v. Gadsden*, 616 F. App'x 539, 544 (4th Cir. 2015) (affirming a conviction under 18 U.S.C. § 1512(c)(1) where a defendant "deleted . . . email accounts with the intent to impair [an] investigation" into his own fraudulent scheme). The DNC has also alleged a direct "nexus" between Corsi's conduct and the official proceeding—namely, that the timing of Corsi's destruction of evidence shows he did so to prevent the discovery of those emails by the House Intelligence Committee.

Papadopoulos. As explained in Section IV.A.3.a.(2)(a), above, the DNC alleges that Papadopoulos lied to the FBI about his contacts with Mifsud and other Russian agents during a January 27, 2017 interview. ¶ 223. Papadopoulos compounded these lies to the FBI on February 17, 2017 by deleting his Facebook account and scrubbing his other social media accounts; and on February 23, 2017 by changing his cell phone number in an attempt to hide his contacts. ¶ 223.

Through these acts, Papadopoulos corruptly altered, destroyed, mutilated, or concealed a record, document, or other object with the intent to impair the object's integrity or availability for use in an official proceeding, in violation of 18 U.S.C. §1512(c)(1). ¶ 297. Specifically, he destroyed documents and records by deleting his Facebook account, and "altered" and "concealed" records by scrubbing his other social media accounts. He also "concealed" or attempted to conceal records by changing his cell number. He committed these acts shortly after lying to the FBI about his contacts with Mifsud and other Russian agents, and did so in an attempt to hide those contacts. Thus, he committed these acts "with intent to impair the document's availability for use" in the FBI's investigation—an "official proceeding" under 18 U.S.C. § 1515(a)(1)(C). *See Gadsden*, 616 F. App'x at 544 (affirming a conviction under 18 U.S.C. § 1512(c)(1) where defendant deleted

email accounts after being questioned by an FBI agent in an FBI investigation).[16] The DNC has also alleged a nexus between Papadopoulos' conduct and the official proceeding—namely, that he destroyed evidence shows he did so to prevent the discovery of those emails by the FBI.

(iii) 18 U.S.C. § 1512(c)(2)

For its part, "[s]ection 1512(c)(2) punishes anyone who 'corruptly . . . otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so.'" *United States v. Tairod Nathan Webster Pugh*, No. 1:15-CR-00116-NGG, 2015 WL 9450598, at *14 (E.D.N.Y. Dec. 21, 2015). "To state an offense under 18 U.S.C. § 1512(c)(2), the [plaintiff] must allege obstructive conduct, an official proceeding, and a relationship between the defendant's obstructive conduct and the official proceeding." *United States v. Ying Lin*, 270 F. Supp. 3d 631, 635 (E.D.N.Y. 2017). Like § 1512(c)(1), § 1512(c)(2) has a "nexus" requirement: "the defendant's conduct must 'have a relationship in time, causation, or logic with the judicial proceeding'; in other words, 'the endeavor must have the natural and probable effect of interfering with the due administration of justice.'" *Tairod*, 2015 WL 9450598, at *14 (quoting *United States v. Reich*, 479 F.3d 179, 185 (2d Cir. 2007)).

Papadopoulos. The DNC also alleges that Papadopoulos corruptly obstructed or impeded an official proceeding, in violation of 18 U.S.C. § 1512(c)(2). ¶ 298. The DNC has pleaded

[16] Papadopoulos argues that he has not engaged in a "pattern" of racketeering activity because the SAC does not allege that he engaged in any criminal activity. Papadopoulos Br. 15-16. But as described in detail above, the DNC alleges that, at the very least, Papadopoulos engaged in two separate but related courses of conduct: he served as a conduit between Russian contacts and the Trump Campaign in a conspiracy to steal the DNC's trade secrets under 18 U.S.C. §§ 1831 and 1832; and later, destroyed evidence to conceal these contacts from federal authorities, in violation of 18 U.S.C. §§ 1503 and 1512. This satisfies 18 U.S.C. § 1961(5).

"obstructive conduct" (*i.e.*, that Papadopoulos deleted and scrubbed his social media accounts); that there was "an official proceeding" (*i.e.,* the FBI investigation); and that there was a relationship between the two (*i.e.*, that Papadopoulos deleted and scrubbed his social media accounts "in an attempt to hide" the contacts about whom he lied to the FBI). *See Ying Lin*, 270 F. Supp. 3d at 635. Finally, the DNC alleges a nexus between Papadopoulos's conduct and the proceeding—namely, that Papadopoulos deleted and scrubbed his social media accounts to hide contacts, which had the "natural and probable effect" of interfering with the FBI's investigation into those contacts. *Tairod*, 2015 WL 9450598, at *14.

Kushner. The DNC alleges that Kushner provided a written statement to Congress claiming that he did not know what the Trump Tower meeting was going to be about. ¶ 219. The House Intelligence Committee Majority's report, however, concluded that Kushner, Trump, Jr., and Manafort attended the meeting "where they expected to receive . . . derogatory information on candidate Clinton from Russian sources." *Id.* In addition, before the Trump Tower meeting, Trump, Jr. forwarded to Kushner his emails with Goldstone with the subject line: "Russia - Clinton - private and confidential." *Id.* Finally, Trump's attorney, Rudy Giuliani, has stated that Kushner, Trump, Jr., Manafort, Gates, and Cohen conducted a preparatory meeting on June 7, 2016 before the Trump Tower meeting on June 9, 2016. *Id.* Kushner therefore knew what was on the agenda for June 9, and thus lied to Congress. *See id.*

In his written statement to Congress, Kushner also denied attempting to create a "secret backchannel" with the Russian government during a meeting with Russian ambassador Sergey Kislyak. ¶ 220. Kislyak, however, told his superiors that Kushner had proposed setting up a secret communications channel between the Trump transition team and Moscow, using Russian

diplomatic facilities that would bypass U.S. intelligence agencies. *Id.* This was another lie Kushner told to Congress.

Through these acts, the DNC alleges, Kushner corruptly attempted to obstruct or impede an official proceeding, in violation of 18 U.S.C. § 1512(c)(2). ¶ 299. Specifically, the DNC pleads that there was "obstructive conduct" (submitting false written testimony to Congress); that there was an "official proceeding" (the House Intelligence Committee investigation); that there was a relationship between the two (Kushner submitted false testimony as a witness in the official proceeding at issue); and that there was a nexus in that the natural and probable effect of Kushner's lies regarding his contacts with Russian was to interfere with Congress's investigation of those contacts.

Stone. The DNC also alleges Stone corruptly attempted to obstruct or impede an official proceeding, in violation of 18 U.S.C. § 1512(c)(2). Specifically, the DNC pleads "obstructive conduct" (attempting to induce Credico to lie to the House Intelligence Committee); an "official proceeding" (the House Intelligence Committee's investigation); a relationship between the two (Stone attempted to convince Credico, through persuasion and through threats, to lie to the House Intelligence Committee in order not to contradict Stone's own testimony); and an obvious nexus.

Trump, Jr. The DNC alleges that on September 7, 2017, Trump, Jr. testified before the Senate Judiciary Committee that no attendee of the Trump Tower meeting requested additional meetings or communications with members of the Trump Campaign, but this testimony was contradicted by subsequently released emails in which Goldstone, on behalf of Aras Agalarov, sought a second meeting between Veselnitskaya and the Trump transition team shortly after the election. ¶ 222. Thus, Trump, Jr. lied to the Senate Judiciary Committee. *See id.* Through these acts, the DNC alleges, Trump, Jr. corruptly attempted to obstruct or impede an official proceeding,

in violation of 18 U.S.C. § 1512(c)(2). ¶ 301. Specifically, the DNC pleads "obstructive conduct" (falsely testifying before the Senate Judiciary Committee); that there was an "official proceeding" (the Senate Judiciary Committee investigation); that there was a relationship between the two (Trump, Jr. falsely testified as a witness in the official proceeding at issue); and there was a nexus (the false testimony's natural and probable effect was to interfere with the Senate Judiciary Committee's investigation).

Manafort. As explained in Section IV.A.3.a.(2)(a), above, the DNC alleges that, on September 14, 2018, Manafort lied to Special Counsel Robert Mueller, telling Mueller that he would cooperate with the Special Counsel's investigation. ¶ 231. However, the DNC alleges, while pretending to tell Mueller everything he knew about Russian meddling in the 2016 election, Manafort in fact used the meetings with Mueller's team to funnel information about the investigation to Trump and to present false information to mislead the Special Counsel. *Id.* Manafort also lied about his repeated interactions with Kilimnik, which continued through at least April 2018, and that in particular, Manafort lied about sharing polling data with Kilimnik related to Trump's 2016 campaign. *Id.* The DNC further alleges that Manafort lied to the Special Counsel by saying that he did not have any communications with officials in the Trump administration, when in fact he communicated with Administration officials until May 26, 2018, if not later. *Id.*

Through these acts, the DNC alleges, Manafort corruptly attempted to obstruct or impede an official proceeding, in violation of 18 U.S.C. § 1512(c)(2). ¶ 302. Specifically, the DNC pleads "obstructive conduct" (lying to the Special Counsel and actively working to undermine the Special Counsel's investigation); that there was an "official proceeding" (the Special Counsel's investigation and the pending grand jury proceeding); that there was a relationship between the two (Manafort presented false information to Mueller and funneled information to Trump

specifically in order to mislead the Special Counsel and threaten his investigation); and a nexus (Manafort's conduct had the natural and probable effect of interfering with the Special Counsel's investigation).

(iv) 18 U.S.C. § 1512(k)

Finally, § 1512(k) states, "Whoever conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy." To allege a conspiracy under this section, a plaintiff must show: "(1) that an agreement existed" between the co-conspirators to commit the substantive offense; "(2) that [the co-conspirators] knew of this conspiracy; and (3) that they knowingly and voluntarily became a part of a conspiracy" to commit the offense. *United States v. Chujoy*, 207 F. Supp. 3d 626, 649 (W.D. Va. 2016), *aff'd sub nom. United States v. Edlind*, 887 F.3d 166 (4th Cir. 2018).

Corsi and Stone. As set forth in detail in Section IV.A.3.a.(2)(a), above, to maintain the false story Stone and Corsi concocted regarding their communications with Assange and hide contrary evidence from the House Intelligence Committee, Corsi deleted all of his incriminating email correspondence that predated October 11, 2016. The DNC also alleges that, later, fearing Credico would undermine Stone's false testimony to the House Intelligence Committee, on November 30, 2017, Stone asked Corsi to write publicly about Credico to discredit or influence his testimony. ¶ 226. These allegations set forth a conspiracy to "corruptly alter[], destroy[], mutilat[e], or conceal[] a record, document, or other object, or attempt[] to do so, with the intent to impair the object's integrity or availability for use in an official proceeding," as well as a conspiracy to corruptly attempt to obstruct or impede an official proceeding and "knowingly use[] intimidation, threats, and other corrupt methods to influence, delay, or prevent" Credico's testimony in an official proceeding, all in violation of 18 U.S.C. § 1512(k).

First, the DNC alleges that an agreement existed between Corsi and Stone to commit the offenses (Stone and Corsi concocted a false narrative and coordinated their suppression of evidence and testimony to the contrary). The DNC further shows that Corsi and Stone knew of this conspiracy (as they coordinated their obstructive activity in order to keep their testimonies consistent). Finally, the DNC shows that Corsi and Stone knowingly and voluntarily became part of the conspiracy (as Stone and Corsi took active, concrete steps to effectuate their plan).

b. Relatedness (Responding to: Kushner Br. 6-8; Papadopoulos Br. 14-15)

"Predicate crimes must be related both to each other (termed 'horizontal relatedness') and to the enterprise as a whole ('vertical related

ness')." *Reich v. Lopez*, 858 F.3d 55, 60-61 (2d Cir. 2017) (quoting *United States v. Cain*, 671 F.3d 271, 284 (2d Cir. 2012)). Kushner and Papadopoulos are the only defendants who challenge the relatedness of their predicate crimes, and their arguments are meritless.

(1) Horizontal Relatedness

Crimes are horizontally related when they "have the same or similar purposes, results, participants, victims, or methods of commission, or otherwise are interrelated by distinguishing characteristics and are not isolated events." *Reich*, 858 F.3d at 61 (quoting *H.J. Inc.*, 492 U.S. at 240). Kushner claims that he only committed one predicate—concealing the Trump Tower meeting in his security clearance application—and a predicate cannot be horizontally related to itself. Kushner Br. 6. As set forth above, the Complaint actually alleges that Kushner: (1) conspired to steal trade secrets in violation of 18 U.S.C. §§ 1831-32; (2) conspired to disseminate trade secrets in violation of 18 U.S.C. §§ 1831-32; and (3) attempted to obstruct or impede an official proceeding, by lying to Congress about his knowledge of the Trump Tower meeting and his attempt to create a "secret backchannel" with the Russian government. ¶¶ 219-

220. All of these crimes are horizontally related. As explained above, Kushner's and Papadopoulos's predicates involving the theft and dissemination of the DNC's trade secrets all involved the same "participants, victims, [and] methods of commission." *Reich*, 858 F.3d at 61. Many of the same "participants" were also involved in Kushner's attempts to impede Congress's investigation: Kushner's lies about the Trump Tower meeting were bolstered by false statements made by other Defendants, ¶¶ 217, 302 (Trump, Jr. lied to Congress regarding purpose of meeting); ¶ 227 (Veselnitskaya lied to Congress about whether she was representing the Russian government at the Trump Tower meeting). Furthermore, as noted above, all of Kushner's and Papadopoulos's predicates were done for the same "purpos[e]": securing Trump's grip on power. *Reich*, 858 F.3d at 61 (quoting *H.J.*, 492 U.S. at 240). Finally, horizontal relatedness may be presumed in a case like this one, where an AIF enterprise is primarily engaged in unlawful activity, *see infra* Section IV.A.3.c.(1), and the relevant predicates are vertically related to the enterprise, *see infra* Section IV.A.3.b.(2). *Reich*, 858 F.3d at 61.

(2) Vertical Relatedness

Kushner also challenges whether his predicate acts are vertically related. *See* Kushner Br. 7. Predicates are vertically related when "the defendant was enabled to commit the offense solely because of his position in the enterprise or his involvement in or control over the enterprise's affairs, or because the offense[s] related to the activities of the enterprise." *Reich*, 858 F.3d at 61 (quoting *United States v. Burden*, 600 F.3d 204, 216 (2d Cir. 2010)). There is no question that Kushner's and Papadopoulos's participation in the conspiracies to steal and disseminate the DNC's information were "related to the activities of the enterprise" because they were designed to help Trump secure his grip on the Presidency. Similarly, Kushner's lies to Congress and Papadopoulos's lies to the FBI concealed the activities of the enterprise so that Defendants could continue using illegal means to secure Trump's grip on power.

c. Continuity (Responding to: Agalarov Br. 10-14, Campaign Br. 31-33, Kushner Br. 7 & n.6, Stone Br. 21, 22, WikiLeaks 1st Br. 16, WikiLeaks 2nd Br. 3-6)

Each Defendant's predicate crimes must "amount to or pose a threat of continued criminal activity." *H.J. Inc.*, 492 U.S. at 239. In other words, each Defendant's predicates must have either "closed-ended or open-ended" continuity. *Reich*, 858 F.3d at 60. Predicates have "closed-ended continuity" if they "extend[ed] over a substantial period of time" in the past. *H.J. Inc.*, 492 U.S. at 242. By contrast, predicates have "open-ended continuity" if they "by [their] nature project[] into the future with a threat of repetition." *Reich*, 858 F.3d at 60 (citation omitted).

(1) Open-Ended Continuity

Each Defendant committed a string of predicate crimes with open-ended continuity. Open-ended continuity "can be established in several ways." *Reich*, 858 F.3d at 60 (citation omitted). For example, a plaintiff can show that the predicates "by their very nature" present a threat of future criminal activity. *Id.* Alternatively, a plaintiff can allege that the predicates were related to an "enterprise . . . [that] projects criminal activity into the future." *Id.*; *see also United States v. Aulicino*, 44 F.3d 1102, 1111 (2d Cir. 1995) (open-ended continuity may be established by "the acts of the defendant *or* the enterprise" (emphasis added)). In this case, the DNC has done both.

First, each Defendant's predicate acts "by their very nature" present a threat of future criminal activity. *Reich*, 858 F.3d at 60. When a predicate act is "inherently unlawful, such as murder or obstruction of justice," and serves an "inherently unlawful goal[]," there is a risk that the defendant will continue violating the law. *Aulicino*, 44 F.3d at 1111. The Defendants' conspiracies to steal and disseminate trade secrets were inherently unlawful. As the Supreme Court has long recognized, "[f]or two or more to confederate and combine together to commit or cause to be committed a breach of the criminal laws is an offense of the gravest character, sometimes quite outweighing, in injury to the public, the mere commission of the contemplated crime. It

involves deliberate plotting to subvert the laws, educating and *preparing the conspirators for further and habitual criminal practices*." *Pinkerton v. United States*, 328 U.S. 640, 644 (1946) (emphasis added). Moreover, in conspiring to steal and disseminate trade secrets, Defendants pursued an inherently unlawful goal: violating the substantive prohibitions in 18 U.S.C. §§ 1831-32. Similarly, Defendants' "obstruction of justice" predicates were inherently unlawful, *Aulicino*, 44 F.3d at 1111, and were undertaken in furtherance of an inherently unlawful goal—concealing the existence of the RICO enterprise so that Defendants could continue using illegal means to secure Trump's grip on power. *See United States v. Kaplan*, 886 F.2d 536, 542-43 (2d Cir. 1989) (defendants' "demonstrated willingness to facilitate corruption" was sufficient to find threat of continued activity). Thus, contrary to Defendants' suggestion, this case is distinguishable from *Westchester Cty. Indep. Party v. Astorino*, where the only alleged predicates were not "inherently unlawful." 137 F. Supp. 3d 586, 611 (S.D.N.Y. 2015).

In addition, Defendants were all participants in an enterprise that "projects criminal activity into the future." *Reich*, 858 F.3d at 60 (citation omitted). Defendants' AIF Enterprise was "primarily" engaged in theft of trade secrets, witness tampering, and destruction of evidence, which (as explained above) are inherently unlawful. *Id.* And while the Trump Campaign was "primarily" pursuing lawful aims, committing RICO predicates was a "regular way" that members of the Campaign did business. *Id.*

Moreover, regardless of whether the enterprise is the AIF Enterprise or the Trump Campaign, members of the enterprise have expressed a willingness to continue committing crimes to secure Trump's grip on power. *See Beauford v. Helmsley*, 865 F.2d 1386 (2d Cir. 1989) (en banc), *vacated and remanded*, 492 U.S. 914, *adhered to on remand*, 893 F.2d 1433 (2d Cir. 1989) (onetime commission of a crime was sufficient to show open-ended continuity where there was a

basis to infer that similar crimes would occur in the future); *DeFalco v. Bernas*, 244 F.3d 286, 324 (2d Cir. 2001) (open-ended continuity sufficiently pled where defendants "had no intention of stopping once they met some immediate goal"). After the election, Defendants stayed in close communication, and even established new secret channels that they could use to continue committing crimes. *See, e.g.*, ¶ 207 (the day that Trump worn the election, WikiLeaks sent a private message to Stone on Twitter: "Happy? We are now more free to communicate."),[17] ¶ 220 (Kushner attempted to create secret backchannel to the Russian government and then lied to Congress to conceal it). Defendants have also been helping one another in suspicious ways. For example, WikiLeaks just months ago published stolen material that threatens the safety of the DNC's electronic systems. ¶ 235. And Russia continues to engage in hacking activity targeting Trump's political opponents. For instance, in August 2017, the GRU attempted to hack into the computer network of Democratic Senator Claire McCaskill, a longtime critic of Trump, Russia, and WikiLeaks. ¶ 232. This and other ongoing illegal activity led senior U.S. national security and intelligence officials in August 2018 to characterize the threat of Russian interference in U.S. domestic politics as "real" and "continuing," with FBI Director Chris Wray noting that "[t]his threat is not going away." ¶ 234. Thus, the racketeering activity in this case, unlike the racketeering activity in *Westchester Cty. Indep. Party*, does not have an "intended and foreseeable endpoint." 137 F. Supp. 3d at 611.

In the face of the overwhelming evidence of open-ended continuity, Defendants attempt to fracture their ongoing criminal conspiracy into two pieces: one before the election and one after. Relying on out-of-circuit authority, several Defendants argue that their post-election obstruction

[17] WikiLeaks's claim that this secret communication "demonstrates the *opposite* of a cover-up" is baffling. WikiLeaks 2nd Br. 5-6. In any event, the Court must draw inferences in Plaintiff's favor.

and witness-tampering cannot be used to support open-ended continuity because it was merely an attempt to cover up the underlying illegal acts committed during the 2016 election and unrelated to the theft of trade secrets. Agalarov Br. 13-14; Campaign Br. 32; Stone Br. 21-23; WikiLeaks 2nd Br. 4-5. This argument ignores that the obstruction-related acts took place against a backdrop of the suspicious activities described in the previous paragraph. Viewing all of Plaintiff's allegations as a whole (as the Court must), it is reasonable to infer that Defendants' obstruction and witness-tampering conduct is geared toward protecting the enterprise to allow their scheme to continue, particularly during the 2020 election when Trump's grip on political power will be threatened most acutely. *See Pension Ben. Guar. Corp.*, 712 F.3d at 732 ("[I]t is well-settled that a complaint must be read as a whole, not parsed piece by piece to determine whether each allegation, in isolation, is plausible." (quotation marks and citation omitted)). Where, as here, "the successful accomplishment of [the purposes of the underlying conspiracy] necessitate concealment," obstruction-related conduct furthers the goals of the enterprise, and can be considered part of the enterprise's criminal activities. *See United States v. Hennings*, No. 95-CR-0010A, 1997 WL 714250, at *4 (W.D.N.Y. Oct. 20, 1997) (quoting *United States v. Grunewald*, 353 U.S. 391 (1957)); *see also United States v. Millar*, 79 F.3d 338, 344-45 (2d Cir. 1996) (robbery and subsequent concealment of the proceeds may be part of the same conspiracy); *United States v. Napout*, No. 15-CR-252, 2017 WL 4685089, at *5 (E.D.N.Y. Oct. 17, 2017) (evidence of obstruction was "admissible to show that Defendants and their co-conspirators attempted to prevent the detection of their criminal activities as part of a broader pattern of conspiratorial conduct"); *United States v. Potamitis*, 739 F.2d 784, 787 (2d Cir. 1984) ("The question whether the proof establishes a single or multiple conspiracies is an issue of fact 'singularly well-suited to resolution by the jury.'").

(2) Closed-ended Continuity

In the alternative, the Complaint also alleges closed-ended continuity for Trump, Jr., Manafort, Kushner, and Stone. "A party alleging a RICO violation may demonstrate continuity over a closed period by proving a series of related predicates extending over a substantial period of time." *H.J. Inc.*, 492 U.S. at 242. Although the Second Circuit generally requires that predicate crimes be committed for two years to establish closed-ended continuity, this is not "a bright-line requirement." *Spool v. World Child Int'l Adoption Agency*, 520 F.3d 178, 184 (2d Cir. 2008) (internal citations omitted); *accord Reich*, 858 F.3d at 60; *see also GICC Capital Corp. v. Tech. Fin. Grp., Inc.*, 67 F.3d 463, 468 (2d Cir. 1995) (noting that "[p]eriods of 19 or 20 months . . . have been held sufficient to support a finding of continuity" (internal quotation marks omitted)). Other relevant factors include the number and variety of predicate acts, the number of participants and victims and the presence of separate schemes. *Kriss v. Bayrock Grp., LLC*, No. 10 Civ. 3959, 2016 WL 7046816, at *15 (S.D.N.Y. Dec. 2, 2016) (citing *Kalimantano BmbH v. Motion in Time, Inc.*, 939 F. Supp. 2d 392, 412 (S.D.N.Y. 2013)).

Here, Trump, Jr., Manafort, Kushner, and Stone all committed a variety of predicate crimes for well over a year. *See* ¶¶ 219, 222, 228, 231, 277-303. Additionally, the number of alleged participants in the predicate acts (dozens of individuals working on behalf of Russia, an international organization and its principal, a presidential campaign and at least six of its employees or affiliates), the number of victims (Plaintiff, dozens of its employees, donors, and affiliates, and various other Democratic Party targets), and the number and variety of predicate acts (dozens of predicate acts spanning economic espionage, theft of trade secrets, obstruction of justice, and witness tampering) further support a finding of closed-ended continuity. *See Kriss*, 2016 WL 7046816, at *15-16.

4. *Injury (Responding to: Campaign Br. 33-37, Papadopoulos Br. 19)*

To survive a motion to dismiss, a RICO plaintiff must allege that it suffered an "*actual*, quantifiable injury" to its "business or property." *Kerik v. Tacopina*, 64 F. Supp. 3d 542, 560 (S.D.N.Y. 2014) (Koeltl, J.) (internal quotation marks omitted) (emphasis added); 18 U.S.C. § 1964(c). The Campaign and Papadopoulos argue that the DNC failed to do so. Campaign Br. 33-37; Papadopoulos Br. 19. However, consistent with RICO's requirement, the Complaint alleges three concrete losses that the DNC suffered when the Defendants conspired to misappropriate—and did misappropriate—the DNC's trade secrets. Each one of these losses (by itself) is sufficient to support the DNC's civil RICO claims.

First, in taking the DNC's trade secrets, GRU agents damaged the DNC's computer systems so badly that the DNC had to "repair and replace all of [its] computer hardware and software, telephone and telephone systems, and back-up systems." ¶ 254. Defendants do not dispute that the DNC suffered an "actual, quantifiable injury" to its property when its computer and phone systems were destroyed. *Kerik*, 64 F. Supp. 3d at 560. Nor do they contest that the DNC suffered an injury to its business when it had to pay consultants to determine how badly Defendants compromised its computer systems and what kind of repairs would be required. *See* ¶ 254.

Second, Defendants took the DNC's trade secrets without permission and without paying for them. *See, e.g.*, ¶¶ 36-37. Courts have repeatedly recognized that when a defendant steals a plaintiff's property, or otherwise prevents the plaintiff from using her property as she wishes, the plaintiff suffers a cognizable injury to her "business or property." 18 U.S.C. § 1964(c); *see, e.g., Bascunan v. Elsaca*, 874 F.3d 806, 824 (2d Cir. 2017) (recognizing that a defendant caused a RICO injury when he "physically stole[]" the plaintiff's property (emphasis omitted)); *Chevron Corp. v. Donziger*, 833 F.3d 74, 135 (2d Cir. 2016) (finding "no serious question" that the plaintiff "suffered injury in its business or property" when it could not "us[e] or dispos[e] of [its] property

as [it] wishe[d]"). The Trump Campaign nonetheless argues that the theft of the DNC's trade secrets does not constitute a RICO injury because the Defendants did not sell the secrets to anyone else. Campaign Br. 36. But Defendants cannot escape liability simply because they stole the DNC's property and kept it for themselves. *See Bascunan*, 874 F.3d at 824 (finding a RICO injury despite the fact that the defendant kept the plaintiff's property). The mere act of taking a plaintiff's property without permission or payment contravenes the plaintiff's property rights and deprives the plaintiff of revenue to which it is entitled. In other words, stealing injures a plaintiff's business or property.

Third, and contrary to Defendants' suggestion, the Complaint alleges that Defendants disseminated the trade secrets that they stole from the DNC. *See, e.g.*, ¶¶ 148, 156. Because these trade secrets derived value from their secrecy, they were worth less after Defendants shared them with the public. *See, e.g.*, *id.* For example, once the DNC's strategy documents became public, they had to develop new strategies so that their rivals would not anticipate their every move. *See id.* Impairing the value of the DNC's trade secrets constitutes an injury to business or property within the meaning of § 1964(c). *See Bartlett v. Bartlett*, No. 3:17-CV-00037(JPG)(SCW), 2017 WL 5499403, at *6 (S.D. Ill. Nov. 16, 2017) (holding that the defendant caused an injury to business or property by compromising the privacy of a trade secret).

Defendants argue that impairing the value of a trade secret is not a cognizable RICO injury because it is not sufficiently concrete or quantifiable. Not so. Expert appraisers are entirely capable of determining the value of a trade secret both before and after it has been exposed to the public; the DNC is entitled to collect the difference between these figures. *See, e.g., BondPro Corp. v. Siemens Power Generation, Inc.*, 463 F.3d 702, 707 (7th Cir. 2006) (noting that a trade secret can have "market value" that allows an expert to estimate "damages from the destruction of the

secret"). To hold otherwise would shield racketeers from civil liability for stealing or destroying property so long as the property they take or ruin is somewhat unique (such as a building, a parcel of land, or a piece of art). There is no reason to impose such a bizarre gloss on § 1964(c).[18]

Defendants also note that several of the other injuries described in the Complaint—such as an impaired ability to connect with voters—are not injuries to "business or property" within the meaning of the civil RICO statute. *See* Campaign Br. 36, Papadopoulos Br. 19-20. While that is true, *Westchester Cty. Indep. Party*, 137 F. Supp. 3d at 615, Defendants nowhere contest that those injuries can support the award of actual or punitive damages under the *non-RICO* causes of action in the Complaint. *Cf. Empire Merchs., LLC v. Reliable Churchill LLLP*, 902 F.3d 132, 143 (2d Cir. 2018) (explaining that RICO imposes unusually strict injury and causation requirements at the pleadings stage).

5. *Causation (Responding to: Agalarov Br. 14-15, Campaign Br. 33-36, Papadopoulos Br. 19)*

The Complaint adequately alleges that the Defendants' RICO violations caused the injuries described above. To satisfy RICO's causation requirement, a plaintiff must allege that "*at least*

[18] At this stage in the litigation, it is enough that the value of Plaintiff's trade secrets can be quantified by an expert appraiser. There is no need for Plaintiff to provide the results of an appraisal in the Complaint—rather than during discovery. *See Safe Sts. All. v. Hickenlooper*, 859 F.3d 865, 885 (10th Cir. 2017) (holding that "neither § 1964(c)'s text nor any ruling by the Supreme Court" establishes a "novel statistical evidentiary pleading standard" that would require a plaintiff to calculate the exact value of his or her damages before filing a complaint); *cf. Ideal Steel Supply Corp. v. Anza*, 652 F.3d 310, 324 (2d Cir. 2011) (holding that a complaint alleging a violation of 18 U.S.C. § 1962(a) was sufficiently detailed because it stated that the plaintiff lost a "substantial" amount of "sales, profits, and local market share").

one" predicate crime proximately caused one of her injuries.[19] *4 K & D Corp. v. Concierge Auctions,* LLC, 2 F. Supp. 3d 525, 543 (S.D.N.Y. 2014) (Koeltl, J.) (emphasis added); *D'Addario*, 901 F.3d at 96 (internal citations and quotation marks omitted). In other words, the plaintiff must allege some sort of "direct" relationship between the relevant predicate crime and the corresponding injury she sustained. *Empire Merchs., LLC*, 902 F.3d at 140 (quoting *Holmes v. Sec. Inv'r Prot. Corp.*, 503 U.S. 258, 268 (1992)). In deciding whether the causal chain between the defendants' misconduct and the plaintiff's injury is sufficiently direct, courts consider: (a) the difficulty of determining how much the defendants' predicate(s)—as opposed to "other factors"—injured the plaintiff; and (b) whether other victims of the defendants' scheme "would be better suited as plaintiffs." *Empire Merchs., LLC*, 902 F.3d at 141. These considerations confirm that Defendants' predicate crimes proximately caused the injuries described above.

a. Difficulty of Determining Causation

In this case, the DNC can easily show that Defendants' predicate crimes—as opposed to "other factors"—caused its injuries. *Empire Merchs., LLC*, 902 F.3d at 141.

(1) Damage to the DNC's Computer Systems

As explained in the Complaint, all of the Defendants committed predicate offenses when they "conspired with" Russia and WikiLeaks to steal the DNC's trade secrets, and Russia took steps "to effect the object of the conspiracy." 18 U.S.C. §§ 1831(a)(5), 1832(a)(5). These steps included installing malware to take the DNC's trade secrets, and actually taking those trade secrets. *See, e.g.*, Am. Compl. ¶¶ 101-08, 180. It is clear that the installation of malware—as opposed to

[19] Thus, contrary to Papadopoulos's suggestion, it is irrelevant that some of the Defendants' predicates harmed the DNC, while others did not. Papadopoulos Br. 14.

other factors—caused damage to the DNC's computer system, such that the DNC had to repair or replace the systems containing the malware. *See Empire Merchs., LLC*, 902 F.3d at 141.

The Trump Campaign argues that it is too difficult to identify which parts of the DNC's computer systems were damaged by hacking that the Russian government undertook on its own in July 2015, and which parts were damaged by hacking activities undertaken in furtherance of Defendants' conspiracy to steal trade secrets. But forensic experts can distinguish between the Russian intelligence agency (nicknamed Cozy Bear) that broke into DNC computers in July 2015, and the agency (known as the GRU and nicknamed Fancy Bear) that broke into DNC systems between April and September of 2016 to steal trade secrets. *See* ¶¶ 114-18. These experts were able to determine that the GRU infected several DNC computers and servers *after* Defendants formed their conspiracy. *See* ¶¶ 105 ("Between April and June of 2016, the GRU gained access to at least 33 DNC computers and the DNC's email server."), 143-44 (on June 10, 2016, GRU agents installed malware onto a DNC backup server nicknamed Raider), 180 (explaining that GRU agents broke into the DNC's AWS servers in September 2016). Thus, the GRU's hacking activity pursuant to the conspiracy caused at least some injuries to the DNC's computer systems.

By contrast, the Agalarovs argue that their misconduct cannot be the definitive cause of the damage to the DNC's computer systems because they did not personally hack into those systems (rather, they left the hacking to their co-conspirators). *See* Agalarov Br. 14-15. Papadopoulos similarly argues that his individual conduct did not cause the DNC injury. Papadopoulos Br. 19. Contrary to these Defendants' suggestion, however, nothing in RICO's proximate cause requirement abrogates the general principle that civil defendants can be liable for damages that flow directly from their co-conspirators' actions. *See, e.g.*, *Frydman v. Verschleiser*, 172 F. Supp. 3d 653, 671 (S.D.N.Y. 2016) (Koeltl, J.) (holding that civil RICO defendants could

be liable for their co-conspirators' wire fraud); 54 Causes of Action 2d 603 ("Proximate cause in a civil conspiracy case will not be defeated merely because the damages were not caused by the present defendants in the suit so long as some coconspirator—even a nonparty—engaged in the unlawful conduct in furtherance of the conspiracy.").

(2) Theft of the DNC's Trade Secrets

It is also clear (to the point of being tautological) that Defendants' conspiracies to steal the DNC's trade secrets in violation of 18 U.S.C. §§ 1831(a)(5) and 1832(a)(5)—as opposed to "other factors"—caused the theft of the DNC's trade secrets. *See Empire Merchs., LLC*, 902 F.3d at 141. The Defendants all agreed to take the DNC's trade secrets, and pursuant to the agreement, the GRU actually took the trade secrets. That taking constituted an injury to the DNC's business or property. *See supra* Section IV.A.4. It is difficult to imagine a simpler causal chain.

(3) Diminished Value of Trade Secrets

The Complaint alleges that, in addition to conspiring to steal the DNC's trade secrets, each Defendant conspired to publish those trade secrets in violation of 18 U.S.C. § 1831(a)(5) and 18 U.S.C. § 1832(a)(5); consistent with that conspiracy, Russia and WikiLeaks in fact published the DNC's trade secrets online. It is clear that this conspiracy to publish the DNC's trade secrets—as opposed to other factors—reduced the value of those secrets. *See Empire Merchs., LLC*, 902 F.3d at 141. As explained in the Complaint, the DNC's trade secrets derived value from their confidentiality. *See, e.g.*, ¶¶ 148, 156. Thus, the moment they were exposed to the general public, they "necessarily" became less valuable. *Empire Merchants, LLC*, 902 F.3d at 143.

b. No Better Plaintiffs

In considering whether Defendants proximately caused the DNC's injuries, the Court should also consider whether there are any "more directly injured victims who would be better suited as plaintiffs." *Empire Merchs., LLC*, 902 F.3d at 141. No such victims exist. As the owner

of the property that was damaged and stolen by Defendants, the DNC is the most direct victim of the Defendants' RICO violations, and is in the best position to remedy them. *See Empire Merchs., LLC*, 902 F.3d at 144 (suggesting that the State of New York was the most immediate victim of the defendants' RICO violation because the defendants effectively stole property (in the form of tax revenue) from the state).

B. Plaintiff Adequately Alleges Defendants Violated the RICO Conspiracy Statute (Responding to: Agalarov Br. 15-16, Campaign Br. 37-38, Kushner Br. 10-11, Papadopoulos Br. 20-21)

Defendants can be held liable for violating the RICO conspiracy statute if: (1) they agreed to facilitate a plan in which one or more of them would "violate RICO's substantive provisions," *Cofacredit, S.A. v. Windsor Plumbing Supply Co.*, 187 F.3d 229, 244 (2d Cir. 1999) (internal quotation marks omitted); *see also Salinas v. United States*, 522 U.S. 52, 64-65, (1997); and (2) pursuant to that agreement, one of them committed a predicate act that harmed the DNC, *Hecht v. Commerce Clearing House, Inc.*, 897 F.2d 21, 25 (2d Cir. 1990). If these conditions are satisfied, each Defendant can be held liable for any acts that he or his co-conspirators took in furtherance of the conspiracy, including acts that his co-conspirators took before he joined the conspiracy. *See Beck v. Prupis*, 529 U.S. 494, 507 (2000); *see also Santos*, 541 F.3d at 73-74; *United States v. Dist. Council of N.Y. City & Vicinity of United Bhd. of Carpenters & Joiners of Am.*, 778 F. Supp. 738, 765 (S.D.N.Y. 1991).

All the evidence supporting the Defendants' conspiracy to steal trade secrets also supports their conspiracy to violate RICO (by stealing trade secrets and committing other predicates). In the face of evidence that they agreed to violate § 1962(c), Defendants argue that they cannot be liable for this agreement unless they also committed substantive RICO violations. *See* Papadopoulos Br. 20, Kushner Br. 10. This argument turns on a misreading of cases stating that "a 1962(d)

conspiracy claim must be dismissed where [a] substantive RICO claim is deficient." *Nat'l Grp. for Commc'ns & Computers Ltd. v. Lucent Techs. Inc.*, 420 F. Supp. 2d 253, 272 (S.D.N.Y. 2006). This statement means that, to be liable for participating in a RICO conspiracy, a defendant must agree to a plan that—if completed—would constitute a substantive RICO violation. *See Salinas*, 522 U.S. at 65; *Baisch v. Gallina*, 346 F.3d 366, 376 (2d Cir. 2003). But the defendant need not complete that plan to incur liability under § 1962(d). *See Beck*, 529 U.S. at 506-07 (a "plaintiff could . . . sue co-conspirators who might not themselves have violated one of the substantive provisions of § 1962").

As the Second Circuit explained in *Baisch*, the "requirements for RICO[] conspiracy charges under § 1962(d) are less demanding" than the requirements for substantive RICO charges under § 1962(c). *Baisch*, 346 F.3d at 376-77. A plaintiff can bring a successful RICO conspiracy claim against a defendant, even if the defendant is incapable of committing a substantive RICO offense, unaware of the exact predicates that his co-conspirators plan to commit, and not involved in the operation or management of an enterprise. *Salinas*, 522 U.S. at 64, *United States v. Applins*, 637 F.3d 59, 76 (2d Cir. 2011). And the Supreme Court has not required completion of a pattern of racketeering acts to trigger conspiracy liability. *See Salinas*, 522 U.S. at 65. Even "the existence of a RICO enterprise is not a required element of a RICO conspiracy claim." *City of New York v. Bello*, 579 F. App'x 15, 17 (2d Cir. 2014) (citing *Applins*, 637 F.3d at 75). Thus, the DNC's RICO conspiracy claim can survive even if its substantive RICO claim founders.

C. The Complaint Adequately Alleges Violations of the Wiretap Act (Responding to: Campaign Br. 38-43, Papadopoulos Br. 21-23, WikiLeaks 1st Br. 16-17)

The Wiretap Act imposes liability on any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" (the "interception provision"); "intentionally discloses, or endeavors

to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection" (the "disclosure provision"); or "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection" (the "use provision"). 18 U.S.C. § 2511(1)(a), (c), (d).

1. *Interception (Responding to: Campaign Br. 38-40, Papadopoulos Br. 21-22, WikiLeaks 1st Br. 16-17)*

Several Defendants claim that the Complaint fails to allege an "interception." 18 U.S.C. § 2511(1). An "interception" occurs whenever an eavesdropper captures an electronic message "contemporaneous[ly]," *i.e.*, as the message is traveling from one computer or electronic source to another. *See, e.g., Pure Power Boot Camp v. Warrior Fitness Boot Camp,* 587 F. Supp. 2d 548, 557 (S.D.N.Y. 2008). And that is precisely what the DNC alleged. The Complaint contains detailed allegations that the GRU placed malware called X-Agent on the DNC network, and that, "[b]ecause X-Agent was always on, the software captured the contents of communications going to and from the affected computers simultaneously with their transmission." ¶ 129; see also ¶¶ 103, 130 (alleging "realtime" surveillance and interception). The Complaint also alleges that GRU Operatives accessed the DNC's Voiceover Internet Protocol transfers, allowing the hackers to monitor voice-based communications, such as phone calls and voicemail, in realtime. ¶ 128. This use of X-Agent to capture communications in realtime constitutes the exact type of contemporaneous eavesdropping that the Wiretap Act prohibits.

2. *Knew or Had Reason to Know (Responding to: Campaign Br. 40, Kushner Br. 11, Papadopoulos Br. 20)*

As noted above, the "use" provision of the Wiretap Act provides that it is unlawful for a defendant to "use or endeavor to use" the contents of a communication *"knowing or having reason to know"* that the information was unlawfully intercepted. 18 U.S.C.A. § 2511(1)(d) (emphasis added). The Trump Campaign and Papadopoulos briefly argue that the DNC fails to allege that the Campaign "knew or should have known that Russian agents acquired the emails contemporaneously with the emails' transmission." Campaign Br. 40, Papadopoulos Br. 22. But such an allegation is not required. At the motion to dismiss stage, the "knowing or having reason to know" provision only requires that the plaintiff "allege that the defendant knew that neither party to the intercepted communication had consented to its interception." *Fernicola v. Specific Real Prop. in Possession, Custody, Control of Healthcare Underwriters Mut. Ins. Co.*, No. 00 CIV 5173 (MBM), 2001 WL 1658257, at *7 (S.D.N.Y. Dec. 26, 2001) (quoting *Peavy v. Dallas Indep. Sch. Dist.*, 57 F. Supp. 2d 382, 388 (N.D. Tex. 1999)). As explained above, the Complaint supports an inference that Defendants knew that Russia was stealing DNC information. *See, e.g.*, ¶ 2 (generally describing the Trump Campaign and its members' collaboration with Russian intelligence to steal and use emails and data to damage the Democratic Party). *id.* ¶¶ 13, 94, 99 (describing Papadopoulos' March-April 2016 meetings with a Kremlin-tied agent on behalf of himself and the Trump Campaign regarding thousands of stolen emails), 14, 133-135 (describing Trump, Jr.'s June 3-7, 2016 discussions with Kremlin-tied agents on behalf of himself and the Trump Campaign regarding stolen "sensitive information" about Hillary Clinton); 219 (describing Trump, Jr., Kushner, Manafort, and Gates' preparatory meeting in advance of the June 9, 2016 Trump Tower meeting); 15, 137-140 (describing Trump, Jr., Manafort, and Kushner's June 9, 2016 meeting with Kremlin-connected Russians at Trump Tower in order to discuss damaging

stolen information about the Democratic Presidential nominee). If, after their communications with Russian operatives to obtain "dirt" on Secretary Clinton, Defendants had any doubts that Russia was eavesdropping on DNC communications, the *Washington Post* dispelled those doubts on June 14, 2016, when it revealed the DNC had been hacked by Russian intelligence agencies. ¶ 146.[20] It is therefore disingenuous for the Trump Campaign to argue that it had no "reason to know" that the materials stolen from the DNC were unlawfully intercepted.

3. *Use Provision (Responding to: Campaign Br. 41-43, Kushner Br. 11, Papadopoulos Br. 22-23, Stone Br. 19)*

Finally, several Defendants argue that the DNC fails to allege a prohibited "use"[21] of an intercepted communication. 18 U.S.C.A. § 2511(1)(d). [22] The crux of Defendants' argument is that they did not violate the use provision by calling attention to documents that WikiLeaks placed in the public sphere. But the DNC does not simply allege that Defendants reacted to information published by WikiLeaks; rather, the Complaint alleges that, *before* WikiLeaks disclosed the DNC's information, Defendants collectively developed a Campaign strategy to promote stolen DNC communications at times they would be most beneficial to Trump. Such conduct falls squarely within the use provision.

---

[20] Confirming the Campaign's knowledge, the day the *Washington Post* revealed this information, Cohen cancelled his plans to meet with top Russian officials in St. Petersburg, including possibly Putin. ¶ 139.

[21] WikiLeaks does not contest that it violated the "disclosure provision."

[22] Stone does not respond to the Wiretap Act allegations except to posit in one sentence: "Stone played no part in the 'illegal interception;' access to the data was 'obtained lawfully,' and the subject matter was 'a matter of public concern.' *See Bartnicki v. Vopper*, 532 U.S. 514 (2001))." Stone Br. 19. The DNC interprets this sentence as an argument that Stone did not violate the Wiretap Act's use provision.

As several courts have explained, "use" simply means doing something slightly active, beyond passive listening or reading. *See, e.g., Peavy v. Harman*, 37 F. Supp. 2d 495, 513-14 (N.D. Tex. 1999), *aff'd in relevant part sub nom. Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000) ("use" "connotes active employment of the contents of the illegally intercepted communication for some purpose"); *Leslie v. Fielden*, No. 10-CV-320-TCK-TLW, 2011 WL 4005939, at *2-3 (N.D. Okla. Sept. 8, 2011) (use provision satisfied where defendant "allegedly listened to and/or watched the [intercepted] recordings and transcribed them, presumably for further use by her or others"); *Dorris v. Absher*, 179 F.3d 420, 426 (6th Cir. 1999) ("There is no doubt that an individual who composes a letter based on intercepted communications would be 'using' those communications" under the Wiretap Act); (holding that the defendants "used" intercepted recordings by analyzing and compiling relevant portions to be transcribed for purposes of an investigation). These cases show that the "use" provision imposes liability on those who, like Defendants, deliberately take advantage of their access to unlawfully intercepted information to build and further their strategic goals.

This conclusion is strongly supported by the statute's legislative history. In the Senate Report on the proposed legislation which ultimately became Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the broader crime-control law that included the Wiretap Act), the Senate noted:

> The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, . . . [e]very spoken word [relative] to each man's personal, marital, religious, political, or commercial concerns ***can be intercepted by an unseen auditor and turned against the speaker to the auditor's advantage***.

S. Rep. No. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2154 (emphasis added). Just as Congress feared, Defendants "turned" the DNC's communications against it, to

Defendants' advantage, by using or endeavoring to use the stolen DNC data as a strategic tool in their candidate's presidential campaign. *See, e.g.*, ¶¶ 14, 133-135 (detailing Trump, Jr.'s work with Russian agents to arrange a meeting to acquire stolen DNC data); 219 (discussing Trump, Jr., Kushner, Manafort, and Gates's preparation of that meeting); 15, 137-140 (discussing the Trump Tower meeting); 161-163 (discussing Stone's work with Russian intelligence, Assange, WikiLeaks, and Corsi to extract more data from the DNC); 173, 201 (discussing Trump, Jr.'s collaboration with WikiLeaks to encourage the public to access DNC data). Moreover, many disclosures of DNC communications "were timed to divert attention from adverse publicity about the Trump campaign, and to obscure positive news about the Clinton campaign and DNC activities." ¶ 160. Moreover, Trump (the de facto leader of the Trump Campaign) repeatedly directed the public to Wikileaks's cache of stolen documents, ¶¶ 196-202, to undermine the Democratic Party's objectives. These activities rise far above the types of transcription and letter-writing that courts have found be "use" under the Wiretap Act—and far above the passive receipt of information that Defendants urge.

D. The Complaint Adequately Alleges a Violation of the Defend Trade Secrets Act (Responding to: WikiLeaks 1st Br. 17-19, WikiLeaks 2nd Br. 2-3)

The Defend Trade Secrets Act ("DTSA") amended the Economic Espionage Act to create a civil cause of action for the misappropriation of trade secrets. 18 U.S.C. § 1836. This cause of action is available to any plaintiff who (1) owns a trade secret (2) that was misappropriated, if (3) the trade secret implicates interstate or foreign commerce. *Hawkins v. Fishbeck*, 301 F. Supp. 3d 650, 657 (W.D. Va. 2017) (quoting 18 U.S.C. § 1836(b)(1)).

The DNC alleges each of these elements. First, the DNC alleges that it owned trade secrets. The DTSA broadly defines "trade secrets" as:

> [A]ll forms of financial, business, scientific, technical, economic, or information, including patterns, plans, compilations, program devices, formulas, designs,

> prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if-
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information[.]

18.U.S.C. § 1839(3). All the trade secrets described in the Complaint satisfy this definition. *See, e.g.*, ¶¶ 1, 3, 14, 44, 47, 83, 156. The Complaint alleges that, in the cyberattack that began on April 18, 2016 and continued through June 2016, the GRU stole "donor information, financial and economic information, proprietary opposition research compiled from multiple sources, [and] information regarding planned political activities[.]" ¶ 105. The DNC explicitly alleges that this information was secret, ¶¶ 105-106, that it derived value from its not being known to those who could have derived economic value from the disclosure of the information, ¶ 108 (GRU could have derived significant economic value from stolen DNC data by, among other possibilities, selling it), and that the DNC had been using reasonable efforts to safeguard its security and secrecy, ¶ 102 (DNC "employ[ed] a firewall to limit access to its computers and require[ed] two-factor authentication for users who attempted to access the servers from remote locations," "periodically monitored its user accounts[,] and imposed password requirements").

The DNC further alleges that, during the cyberattack that began in September 2016, the GRU accessed and stole a plethora of confidential information from servers housing voter contact information, DNC email lists, important proprietary data such as the number of times internet users click on DNC advertisements (or "click rates") and the number of times internet users click on

links embedded in DNC emails (or "engagement rates"), and volunteer information. ¶ 182. The GRU also stole computer code created by DNC computer engineers, including Vertica and Tableau "queries". ¶¶ 180, 182-86, 189. These queries were secret, ¶¶ 184, 186, 188-189; derived value from not being known to those who could have derived economic value from the disclosure of the information, ¶¶ 193-94 (GRU could have derived significant economic value from the DNC's code); and the DNC had been using reasonable efforts to safeguard their security, ¶¶ 190-92 (DNC restricted access to authorized users, employed "two-factor authentication," and used firewalls and cybersecurity best practices).

The DNC also alleges all of the stolen trade secrets "related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C.A. § 1836(b)(1). Defendants do not challenge, and thus concede, this point. The information Russia stole during the April-June 2016 attack was used to support services that the DNC provided in "interstate commerce," including "fundraising and organizing events," ¶ 107. Similarly, Russia stole Vertica queries during the September 2016 attack. Vertica queries were used "to develop political, financial, and voter engagement strategies and services," and many were "used or intended for use in interstate commerce," ¶ 184. The Tableau queries Russia stole during the September 2016 attack were used to "develop graphs, maps, and other visual reports based on the data stored on Vertica," and "[m]any of these queries are used or intended for use in interstate commerce," ¶ 186. Finally, the other software in the "testing cluster" which Russia stole during the September 2016 attack was used to develop queries and was therefore related to a product "used or intended for use in interstate commerce," ¶ 189.

The DNC also alleges that its trade secrets were "misappropriated" under the DTSA. The DTSA defines "misappropriation" as the "acquisition of a trade secret of another by a person who

knows or has reason to know that the trade secret was acquired by improper means;" or the "disclosure or use" of a trade secret without the consent of the owner. *Teva Pharm. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 674 (E.D. Pa. 2018) (quoting 18 U.S.C. §§ 1839(5)(A)-(B)). Here, the DNC alleges that WikiLeaks acquired the DNC's trade secrets not only *knowing* that they had been stolen by the GRU, but as an active collaborator in the theft. *See* ¶¶ 149-56, *supra* Sections IV.A.1, IV.A.3.a.(1). Nevertheless, WikiLeaks protests that it never published anything that could qualify as a trade secret under the DTSA. WikiLeaks 1st Br. 18. This argument overlooks the DNC's allegations that on July 22, 2016, WikiLeaks published "sensitive trade secrets belonging to the DNC, including donor lists and detailed proprietary fundraising strategies based on the DNC's analysis of trends in donation data collected over years." ¶ 156. As explained above, these documents were the type of "financial," "business," and "economic" materials that qualify as "trade secrets" under 18 U.S.C. § 1839(3).

WikiLeaks also protests that it cannot be liable violating the DTSA because that statute does not apply extraterritorially. WikiLeaks 1st Br. 18-19. But, consistent with the language of the statute, the DNC alleges that "an act in furtherance of the offense was committed in the United States." 18 U.S.C.A. § 1837. An "act in furtherance of [an] offense" can be an act that is a "necessary precursor" to the crime charged. *See United States v. Scarano*, 975 F.2d 580, 587 (9th Cir. 1992), *as amended* (Nov. 24, 1992) (in a fraud case, holding that staging an automobile collision was "an act in furtherance of the offense" of defendant's commission of social security fraud). Here, the DNC alleges that several "necessary precursor[s]" to WikiLeaks's offense occurred in the United States, including the theft of trade secrets from DNC servers in Virginia and Washington D.C., ¶¶ 101, 304, 308, 347. WikiLeaks also sent messages to its co-conspirators located in the United States. *See, e.g.*, ¶ 173. That domestic activity is enough to hold WikiLeaks

liable. *See TianRui Grp. Co. v. Int'l Trade Comm'n*, 661 F.3d 1322, 1330 n.4 (Fed. Cir. 2011) ("Congress . . . recognized that misappropriation of U.S. trade secrets can, and does, occur abroad, and that it is appropriate to remedy that overseas misappropriation when it has a domestic nexus.")

E. The Complaint's State-Law Claims Should Be Sustained (Responding to: Agalarov Br. 21-24, Campaign Br. 43-50, Kushner Br. 12-15, Papadopoulos Br. 23-26, Stone Br. 18-19, WikiLeaks 1st Br. 25)

Several Defendants ask the Court to decline to exercise supplemental jurisdiction over Plaintiff's state-law claims and to find that those claims are not adequately alleged. The Court should reject these arguments.[23]

1. *The Court Should Exercise Supplemental Jurisdiction Over the State-Law Claims (Responding to: Agalarov Br. 24, Campaign Br. 43-45, Papadopoulos Br. 23, WikiLeaks 1st Br. 25)*

Several Defendants argue that the Court should decline to exercise supplemental jurisdiction over Plaintiff's state-law claims against them. Where a district court has "original jurisdiction" over some of a plaintiff's claims, it may exercise "supplemental jurisdiction" over any other claims that "form part of the same case or controversy under Article III of the United States Constitution." 28 U.S.C. § 1367(a), with some exceptions listed in 28 U.S.C. § 1367(c). The "Second Circuit has held that a district court's exercise of supplemental jurisdiction is mandatory over any claim that satisfies the elements of 28 U.S.C. § 1367(a) unless the claim also falls within one of the exceptions enumerated in § 1367(c)." *Metro Found. Contractors, Inc. v. Arch Ins. Co.*, No. 09-CV-6796 (JGK), 2011 WL 2150466, at *5 (S.D.N.Y. May 31, 2011) (Koeltl, J.) (citing *Itar-Tass Russ. News Agency v. Russ. Kurier, Inc.*, 140 F.3d 442, 447 (2d Cir. 1998)). Section

[23] Stone does not appear to seek dismissal of any state law claims asserted against him except, arguably, conspiracy to commit trespass to chattels under Virginia law. *See* Stone Br. 18-19. He thus concedes the remainder of the state-law claims asserted against him are adequately alleged.

1367(c) provides that a court may decline to exercise supplemental jurisdiction only if: "(1) the claim raises a novel or complex issue of State law, (2) the claim substantially predominates over the claim or claims over which the district court has original jurisdiction, (3) the district court has dismissed all claims over which it has original jurisdiction, or (4) in exceptional circumstances, there are other compelling reasons for declining jurisdiction." 28 U.S.C. § 1367(c). "In providing that a district court 'may' decline to exercise such jurisdiction, [section 1367(c)] is permissive rather than mandatory." *Valencia ex rel. Franco v. Lee*, 316 F.3d 299, 305 (2d Cir.2003) (citations omitted).

None of the Defendants contest that Plaintiff's state-law claims "form part of the same case or controversy" as the federal-law claims over which the Court has original jurisdiction. 28 U.S.C. § 1367(a). Rather, the Campaign argues that Plaintiff's state law claims raise a "novel or complex issue of State law." 28 U.S.C. §1367(c)(1). *See* Campaign Br. 43-44. Presumably referring to Count VIII (Washington D.C. Uniform Trade Secrets Act), the Campaign insists that "[t]he trade secrets claim raises the novel issue whether a political party's donor information qualifies as a trade secret," and it would be complex to sort through thousands of documents to determine which of the DNC's documents qualify as trade secrets. Campaign Br. 43. This argument is baseless. Courts across the country routinely determine whether data qualifies for protection as a trade secret, a determination guided by a well-developed body of case law. Indeed, DC's Uniform Trade Secrets Act ("DCUTSA") is based on the same model act adopted by *forty-seven* states, *Innovative BioDefense, Inc. v. VSP Techs., Inc.*, No. 12-CV-3710 (ER), 2013 WL 3389008, at *2 n.4 (S.D.N.Y. July 3, 2013), and is also substantively identical to the federal Defend Trade Secrets Act of 2016 ("DTSA"), *see, e.g.*, *Kuryakyn Holdings, LLC v. Ciro, LLC*, 242 F. Supp. 3d 789, 797

(W.D. Wis. 2017) (Wisconsin UTSA and DTSA are substantively "essentially the same").[24] Underscoring the routine nature of the trade secrets analysis, the Campaign itself appears to have no trouble setting forth the legal test for trade secret protection under the DCUTSA, and identifying information it claims is not subject to protection. Campaign Br. 45-47.

The Campaign next argues that Plaintiff's claim for conspiracy to commit trespass to chattels "raises novel issues regarding the scope of the tort of trespass to chattels in Virginia." Campaign Br. 43. The Campaign does not explain what aspects of Plaintiff's claim are novel, and, again, the Campaign's own brief undermines its argument by reciting the elements of the claim and citing case law applying the claim in the computer hacking context. Campaign Br. 47-49. Furthermore, it is difficult to see how exercising supplemental jurisdiction would require the Court to resolve a novel issue regarding trespass to chattels when Defendants do not raise one: As explained below, no Defendant challenges that the Complaint adequately alleges trespass to chattels under Virginia law. *See infra* Section IV.E.3.

Finally, the Campaign argues that Plaintiff's Virginia Computer Crimes Act claim raises the novel issue regarding whether the Act imposes liability on aiders and abettors. Campaign Br. 44. But there is nothing novel in courts considering whether Virginia's criminal statutes provide for aiding and abetting liability. Indeed, as explained below, the Eastern District of Virginia just recently held that Virginia's wiretap statute provides for aiding and abetting liability, including because "a number of cases have concluded that there" is "an independent cause of action for aiding and abetting in Virginia." *Marsh v. Curran*, No. 1:18-CV-787, 2019 WL 332801, at *6 (E.D. Va. Jan. 25, 2019). There is no reason why this Court cannot reach the same conclusion here.

---

[24] *See Vermont Microsystems, Inc. v. Autodesk, Inc.*, 138 F.3d 449 (2d Cir. 1998) (Judges Van Graafeiland, Walker, Koeltl interpreting the California UTSA).

The Campaign also urges the Court to decline to exercise supplemental jurisdiction if it dismisses the federal claims in the case. *See* Campaign Br. 44; 28 U.S.C. §1367(c)(3). However, given that Plaintiff raises claims under the laws of different states, a significant portion of the relevant events occurred in New York, and multiple Defendants are at home in New York, the Court should retain jurisdiction over Plaintiff's state law claims regardless of the disposition of its federal claims.

Finally, "where at least one of the subsection 1367(c) factors is applicable," a district court should only decline to exercise supplemental jurisdiction to promote "economy, convenience, fairness, and comity." *Jones v. Ford Motor Credit Co.*, 358 F.3d 205, 214 (2d Cir. 2004). The Campaign claims that, in this case, declining to exercise supplemental jurisdiction would promote those values because, if this case proceeds, the Special Counsel and congressional investigators would have to "coordinate their efforts with a private plaintiff's discovery demands." Campaign Br. 44. First, the Special Counsel's investigation is complete. As for congressional investigations, the Campaign's argument is premature, as the investigations may well have concluded by the time any discovery is requested in this matter. Moreover, federal investigations routinely run concurrently with private civil suits, and the Campaign does not explain how or why congressional investigators would be "forc[ed]" to coordinate with discovery here. Campaign Br. 44. If and when the Campaign's speculative concerns materialize, the DNC will work diligently with the Court to determine what, if any, coordination is required.

Next, the Campaign argues that exercising supplemental jurisdiction "may" require it to stay proceedings in this case to ensure discovery does not interfere with the GRU agents' rights in a pending criminal case. Campaign Br. 44. This argument does not apply, as the GRU agents are no longer defendants in this matter.

2. *Plaintiff Adequately Alleges a DCUTSA Claim (Responding to: Agalarov Br. 21-22, Campaign Br. 45-47, Kushner Br. 12, Papadopoulos Br. 23-24)*

The DCUTSA prohibits the misappropriation of trade secrets. D.C. Code Ann. § 36-401 et seq. To qualify as a trade secret, "(1) the information must be secret; (2) its value must derive from its secrecy; and (3) its owner must use reasonable efforts to safeguard its secrecy." *Econ. Research Servs., Inc. v. Resolution Econ., LLC*, 208 F. Supp. 3d 219, 232 (D.D.C. 2016) (internal quotation marks and citation omitted). "To establish a trade secret misappropriation claim, [a plaintiff] must demonstrate (1) the existence of a trade secret; and (2) acquisition of the trade secret by improper means, or improper use or disclosure by one under a duty not to disclose." *DSMC, Inc. v. Convera Corp.*, 479 F. Supp. 2d 68, 77 (D.D.C. 2007).

The DNC alleges each of these elements in the Complaint. First, as explained in the context of the Defend Trade Secrets Act in Section IV.D., above, the DNC alleges that it possessed secret information (¶¶ 105-106, 182, 184, 186, 188-189) which derived value from its secrecy (¶¶ 106, 184, 186) and which the DNC used reasonable efforts to keep secret (¶¶ 102, 190-192). *See also supra* Section IV.A.3.a.(1).

Second, the DNC more than adequately alleges that these trade secrets were acquired by improper means. The DCUTSA defines "improper means" as "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means." D.C. Code § 36-401(1). *See also DSMC, Inc.*, 479 F. Supp. 2d at 79 (citing same). Here, the DNC explicitly alleges that its trade secrets were taken by theft, and demonstrates that its trade secrets were taken by espionage through electronic means. The DNC provides a detailed description of the efforts that the GRU hacking teams code-named "Cozy Bear" and "Fancy Bear" undertook to gain unauthorized access to the DNC's computer systems during the April 2016 cyberattack, referring to the intrusion as a "hack" and an "attack"; and further describes the efforts

the DNC took to diagnose the attack, assess the damage, and repair or replace parts of the DNC network in order to remove the unauthorized hackers from the system. ¶¶ 101, 114-131. These efforts included engaging CrowdStrike, a cybersecurity firm, to perform the necessary forensic analysis. ¶ 110. The DNC also identifies the hackers' improper motivations for infiltrating their computer system. ¶ 119 ("CrowdStrike determined that the GRU's objective was to collect information about the DNC's political and research activities.").

Similarly, the DNC describes the GRU's September 2016 unauthorized access of the DNC's cloud-computing service as a further "attack" on the DNC's networks. The DNC alleges that the GRU gained "unauthorized access" to the DNC's cloud-computing service, stealing valuable trade secrets and other data; that Crowdstrike discovered a "breach" of the servers; and that the U.S. government "later concluded that this cyberattack had been executed by the GRU as part of its broader campaign to damage [] the Democratic [P]arty." ¶¶ 180, 193. *See also, generally,* ¶¶ 180-194. These allegations are more than sufficient to demonstrate that the acquisition of the DNC's trade secrets occurred by "improper means" and for an "improper use" under the DCUTSA. *See DSMC, Inc*. 479 F. Supp. 2d at 77.

Nevertheless, the Trump Campaign, Kushner, the Agalarovs, and Papadopoulos argue that the DNC fails to allege a misappropriation of trade secrets under the DCUTSA for a variety of reasons—each of which is invalid. First, the Trump Campaign and the Agalarovs contend that the DNC fails to describe the trade secrets alleged to be stolen. Campaign Br. 45; Agalarov Br. 22. This is not the case: as described in detail above, the DNC alleges that the stolen trade secrets consisted of "donor information, financial and economic information, proprietary opposition research compiled from multiple sources, [and] information regarding planned political activities" during the April 2016 attack, and voter contact information, click rates, engagement rates,

volunteer information, and Tableau and Vertica queries during the September 2016 attack. ¶¶ 105, 180, 182-86, 189.

The Trump Campaign also protests that the DNC's donor information and opposition research "encompass at least some plainly public information," and therefore cannot be entitled to trade secret protection. Campaign Br. 45. This too misses the mark: under trade secret jurisprudence, compilations of data—even compilations that contain public data—are entitled to trade secret protection if they otherwise meet the definition of "trade secrets." In the context of the Economic Espionage Act, the Ninth Circuit has held that, where an executive search company's core asset was a searchable database comprised of "source lists" of potential candidates, those "source lists" were entitled to trade secret protection, even though they were "composed largely, if not entirely, of public information." *United States v. Nosal*, 844 F.3d 1024, 1042 (9th Cir. 2016). This is because the "source lists" were not "unwashed, public-domain lists of all financial executives in the United States," nor could they be searched using publicly available sources. *Id.* Instead, they were the result of extensive culling efforts, requiring the company's expense and time. *Id. See also, e.g., Hertz v. Luzenac Grp.*, 576 F.3d 1103, 1114 (10th Cir. 2009) (a customer list may be a trade secret where "it is the end result of a long process of culling the relevant information from lengthy and diverse sources, even if the original sources are publicly available").[25] And in the context of the DCUTSA, "[e]ven if individual elements are known to the

[25] *Accord Computer Care v. Serv. Sys. Enters., Inc.*, 982 F.2d 1063, 1074 (7th Cir. 1992) ("A trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process design and operation of which in unique combination affords a competitive advantage and is a protectable trade secret" (internal citation omitted)).

public, a trade secret can exist in a unique combination of those otherwise publicly available elements." *DSMC, Inc.*, 479 F. Supp. 2d at 78.

This is precisely what the DNC alleges. *See, e.g.*, ¶ 156 (explaining that some of the stolen documents "were sensitive trade secrets belonging to the DNC, including donor lists and detailed proprietary fundraising strategies based on the DNC's analysis of trends in donation data collected over years."); ¶ 182 (explaining that stolen data from the cloud-computing servers included "volunteer information," such as "the list of people who have signed up for DNC-sponsored events and the number of people who attended those events.") Because the DNC spent time, effort, and expense developing the stolen documents, they were the type of unique combinations of data that are afforded trade secret protection, even though some of that data may be publicly available. *See also Free Country Ltd v. Drennen*, 235 F. Supp. 3d 559, 566 (S.D.N.Y. 2016) ("Under Second Circuit precedent, a customer list 'developed by a business through substantial effort and kept in confidence may be treated as a trade secret . . . provided the information it contains is not otherwise readily ascertainable.'") (quoting *N. Atl. Instruments, Inc. v. Haber*, 188 F.3d 38, 46 (2d Cir. 1999)). And because the DNC relied on the information that it had developed in these documents to conduct its core functions, such as fundraising, voter engagement, and volunteer recruiting, the DNC derived a competitive advantage from these unique combinations of data.

Next, the Trump Campaign argues that "donor information" and "opposition research" do not derive value by virtue of their secrecy. Campaign Br. 45. The Agalarovs appear to make a similar argument. Agalarov Br. 22. But these arguments simply ignore the Complaint, which explicitly states that such information derives value by virtue of its secrecy. In the Complaint, the DNC explains that the "compilations of public and private information" stolen in the April-June 2016 hack "derived substantial value from their amalgamation and organization," and "derived

economic value from the fact of their secrecy." ¶ 106. The DNC also explains *how* this data derived value from its secrecy: "if the data they contained were made public, it would reveal critical insights into the DNC's political, financial, and voter engagement strategies." *Id.* Moreover, the DNC alleges that it "used this data in interstate commerce by, among other things, fundraising and organizing events." ¶ 107. Thus, if the DNC's financial and voter engagement strategies were revealed, the DNC would face strategic and fundraising consequences—which is exactly why the DNC strove to keep these documents secret in the first place. Similarly, the DNC explains that it derives substantial value from the secrecy of its proprietary code, since, "if made public, these queries [the code] would reveal critical insights into the DNC's political, financial, and voter engagement strategies and services" and could reveal "fundamental elements of the DNC's political and financial strategies" if disclosed. ¶¶ 184, 186. The DNC further identified these pieces of code as "its most important, valuable, and highly confidential tools." ¶ 188. Thus, if this code were made public, it would threaten the DNC's political and financial strategies; if kept confidential, the DNC could continue to derive value from its secrecy.

The Trump Campaign, Kushner, Papadopoulos, and the Agalarovs argue that because they did not steal or disclose the information at issue, or use it before it became public knowledge, they cannot be liable for the theft of trade secrets. Campaign Br. 46-47; Kushner Br. 12; Papadopoulos Br. 23-24; Agalarov Br. 22. Under the DCUTSA, a plaintiff claiming misappropriation of trade secrets may show that the defendant gained access to the trade secrets through improper means *or* "that the defendant improperly used or disclosed trade secrets." *DSMC, Inc.*, 479 F. Supp. 2d at 79. Though D.C. courts have not interpreted the "used" or "disclosed" provisions, since the D.C. Uniform Trade Secrets Act "is based on the Uniform Trade Secrets Act, . . . as are the trade secrets statutes of several states, it is appropriate to consider how the courts in those states have interpreted

their states' trade secret acts when interpreting the D.C. trade secrets statute." *Catalyst & Chem. Servs., Inc. v. Glob. Ground Support*, 350 F. Supp. 2d 1, 7 n.3 (D.D.C. 2004).[26] In interpreting "use" under the Uniform Trade Secrets Act, the Eleventh Circuit has consulted the Restatement of Unfair Competition:

> There are no technical limitations on the nature of the conduct that constitutes 'use' of a trade secret. . . . As a general matter, any exploitation of the trade secret that is likely to result in injury to the trade secret owner or enrichment to the defendant is a 'use'. . . .

Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1292-93 (11th Cir. 2003) (quoting Restatement (Third) of Unfair Competition § cmt c. (1995)). Here, it is clear that the Trump Campaign, Kushner, Papadopoulos, and the Agalarovs "exploited" the DNC's trade secrets in a way that was "likely to result in injury to the trade secret owner." Specifically, Defendants exploited the DNC's trade secrets by using the stolen DNC information as strategic tools in their candidate's presidential campaign. *See supra* Sections IV.A.3.a.(1), IV.D. Further, the DNC alleges that Stone, communicating with the Trump Campaign, directed Corsi to connect with Assange and WikiLeaks to gather additional information about the trove of stolen materials, including trade secrets, that WikiLeaks had received from Russia, and that Corsi reported WikiLeaks' plans back to Stone, *see* ¶¶ 156, 161-62; and that WikiLeaks provided Trump, Jr. with a password to an anti-Trump political action committee website in exchange for Trump, Jr.'s assistance getting his father retweet a link to a WikiLeaks website containing stolen Democratic documents, including trade secrets, *see* ¶¶ 156, 173.

[26] It is particularly appropriate to look to the Trade Secrets Act decisions of courts in other jurisdictions because the D.C. statute was intended to 'make uniform the law with respect to trade secrets among the District of Columbia and those states enacting it." *Catalyst*, 350 F. Supp. 2d at 7 n.3. (quoting D.C. Code § 36-408).

Finally, the Trump Campaign argues that the Complaint "nowhere describes measures the DNC took to keep its information secret before the theft." Campaign Br. 47. This is simply false. The DNC alleges in detail that, with respect to the trade secrets stolen during the April 2016 hack, the DNC safeguarded the security of that information at that time by employing a firewall, requiring two-factor authentication, monitoring its accounts, and imposing stringent password requirements. ¶ 102. With respect to the trade secrets stolen during the September 2016 hack, as explained above at Section IV.D, the DNC includes detailed descriptions of the security measures in place to protect the data and code contained in its cloud-computing servers, including restricting access, requiring use of a VPN, and employing two-factor authentication. ¶¶ 190-92. Additionally, the DNC protected its AWS cloud-computing servers with firewalls and cybersecurity best practices, including: (a) limiting the IP addresses and ports with which users could access servers; (b) auditing user account activities; and (c) monitoring authentication and access attempts. ¶ 192. This level of detail more than demonstrates that the DNC used "reasonable efforts to safeguard [the] secrecy" and security of its trade secrets. *Econ. Research Servs.*, 208 F. Supp. 3d at 232-3.

3. *Plaintiff Adequately Alleges Conspiracy to Commit Trespass to Chattels Under Virginia Law (Responding to: Agalarov Br. 23-24, Campaign Br. 47-48, Kushner Br. 12-14, Papadopoulos Br. 24-25, Stone Br. 18)*

Under Virginia law, "[a] common law conspiracy consists of two or more persons combined to accomplish, by some concerted action, some criminal or unlawful purpose or some lawful purpose by a criminal or unlawful means." *Sines v. Kessler*, 324 F. Supp. 3d 765, 798-99 (W.D. Va. 2018) (quoting *Commercial Bus. Sys., Inc. v. BellSouth Servs., Inc.*, 453 S.E.2d 261 (Va. 1995)). "A claim of civil conspiracy also requires proof that the underlying tort was committed by a co-conspirator in furtherance of that conspiracy." *Id.* at 799 (quoting *Almy v. Grisham*, 639 S.E.2d 182 (Va. 2007); *Terry v. SunTrust Banks, Inc.*, 493 F. App'x 345, 357 (4th Cir. 2012)).

The Complaint alleges that "two or more" Defendants "combined to accomplish" a trespass to chattels. *Sines*, 324 F. Supp. 3d at 798-99. In other words, Defendants combined to "intentionally use[] or intermeddle[] with personal property in [the DNC's] rightful possession . . . without authorization." *Am. Online, Inc. v. LCGM Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998). As explained above at Section IV.A.3.a.(1), Defendants agreed that Russia would "intrude[] into [the DNC's] computer system through hacking, malware, and unwanted [spear phishing] e-mail communications," and that intrusion "may form the basis for claims of trespass to chattels and conversion." *Microsoft Corp. v. John Does 1-8*, No. 1:14-CV-811, 2015 WL 4937441, at *11 (E.D. Va. Aug. 17, 2015) (citing *Am. Online Inc. v. IMS*, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998); *Physicians Interactive v. Lathian Sys., Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *9 (E.D. Va. Dec. 5, 2003)).

Defendants do not dispute that Russia committed a trespass to chattels; rather, they argue that the Complaint fails to show that they (1) personally participated in the trespass; or (2) specifically agreed to the trespass. *See* Campaign Br. 42-43; Papadopoulos Br. 24; Kushner Br. 12; Agalarov Br. 22-23; Stone Br. 18-19. Stone also argues that he cannot be a member of the conspiracy because he did not join the conspiracy "before the hacking occurred." Stone Br. 18. These arguments reveal a fundamental misunderstanding of Virginia civil conspiracy law. The very cases upon which the Campaign relies explain why: "The object of a civil conspiracy claim is to spread liability to persons *other than* the primary tortfeasor." *Gelber v. Glock*, 800 S.E.2d 800, 821 (Va. 2017) (emphasis added). More specifically, "the purpose of a [civil] conspiracy claim is to impute liability—to make X jointly liable with D for what D did to P. Thus, a civil conspiracy plaintiff must prove that *someone* in the conspiracy committed a tortious act that proximately caused his injury; the plaintiff can then hold other members of the conspiracy liable

for that injury." *Id.* (emphasis added) (quoting *Beck v. Prupis*, 162 F.3d 1090, 1099 n.18 (11th Cir. 1998), *aff'd* 529 U.S. 494, 501-03 (2000)). The members of the conspiracy did not have to agree to every detail of Russia's hacking; rather, it is enough that they agreed to a general plan to hack and steal. *See id.* ("damage[s] caused by the acts committed *in furtherance* of the conspiracy" (emphasis added) (quoting *BellSouth*, 453 S.E.2d at 267)); *accord Sines*, 324 F. Supp. 3d at 799 ("A claim of civil conspiracy requires proof that the underlying tort was committed by a co-conspirator in furtherance of th[e] conspiracy." (internal quotation marks and citation omitted)); *see also Terry*, 493 F. App'x at 357 (under California civil conspiracy law, which the court noted is substantively the same as in Virginia, "[b]y participation in a civil conspiracy, a coconspirator effectively adopts as his or her own the torts of other coconspirators within the ambit of the conspiracy"). The DNC alleges that each Defendant was a member of this conspiracy. *See supra* Section IV.A.3.a.(1) (discussing the evidence of each Defendant's membership in the conspiracy to steal trade secrets). And as explained above, a member of a conspiracy can be held liable for the acts committed by his co-conspirators before he joins the conspiracy. *See also, e.g., State v. Carruthers*, 35 S.W.3d 516, 556 (Tenn. 2000); *Com. v. Albert*, 745 N.E.2d 990, 994 (2001).

Having adequately alleged (1) that Defendants entered into a conspiracy to accomplish an unlawful purpose (or alternatively, a lawful purpose by unlawful means); and (2) that Russia, a member of the conspiracy, caused damage to Plaintiff by committing the tort of trespass to chattels in furtherance of that conspiracy, the Complaint adequately alleges that Defendants are liable for civil conspiracy to commit trespass against chattels under Virginia law.[27]

[27] Moreover, though not required to establish a civil conspiracy claim, the Complaint also alleges that the Campaign conspired with Russia *specifically* to hack the DNC's computer systems. For instance, the Complaint alleges that "[a]t

4. *Plaintiff Adequately Alleges a Virginia Computer Crimes Act Claim (Responding to: Agalarov Br. 22-23, Campaign Br. 49-50, Kushner Br. 14-15, Papadopoulos Br. 25-26)*

Next, several Defendants argue that the DNC does not plausibly state a claim for relief under the Virginia Computer Crimes Act ("VCCA") Va. Code Ann. § 18.2-152.1, claiming that (1) the VCCA does not permit aiding and abetting liability, and (2) that the DNC has not sufficiently alleged an aiding and abetting violation of the VCCA. Defendants' arguments fail on both counts.

These Defendants first argue that Virginia law does not permit aiding and abetting liability under the VCCA, because when a Virginia statute is silent about aiding and abetting liability, that liability cannot be read into the statute. Agalarov Br. 22-23; Kushner Br. 14-15; Papadopoulos Br. 25; Campaign Br. 49-50. In support of this argument, Defendants attempt to make the ancillary point that Virginia courts are so reluctant to find that aiding and abetting liability may attach to torts arising out of common law that those courts could not possibly find that aiding and abetting liability attaches to statutory offenses. But Defendants misstate the law on both of these points.

As an initial matter, Virginia courts can and do find that aiding and abetting liability attaches to statutory offenses, even when the statute does not contain an aiding and abetting liability provision. Notably, just this past January, the Eastern District of Virginia found that a defendant may be liable for aiding and abetting the violation of the Virginia wiretap statute—a

---

a press conference on July 27, 2016, after commenting extensively on the materials that were stolen from the DNC servers, Trump called on the Russians to continue their hacking" and that Manafort "shar[ed] polling data . . . related to the 2016 presidential campaign" with Kilimnik that would "help[] Russia assess the most effective ways to interfere in the election." ¶¶ 91, 158 (internal citation omitted). Subsequently, Russia launched another attack on DNC servers housing sensitive information, an attack the U.S. government later concluded "had been executed by the GRU as part of its broader campaign to damage [] the Democratic [P]arty." ¶ 180.

portion of the Virginia criminal code that, like the VCCA, does not explicitly recognize aiding and abetting liability. In finding that the plaintiff's aiding and abetting claim should survive the defendants' motion to dismiss, the court observed: "The case law is uncertain as to whether there is an independent cause of action for aiding and abetting in Virginia . . . but a number of cases have concluded that there is." *Marsh*, 2019 WL 332801, at *6 (internal citation omitted) (citing *Jordan v. Osmun*, No. 1:16-CV-501, 2016 WL 7173784, at *4 (E.D. Va. Dec. 8, 2016)). Like the plaintiff in *Marsh*, the DNC brought a civil action in which it alleged that Defendants aided and abetted a violation of the Virginia criminal code. And just as the *Marsh* court found this theory of liability permissible under Virginia law, so should this Court find that Virginia law provides for aiding and abetting liability here.

The Campaign attempts to make the theoretical point that Virginia courts' refusal to recognize aiding and abetting liability in the context of common law torts reflects their reticence to exercise their authority to "define the scope of tort actions," and therefore signals their unwillingness to find aiding and abetting liability for actions arising under a statute. Campaign Br. at 50. But Defendants misinterpret the case law that they cite in support of this point: Defendants identify and quote cases that stand for the proposition that there is no *independent cause of action* for aiding and abetting a tort in Virginia. By contrast, Virginia law recognizes that "[a] defendant who aids and abets in the commission of a tort may *be jointly liable for that tort*," even if he is not liable for a *separate* tort of aiding and abetting. *Tysons Toyota, Inc. v. Commonwealth Life Ins.*, 20 Va. Cir. 399 (1990) (emphasis added); *Sherry Wilson & Co. v. Generals Court, L.C.*, No. 21696, 2002 WL 32136374, at *1 (Va. Cir. Ct. Sept. 27, 2002) ("Thus, unlike some jurisdictions, it may be said that the common law of the Commonwealth has looked with favor upon recovery in tort against those who aid and abet others in the commission of the civil wrong for which damages

may be maintained."). Moreover, Virginia law recognizes that other offenses based in the common law, such as fraud and breach of fiduciary duty, *may* support a cause of action for aiding and abetting. *See, e.g., Priester v. Small,* No. 26541, 2003 WL 21729900, at *2 (Va. Cir. Ct. Apr. 14, 2003) ("Where one aids and abets a fraud, they may be held liable for the damages sustained as a result of the actions of the principal."); *Tysons Toyota, Inc. v. Globe Life Ins. Co.*, Nos. 93-1359, 93-1443, 93-1444, 1994 WL 717598, at *3 (4th Cir. Dec. 29, 1994) ("Under Virginia law, one who aids and abets a third party's breach of fiduciary duty may be held liable for providing such assistance.").

Finally, Defendants briefly protest that the DNC has not adequately alleged that Defendants took any actions to aid and abet Russia's hack of the DNC's servers. However, as set forth in more detail above, the DNC alleged that Defendants worked with one another to coordinate the theft of materials from DNC computers before those materials were published. *See supra* Section IV.A.3.a.(1) (detailing evidence of Defendants' conspiracy to steal trade secrets).

F. The First Amendment Does Not Shield Defendants From Liability (Responding to: Campaign Br. 6-10, Kushner Br. 11-12, Papadopoulos Br. 26, Stone Br. 19, Wikileaks 1st Br. 3-10)

Several Defendants argue that the Court should dismiss "all" claims against them because, under *Bartnicki v. Vopper*, 532 U.S. 514 (2001), they had a First Amendment right to disclose the DNC's documents and data. But nothing in *Bartnicki* countenances Defendants corrupt, coordinated effort to steal DNC documents and use them to help a hostile foreign power interfere

in American elections. Moreover, contrary to Defendants' suggestion, *see* Campaign Br. 6, Defendants' asserted right to disclose information only bears on a handful of the DNC's claims.[28]

a. Bartnicki Is Inapplicable Here (Responding to Campaign Br. 6-10, Stone Br. 19, WikiLeaks 1st Br. 3-6)

Defendants' sole First Amendment argument is that this case is directly analogous to *Bartnicki*, where the Supreme Court recognized a limited First Amendment right to disclose stolen information under "specific fact[ual]" circumstances. *Bartnicki*, 532 U.S. at 524; *see also id.* at 535-36 (Breyer, J., joined by O'Connor, J., concurring and providing the deciding votes) ("I agree with [the majority's] narrow holding limited to the[se] special circumstances[.]"). Those factual circumstances, however, are not present here.

In *Barnicki*, one of the defendants, Jack Yokum, found a tape in his mailbox containing an illegally recorded cellphone conversation between the two plaintiffs, who were leaders of a local teachers' union. 532 U.S. at 518-519. After listening to the tape, Yokum gave it to a reporter,

[28] It is beyond dispute that the First Amendment provides no protection for stealing and conspiring to steal trade secrets, in violation of 18 U.S.C. §§ 1831-32, 1836 *et seq.*, 1962, and Va. Code Ann. § 18.2-152.1 *et seq.*; obstructing justice, in violation of 18 U.S.C. §§ 1503, 1962; tampering with witnesses and evidence, in violation of 18 U.S.C. §§ 1512, 1962; using the contents of illegal wiretaps to further their criminal plot to secure Trump's grip on power, in violation of 18 U.S.C. § 2511(1)(d), *see Bartnicki*, 532 U.S. at 526-27 (§ 2511(1)(d) regulates "conduct," not "speech"); conspiring to commit trespass to chattels, in violation of Virginia common law; or aiding and abetting the destruction of Plaintiff's computer system, in violation of Va. Code Ann. § 18.2-152.1 *et seq*. *See Branzburg v. Hayes*, 408 U.S. 665, 691 (1972) ("It would be frivolous to assert—and no one does in these cases—that the First Amendment, in the interest of securing news or otherwise, confers a license on either the reporter or his news sources to violate valid criminal laws. Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news."); *accord Bartnicki*, 532 U.S. at 532 n.19.

Fredrick Vopper, who played the tape on his public affairs talk show. *Id.* at 519. The plaintiffs later sued Yokum and Vopper for "disclos[ing]" the contents of the tape in violation of the Wiretap Act, 18 U.S.C. § 2511(c). *Id.* at 524. The Court held that, because Yokum and Vopper had behaved entirely lawfully at all times, and because they disclosed a conversation about union-approved violence, the First Amendment protected their conduct. *Id.* at 525. From the Court's perspective, the "normal method of deterring unlawful conduct" such as wiretapping is to "impose an appropriate punishment on the person who engages in it." *Id.* at 529. The Court therefore held that the government could not limit the speech rights of "law-abiding" individuals like Yokum and Vopper who stumble upon stolen information about a matter of public concern. *Id.*

There are several crucial factual differences between this case and *Bartnicki* that strip Defendants' conduct of constitutional protection. *First*, the *Bartnicki* defendants had completely clean hands: they did not aid, abet, or conspire with the individuals who engaged in the illegal wiretapping. *See Bartnicki*, 532 U.S. at 525 (majority opinion) (noting that the defendants played "no part" in the wiretapping); *id.* at 538 (Breyer, J., concurring) ("No one claim[ed] that they ordered, counseled, encouraged, or otherwise aided or abetted the interception, the later delivery of the tape by the interceptor to an intermediary, or the tape's still later delivery by the intermediary to the media."). Rather, the defendants "found out about the [illegal wiretap] only after it occurred," *id.* at 525 (majority opinion). By contrast, in this case, Defendants joined a complex, ongoing criminal conspiracy to steal and disseminate the DNC's information. *See supra* Section IV.A.3a.(1). By participating in this criminal scheme, Defendants became liable for Russia's information theft (undertaken in furtherance of the scheme).[29] *See Santos*, 541 F.3d at 73-

[29] Defendants are not liable for the information theft that occurred in 2015, before there was any conspiracy at all. However, they are liable for the information theft that occurred after the conspiracy was formed in March 2016.

74 (explaining that a defendant "incur[s] liability" for the unlawful acts of co-conspirators "committed both before and after" the defendant joined the conspiracy (citation omitted)); *Dist. Council of New York City*, 778 F. Supp. at 765. Because Defendants were legally responsible for stealing the DNC's information, they can be sued for cooperating with Russia to disseminate it. *See Bartnicki*, 532 U.S. at 529 ("assum[ing]" that that it would be constitutional to hold information thieves liable for disseminating stolen documents).

Consistent with this reasoning, several courts have concluded that, when a defendant conspires to steal information, he or she can be liable for disseminating it. For example, in *Peavy*, the Fifth Circuit recognized that it was constitutional to hold a journalist liable for disclosing the contents of an illegal wiretap because the journalist condoned his source's ongoing wiretapping, going so far as to instruct the source "not to turn the tape recorder on and off while recording intercepted conversations, and not to edit them, so that the tapes' authenticity could not be challenged." 221 F.3d at 164 (emphasis omitted). Similarly, in *In re Zyprexa Injunction*, the court held that a journalist could be liable for conspiring with a source to steal and disseminate documents sealed by court order. *In re Zyprexa Injunction*, 474 F. Supp. 2d 385, 396 (E.D.N.Y. 2007), *judgment entered sub nom. In re Zyprexa Litig.*, No. 07-CV-0504, 2007 WL 669797 (E.D.N.Y. Mar. 1, 2007), *and aff'd sub nom. Eli Lilly & Co. v. Gottstein*, 617 F.3d 186 (2d Cir. 2010); *see also Cockrum v. Donald J. Trump for President, Inc.*, —— F.3d ——, 2019 WL 1233857, at *3 (E.D. Va. Mar. 15, 2019) ("Here, unlike *Bartnicki*, the Campaign is alleged to have conspired with the Kremlin and WikiLeaks prior to the information being released and for its own benefit."). Following *Peavy* and *Zyprexa*, it should be beyond cavil that individuals who conspire to steal information forfeit their First Amendment right to disseminate it.

Second, Defendants in this case, unlike the *Bartnicki* defendants, were cooperating with a hostile foreign power to undermine Americans' right to self-governance. As explained above, Defendants conspired with Russia to disseminate stolen Democratic information in a way that would boost the electoral prospects of Russia's preferred presidential candidate. The First Amendment does not create a right to undermine fair democratic processes or commit espionage (in violation of 18 U.S.C. § 1831). *See Eu v. San Francisco Cty. Democratic Cent. Comm.*, 489 U.S. 214, 231 (1989) ("A State indisputably has a compelling interest in preserving the integrity of its election process."); *Bluman v. Fed. Election Comm'n*, 800 F. Supp. 2d 281, 288 (D.D.C. 2011) (Kavanaugh, J.) ("[T]he United States has a compelling interest for purposes of First Amendment analysis in . . . preventing foreign influence over the U.S. political process."), *aff'd*, 565 U.S. 1104 (2012); *United States v. Rosenberg*, 195 F.2d 583, 591 (2d Cir. 1952) (denying the existence of a constitutional right to engage in espionage). There is no First Amendment right to dissolve the foundations of our democracy: The Constitution "does not carry the seeds of destruction in its own bosom." *Ex parte Milligan*, 71 U.S. 2, 81 (1866) (argument of counsel).[30]

[30] In addition to using stolen DNC documents to gain a general electoral advantage, Defendants deliberately used stolen documents to disrupt the DNC's process for nominating a presidential candidate. *See* ¶ 150. The Supreme Court has repeatedly and "vigorously affirm[ed] the special place the First Amendment reserves for, and the special protection it accords, the process by which a political party 'select[s] a standard bearer who best represents the party's ideologies and preferences.'" *California Democratic Party v. Jones*, 530 U.S. 567, 575 (2000) (quoting *Eu*, 489 U.S. at 224). "The moment of choosing the party's nominee . . . is 'the crucial juncture at which [an] appeal to common principles may be translated into concerted action, and hence to political power in the community.'" *Id.* at 568 (*quoting Tashjian v. Republican Party of Connecticut*, 479 U.S. 208, 216 (1986)). Defendants had no constitutional right to help Russia use stolen information to interrupt this pivotal moment in the electoral process.

Third, the DNC, unlike the plaintiffs in *Bartnicki*, had a "legitimate interest in maintaining the privacy of [its stolen] conversation[s]." 532 U.S. at 539 (Breyer, J., concurring). As the Supreme Court has recognized, "[r]epresentative democracy . . . is unimaginable without the ability of citizens to band together" in organizations like the DNC, which "promot[e] among the electorate candidates who espouse [the organization's] political views." *California Democratic Party v. Jones*, 530 U.S. 567, 574 (2000). But political organizations—like any other organizations—cannot function effectively unless their members can have frank internal deliberations about the strategies they should pursue. *See NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 150-51 (1975). Nor can political organizations function effectively without the ability to control the organization's message. *See California Democratic Party*, 530 U.S. at 579-80. The DNC therefore had a paramount interest in keeping individual staff members' communications private, both so that staff could continue to have robust internal debates, and so that they could craft and deliver specific messages to the American public. Defendants' conduct fundamentally compromised those constitutionally protected interests.

Fourth, Defendants disclosed the DNC's documents to further the agenda of a racketeering enterprise. *See supra* Section IV.A. Nothing in *Bartnicki* shelters individuals who engage in racketeering: the First Amendment "does not reach so far as to override the interest of the public in ensuring that neither reporter nor source is invading the rights of other citizens through reprehensible conduct forbidden to all other persons." *Branzburg*, 408 U.S. at 691-92. The First Amendment protects the right to speak—not the right to engage in organized crime.

Fifth and finally, while the *Bartnicki* Court specified that its holding did not permit the disclosure of trade secrets, *see* 532 U.S. at 533, Defendants disseminated the DNC's trade secrets to the public. Courts have repeatedly enforced trade secret laws because they create an important

"incentive for investment in innovation." *DVD Copy Control Assn. v. Bunner*, 31 Cal. 4th 864, 880 (2003) (internal quotation marks omitted) (holding that a trade secret law remained constitutional after *Bartnicki*); *see also Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 493 (1974) ("Trade secret law encourages the development and exploitation of those items of lesser or different invention than might be accorded protection under the patent laws, but which items still have an important part to play in the technological and scientific advancement of the Nation.").[31]

In sum, Defendants' misconduct went far beyond that of the *Bartnicki* defendants, and their First Amendment arguments stretch far beyond the boundaries of the Constitution.

b. Holding Defendants Liable Will Not Threaten Freedom of the Press (Responding to: Amicus Brief, Campaign Br. 7-8, WikiLeaks 1st Br. 6-10)

Contrary to WikiLeaks's and the *amici curiae*'s[32] suggestion, holding WikiLeaks liable for disclosing the DNC's stolen information will not present a threat to freedom of the press. The DNC's claim that WikiLeaks participated in a criminal conspiracy to steal and disseminate information is *not* based solely on allegations that WikiLeaks engaged in common journalistic practices, such as meeting with information thieves or even soliciting stolen information. For example, the Complaint alleges that WikiLeaks sent Trump, Jr. a "password to an anti-Trump political action committee website," so that Trump, Jr. could access the site without permission (likely in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030). ¶ 173. Giving

[31] The first, second, fourth and fifth considerations discussed above also serve to distinguish this case from the other decisions that Defendants cite, including: *Florida Star v. B.J.F.*, 491 U.S. 524 (1989), *Boehner v. McDermott*, 484 F.3d 573 (D.C. Cir. 2007) (en banc), and *New York Times Co. v. United States*, 403 U.S. 713 (1971).

[32] *See* Brief of American Civil Liberties Union, Knight First Amendment Institute at Columbia University, Reporters Committee for Freedom of the Press, ECF No. 238.

sources stolen passwords to facilitate a computer crime is not an accepted journalistic technique. *See Zyprexa*, 474 F. Supp. 2d at 396 (quoting The New York Times, *Ethical Journalism: A Handbook of Values and Practices for the News and Editorial Departments*, 9 (Sept. 2004)). Nor is counselling foreign intelligence services on the best way to disrupt American elections, ¶ 150, or asking foreign intelligence services to steal "new material" from American targets. ¶ 149. Inferring WikiLeaks's participation in the conspiracy to steal DNC information from these and other acts creates no risk that law-abiding journalists will face liability for presenting stolen information to the public. *Compare, e.g., Peavy*, 221 F.3d at 163-64, 191-93 (freedom of the press would not be undermined if journalist were held liable for participating in a wiretapping scheme, where journalist advised source "not to turn the tape recorder on and off" during any future wiretaps) *with Jean v. Massachusetts State Police*, 492 F.3d 24, 31 (1st Cir. 2007) (freedom of the press would be undermined if publisher were held liable for accepting and disseminating an illegally recorded video from a source) *and Zerilli v. Evening News Ass'n*, 628 F.2d 217, 224 (D.C. Cir. 1980) (the "values served by a free and vigilant press" would be threatened if newspapers could be liable for "uncovering and publishing information that it deems newsworthy").

Nor will imposing liability on the other Defendants threaten journalistic values. "This is not a case of a government employee, whistleblower, protestor, or juror who faces the difficult choice of 'conform[ing his] behavior to the official "law" while protesting that the law was "wrong" . . . or . . . conform[ing] to [his] interpretation' of the law, absorbing whatever legal sanctions are a consequence of the choice." *Zyprexa*, 474 F. Supp. 2d at 396 (quoting Robert M. Cover, *Nomos and Narrative*, 97 Harv. L. Rev. 4, 47 (1983)). Rather, this is a case where individuals running a presidential campaign neglected their duties to the American public and collaborated with a hostile foreign government.

G. The Court Has Personal Jurisdiction Over the Agalarovs and WikiLeaks (Responding to: Agalarov Br. 16-21, WikiLeaks 1st Br. 19-23)

The Agalarovs and WikiLeaks argue that the Complaint fails to allege facts sufficient for the Court to exercise personal jurisdiction over them.[33] Personal jurisdiction must be established for each claim in a complaint. *Charles Schwab Corp. v. Bank of Am. Corp.*, 883 F.3d 68, 83 (2d Cir. 2018). As an initial matter, neither the Agalarovs nor WikiLeaks contest that the Court has personal jurisdiction to adjudicate the RICO claims against them. *See* Agalarov Br. 20-21 (citing 18 U.S.C. § 1965(b)); *Elsevier Inc. v. W.H.P.R., Inc.*, 692 F. Supp. 2d 297, 314-15 (S.D.N.Y. 2010).[34] It is also undisputed that the Court may exercise pendent personal jurisdiction over Plaintiff's state law claims. *See Charles Schwab*, 883 F.3d at 88. Consequently, the only question is whether the Court has personal jurisdiction to adjudicate the other causes of action asserted against the Agalarovs and WikiLeaks.

Personal jurisdiction is a two-step inquiry. First, the court determines whether there is a "statutory basis for exercising personal jurisdiction." *Marvel Characters, Inc. v. Kirby*, 726 F.3d

---

[33] The remainder of the Defendants do not contest, and thus concede, that this Court has personal jurisdiction over them with respect to all claims asserted.

[34] 18 U.S.C. § 1965(b) allows for personal jurisdiction over all defendants "where the ends of justice so require" as long as personal jurisdiction based on minimum contacts is established as to at least one defendant. *Elsevier*, 692 F. Supp. 2d at 314-15. The "ends of justice" requirement is met where "the RICO claim could not otherwise be tried in a single action because no district court could exercise personal jurisdiction over all of the defendants." *Id.* at 315 (collecting cases). Here, there can be no dispute that at least the Trump Campaign, which is headquartered in this district, and Trump, Jr., who resides in this district, are subject to personal jurisdiction in New York under 18 U.S.C. § 1965(a). No Defendant contends "that any other district would be able to hear the RICO claim against all of the Defendants." *Elsevier*, 692 F. Supp. 2d at 315. Accordingly, "it would be proper to exercise 'ends of justice' RICO jurisdiction" here. *Id.*

119, 128 (2d Cir. 2013) (citation omitted). "Federal courts ordinarily follow state law in determining the bounds of their jurisdiction over persons." *Daimler AG v. Bauman*, 571 U.S. 117, 125 (2014). Thus, the forum state's personal jurisdiction statute governs unless a federal statute "specifically provide[s] for national service of process." *PDK Labs, Inc. v. Friedlander*, 103 F.3d 1105, 1108 (2d Cir. 1997) (citation omitted). Second, the court considers whether exercise of personal jurisdiction over the defendant is consistent with due process under the Constitution. *Licci ex. rel Licci v. Lebanese Canadian Bank, SAL*, 732 F.3d 161, 167-68 (2d Cir. 2013). Applying this two-step procedure, it is clear that the Court has personal jurisdiction to adjudicate all the claims against WikiLeaks and the Agalarovs.

1. *New York's Long-Arm Statute Provides the Statutory Basis for Exercising Personal Jurisdiction over the Agalarovs*

New York's long-arm statute, N.Y.C.P.L.R. § 302, provides for personal jurisdiction over a non-domiciliary who "transacts any business within the state or contracts anywhere to supply goods or services in the state[.]" N.Y.C.P.L.R. § 302(a)(1). To determine whether jurisdiction exists under Section 302(a)(1), "a court must decide (1) whether the defendant transacts any business in New York and, if so, (2) whether this cause of action arises from such a business transaction."[35] *Best Van Lines, Inc. v. Walker*, 490 F.3d 239, 246 (2d Cir. 2007) (internal quotation marks and citation omitted).

The Complaint alleges that the Agalarovs transacted business in New York. "A defendant need not physically enter New York State in order to transact business, so long as the defendant's activities [there] were purposeful." *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL*, 673 F.3d

[35] "The transaction of business is not narrowed to a strict commercial sense[.]" *Otterbourg, Steindler, Houston & Rosen, P.C. v. Shreve City Apartments Ltd.*, 147 A.D.2d 327, 981 (N.Y. Sup. Ct., 1st App. Div. 1989) (quoting *Elman v. Belson*, 32 A.D.2d 422, 425 (N.Y. Sup. Ct., 2d App. Div. 1969)).

50, 61 (2d Cir. 2012) (internal quotation marks and citation omitted). "Purposeful activities are those with which a defendant, through volitional acts, avails itself of the privilege of conducting activities within [New York.]" *Eades v. Kennedy, PC Law Offices*, 799 F.3d 161, 168 (2d Cir. 2015) (citation omitted). A "single" purposeful activity is sufficient to trigger the statute. *Chloe v. Queen Bee of Beverly Hills, LLC*, 616 F.3d 158, 170 (2d Cir. 2010) (citation omitted). The Agalarovs purposefully conducted activities in New York State by, among other things, coordinating with Trump, Jr. to set up the Trump Tower Meeting, ultimately agreeing it would take place in Manhattan, ¶ 136, and sending their publicist Rob Goldstone and business associate Irakyl Kaveladze to that meeting, ¶ 137.

These "purposeful activities" in New York have a "substantial relationship" to all the claims in the Complaint, because Defendants used the Trump Tower meeting to make plans for their criminal conspiracies. ¶¶ 283, 290, 306, 307; *see Exxon Mobil Corp. v. Schneiderman*, 316 F. Supp. 3d 679, 697 (S.D.N.Y. 2018) (a single meeting may establish personal jurisdiction under N.Y.C.P.L.R. § 302(a)(1) where the meeting played a "significant role in establishing or substantially furthering the relationship of the parties" (quotation marks and citation omitted)). Thus, Plaintiff adequately pleads that New York's long-arm statute provides for personal jurisdiction over the Agalarovs.

2. *Fed. R. Civ. P. 4(k)(2) Provides The Statutory Basis for Exercising Personal Jurisdiction over the Agalarovs and WikiLeaks*

Even if the Court concludes New York's long-arm statute does not apply to the Agalarovs, Federal Rule of Civil Procedure 4(k)(2) provides the statutory basis for the Court to exercise personal jurisdiction over them and WikiLeaks. Rule 4(k)(2), the federal equivalent of a long-arm statute, establishes personal jurisdiction where "(1) the claim arises under federal law, (2) the defendant is not subject to jurisdiction in any state's courts of general jurisdiction, and (3)

exercising jurisdiction is consistent with the United States Constitution and laws." *BMW of N. Am. LLC v. M/V Courage*, 254 F. Supp. 3d 591, 598-99 (S.D.N.Y. 2017) (citation omitted).

These elements are readily met. First, Plaintiff's claims against the Agalarovs and WikiLeaks arise under federal law.[36] Second, if the Court rejects the DNC's analysis of the New York long-arm statute, neither the Agalarovs nor WikiLeaks will be subject to jurisdiction in any state's courts of general jurisdiction. *See* Decl. of Joseph M. Sellers.[37] The Agalarovs themselves admit that they are not subject to jurisdiction in any state. *See* Agalarov Br. 20 (disclaiming any U.S. presence or connection). "By arguing that [they] ha[ve] no presence in the United States and did not engage in transactions in New York sufficiently related to the instant dispute, . . . [the Agalarovs] ha[ve] in fact established the second necessary predicate for personal jurisdiction pursuant to Fed. R. Civ. P. 4(k)(2)." *BMW of N. Am. LLC*, 254 F. Supp. 3d at 599. Finally, as explained below, the Court's exercise of jurisdiction is consistent with Constitutional due process.

3. *The Court's Exercise of Personal Jurisdiction Over the Agalarovs and WikiLeaks is Consistent with Due Process*

Consistent with the Due Process Clause, Defendants have minimum contacts with the relevant fora and it is reasonable to litigate the DNC's claims in New York.

---

[36] Counts II and III against the Agalarovs and WikiLeaks, and Counts IV and VII against WikiLeaks, are federal law claims.

[37] This Court has held that a plaintiff can make the necessary showing that a defendant is not subject to jurisdiction in any state's courts of general jurisdiction by so certifying. *Freeplay Music, LLC v. Nian Infosolutions Private Ltd.*, No. 16-cv-5883-JGK-RWL, 2018 WL 3639929, at *13 (S.D.N.Y. July 10, 2018), *report and recommendation adopted*, No. 16-cv-5883 (JGK) (2018); *accord In re South African Apartheid Litig.*, 643 F. Supp. 2d 423, 429 (S.D.N.Y. 2009) (citing *United States v. Swiss Am. Bank, Ltd.*, 191 F.3d 30, 41 (1st Cir. 1999)).

a. Minimum Contacts

To show minimum contacts with New York, a plaintiff must allege "[f]irst, [that] the defendant . . . purposefully availed itself of the privilege of conducting activities within [New York] or . . . purposefully directed its conduct into [New York]," and "[s]econd, [that] the plaintiff's claim[s] . . . arise out of or relate to the defendant's [New York] conduct." *U.S. Bank Nat'l Ass'n v. Bank of Am. N.A.*, 916 F.3d 143, 150 (2d Cir. 2019) (internal quotation marks and citations omitted).

Because New York's long-arm statute closely tracks the requirements for minimum contacts under the Constitution, "personal jurisdiction permitted under [New York's] long-arm statute may theoretically be prohibited under due process analysis," but the Second Circuit "expect[s] such cases to be rare[,]" and has noted that it is not aware of any "such decisions in this Circuit." *Licci I*, 732 F.3d at 170. Here, there is no apparent reason why the Agalarovs' contacts with New York would satisfy New York's long-arm requirements, but not the Constitution.

If the Court exercises jurisdiction over the Agalarovs under Rule 4(k)(2), it is even clearer that that they had minimum contacts with the relevant forum. Under Rule 4(k)(2), the minimum contacts analysis "contemplates a defendant's contacts with the *entire* United States, as opposed to the state in which the district court sits." *RegenLab USA LLC v. Estar Techs. Ltd.*, 335 F. Supp. 3d 526, 546 (S.D.N.Y. 2018) (emphasis added); *accord BMW of N. Am. LLC*, 254 F. Supp. 3d at 599. The Agalarovs' relevant contacts with the United States include multiple efforts to influence the results of our elections and secure the President's grip on power, including their communications with the Trump Associates to arrange the Trump Tower meeting and their efforts to arrange a second meeting between Kremlin-connected attorney Natalia Veselnitskaya and the Trump transition team shortly after the election. ¶ 222. *See In re Terrorist Attacks on Sept. 11,*

2001, 392 F. Supp. 2d 539, 559 (S.D.N.Y. 2005) (minimum contacts include activities "purposefully directed" at the "residents of the forum" (citation omitted)).

WikiLeaks also engaged in many activities that were "purposefully directed" at United States residents. *Id.* In addition to repeatedly communicating and coordinating with Stone and Corsi (located in the United States) in furtherance of criminal conspiracies, *see United Res. 1988-I Drilling & Completion Program, L.P. v. Avalon Exploration, Inc.*, 1994 WL 9676, at *4 (S.D.N.Y. 1994) (sufficient minimum contacts where bank made phone calls and sent letters to residents of the forum), WikiLeaks purposefully directed its activities, such as dissemination of Plaintiff's trade secrets, toward the United States. Indeed, WikiLeaks admitted its activities were geared toward sowing conflict within the Democratic Party to increase Trump's chances of winning the 2016 election. *See* ¶ 150.

Moreover, the forum contacts of a member of a conspiracy may be imputed to co-conspirators where a plaintiff alleges that "(1) a conspiracy existed; (2) the defendant participated in the conspiracy; and (3) a co-conspirator's overt acts in furtherance of the conspiracy had sufficient contacts with a [forum] to subject that co-conspirator to jurisdiction in that [forum]." *Charles Schwab Corp.*, 883 F.3d at 87; *FrontPoint Asian Event Driven Fund, L.P. v. Citibank, N.A.*, No. 16 CIV. 5263 (AKH), 2018 WL 4830087, at *7 (S.D.N.Y. Oct. 4, 2018). Plaintiff alleges that the Agalarovs and WikiLeaks participated in criminal conspiracies with the other Defendants. In furtherance of those conspiracies, the other Defendants held meetings in New York (including the Trump Tower meeting), emailed Credico—who is based in New York—to ask for additional documents from Assange and WikiLeaks, ¶ 171, met with Kilimnik in New York, ¶ 168, and tampered with a witness, Credico, located in New York, *see* ¶ 228. Moreover, with respect to Rule

4(k)(2), nearly every overt act alleged in the Complaint occurred within the United States. *See, e.g.*, ¶¶ 101-105, 180, 208-231, 236.

b. Reasonableness

The final due process requirement is that "the exercise of jurisdiction must be reasonable under the circumstances." *U.S. Bank*, 916 F.3d at 150 (internal quotation marks and citations omitted). Under the reasonableness inquiry, a court evaluates: (1) the burden on the defendant, (2) the interests of the forum state, (3) the plaintiff's interest in obtaining relief, (4) the "interstate judicial system's interest in obtaining the most efficient resolution of controversies," and (5) "the shared interests of the several States in furthering fundamental substantive social policies." *Id.* at 151 n.5 (quotation marks and citation omitted). The first factor is the primary one. *Id.*

The Agalarovs do not contest that it is reasonable to exercise personal jurisdiction over them. Nor could they: Given their wealth, it would not be unduly burdensome for them to travel to the United States. *See* ¶¶ 50-51. At the same time, it would be efficient to litigate the claims against the Agalarovs and their co-conspirators (who do not raise personal jurisdiction defenses) in the same forum. Finally, Plaintiff's interests, New York's interests, and the United States' interests could not be stronger: The Complaint alleges that the Agalarovs engaged in a conspiracy (partly in New York) to illegally obtain and disseminate the DNC's legally protected information and subvert the American electoral process. It would not "offend traditional notions of fair play or substantial justice" to hold them accountable for this grave misconduct. *U.S. Bank*, 916 F.3d at 156.

For nearly identical reasons, the Court's exercise of personal jurisdiction over WikiLeaks is "reasonable under the circumstances." *U.S. Bank*, 916 F.3d at 150. WikiLeaks does not identify any burden in being required to litigate this action in this forum, relying instead on a conclusory assertion that it would be offensive to "traditional notions of fair play and substantial justice" to

hold it accountable in this forum. WikiLeaks 1st Br. 23 (citing *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945)). But WikiLeaks freely chose to engage in an illegal scheme unprecedented in scope during the 2016 election (and after) with the intent of sowing division within the Democratic Party to help secure Trump's grip on political power. Having conspired to undermine the American electoral system, WikiLeaks cannot now claim any "unfairness" in being held to account in the United States.

H. Defendant-Specific Arguments (Responding to: Campaign Br. 10-12, Stone Br. 14-17, WikiLeaks 1st Br. 10-12, 23-25)

1. *Stone: Article III Standing (Responding to: Stone Br. 14-17)*

Stone argues that Plaintiff lacks Article III standing. Article III standing requires "(1) *injury-in-fact*, which is a concrete and particularized harm to a legally protected interest; (2) *causation* in the form of a fairly traceable connection between the asserted injury-in-fact and the alleged actions of the defendant; and (3) *redressability*, or a non-speculative likelihood that the injury can be remedied by the requested relief." *Harry v. Total Gas & Power N. Am., Inc.*, 889 F.3d 104, 110 (2d Cir. 2018) (citation omitted). "[T]he pleading standard for constitutional standing is lower than the standard for a substantive cause of action." *Id.* at 110.

Stone challenges only the causation element. He argues that the allegations against him relate solely to the theft of documents from the Democratic Congressional Campaign Committee ("DCCC") and John Podesta, Secretary Clinton's campaign manager, and these thefts did not cause the DNC's injuries. Stone Br. 14-15. But the Complaint's allegations relating to the DCCC and Podesta are simply two of the many pieces of evidence suggesting that Stone participated in a broad conspiracy to steal and disseminate materials from Democratic targets, including the DNC. The DNC is only seeking redress for its own injuries at the hands of the conspirators.

Stone fails to recognize that Article III's "causation standard does not require that the defendant personally commit the act that harms the plaintiff." *Merriam v. Demoulas*, No. 11-10577-RWZ, 2013 WL 2422789, at *4 (D. Mass. June 3, 2013). For instance, it is well-settled that a plaintiff has standing to sue a principal for acts committed by her agent. *See, e.g.*, *Chevron Corp. v. Donziger*, 833 F.3d 74, 150 (2d Cir. 2016) (quoting Restatement (Third) of Agency § 7.04 (2006)). Likewise, it is settled that a plaintiff has standing to sue a member of a conspiracy for harms directly caused by the actions of a co-conspirator. *See, e.g.*, *Schaffer v. Comm'r*, 779 F.2d 849, 851 (2d Cir. 1985) ("One who participates with others in a joint enterprise may be held criminally and civilly liable for all the actions taken by any participant in furtherance of the venture."); *see also DiPizio v. Empire State Dev. Corp.*, 745 F. App'x 385, 387-88 (2d Cir. 2018) (plaintiffs had standing where they alleged the defendants "engaged in an 'unlawful conspiracy'" that caused plaintiffs harm).

In view of this caselaw, Stone's argument collapses. The Complaint repeatedly alleges that Defendants—including Stone—entered into a conspiracy "to secure Trump's grip on the Presidency through illegal means." ¶ 70. The Complaint is replete with allegations that Stone was actively involved in that conspiracy. *See, e.g.*, ¶ 58 (Stone held himself out to senior members of the Trump campaign as a conduit to WikiLeaks); ¶¶ 161, 164, 165, 167, 170, 171-72, 174, 176 (Stone was in frequent contact with Assange and WikiLeaks as well as Guccifer 2.0, regularly discussing stolen data); ¶ 162 (on July 25, 2016, Stone directed Corsi to contact Assange and WikiLeaks to gather additional information about stolen materials WikiLeaks had received from Russia); ¶¶ 179-80 (after Stone told Russia that stolen turn-out models were "[p]retty standard," Russia took snapshots of the virtual servers that housed key pieces of the DNC's analytics infrastructure). Though Stone now claims he did nothing wrong, his protestations of innocence are

difficult to square with the extreme measures he took to cover up the foregoing activities, including criminal obstruction of justice and witness tampering. *See, e.g.*, ¶¶ 214-15, 224-26, 228, 293, 300.

2. *Trump Campaign: Political Question Doctrine (Responding to: Campaign Br. 10-12)*

The Trump Campaign claims that the political question doctrine "precludes judicial review of the DNC's criticisms of President Trump's political decisions." Campaign Br. 10-12. As explained below at Section IV.I.2, the political question doctrine is narrowly tailored to avoid judicial review of policy decisions explicitly delegated to the other branches. But the DNC is not asking the Court to review or adjudicate the lawfulness of any of President Trump's decisions. Rather, the Complaint simply asks the Court to infer that certain actions strengthened Russia's incentives to continue fighting to preserve Trump's grip on power. Indeed, Trump is neither a defendant nor an alleged co-conspirator and the DNC has not asked the Court to determine whether he violated any laws. Thus, contrary to the Campaign's claims that the Complaint requires "judicial review of discretionary military decisions" and that it would result in the court "rul[ing] on the President's statements threatening" withdrawal from a treaty, Campaign Br. 11-12, there is simply nothing about Trump's executive decisions for this Court to adjudicate. And even if the Court wishes to strike the handful of allegations regarding Trump's actions while in office, ¶¶ 237-43, the Complaint still contains ample allegations to support the DNC's claims.

3. *WikiLeaks: Venue and Communications Decency Act (Responding to: WikiLeaks 1st Br. 10-12, 23-25)*

WikiLeaks asserts that: (1) venue does not lie in this district; and (2) the Communications Decency Act shields it from liability. The Court should reject both contentions.

a. Venue is Proper in this District (Responding to: WikiLeaks 1st Br. 23-25)

The federal venue statute provides that "a civil action may be brought in . . . a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred . . . ." 28 U.S.C. § 1391(b)(2). Section 1391(b)(2) does not restrict venue to the district in which the "most substantial" events giving rise to a claim occurred; rather, "[v]enue may be proper even if a greater part of the events giving rise to a claim happened in another forum." *City of New York v. CyCo.net, Inc.*, 383 F. Supp. 2d 526, 543 (S.D.N.Y. 2005). A substantial part of the events giving rise to Plaintiff's claims clearly occurred in New York City: the Trump Campaign was headquartered and presumably made strategic decisions in New York, and the Trump Tower meeting and Manafort's meeting with Kilimnik to share information regarding the election both took place in New York. WikiLeaks's breezy dismissal of these allegations reveals a fundamental misunderstanding of Plaintiff's claims and conspiracy law more generally. As explained above, the Court can and should infer that the Trump Tower meeting was a pivotal moment for the conspirators. By faulting the DNC for failing to allege the exact "content" of the meeting, WikiLeaks 1st Br. 23, WikiLeaks is ignoring the Second Circuit's admonition that "conspiracies are rarely evidenced by explicit agreements, but nearly always must be proven through inferences that may fairly be drawn from the behavior of the alleged conspirators." *Anderson News, L.L.C.*, 680 F.3d at 183 (internal quotation marks omitted). As detailed above at Section IV.A.3.a.(1), the events surrounding the Trump Tower meeting and the communications between the co-conspirators leading up to and following the meeting amply support the plausible inference that the meeting was intended to exchange or plan the acquisition of stolen Democratic information.

Moreover, the RICO statute provides that "[a]ny civil action or proceeding under this chapter against any person may be instituted in the district court of the United States for any district

in which such person resides, is found, has an agent, or transacts his affairs." 18 U.S.C. § 1965(a). This provision "is supplemental to the general federal venue provision found in 28 U.S.C. § 1391." *Cyco.Net, Inc.*, 383 F. Supp. 2d at 544. "This means Plaintiff may properly lay venue [for its RICO claims] in accordance with *either* 18 U.S.C. [§] 1965 or 28 U.S.C. [§] 1391." *Id.* at 544. "[I]t is the policy in this Circuit to conflate personal jurisdiction and venue by reading the RICO venue provision to permit adjudication in any district where minimum contacts are established." *Id.* (citing *PT United Can Co. v. Crown Cork & Seal Co.*, 138 F.3d 65, 71 (2d Cir.1998)). This inquiry merely requires that "at least one defendant" have minimum contacts with the district. *Id.* at 541 (quoting *PT United*, 138 F.3d at 71). Because both the Campaign and Trump, Jr. reside in this district, and thus have minimum contacts with it, venue over Plaintiff's RICO claims is proper. *Id.*

b. The Communications Decency Act Does Not Protect WikiLeaks's Conduct (Responding to: WikiLeaks 1st Br. 10-12)

WikiLeaks argues that it cannot be held liable for its role in the dissemination of the DNC's stolen trade secrets because, it claims, it is protected from civil liability under the Communications Decency Act, 47 U.S.C. § 230 ("CDA").[38] WikiLeaks's argument, however, rests on a tortured interpretation of the CDA.

Congress drafted Section 230 of the CDA to provide immunity from state-law claims "for 'interactive computer services' that make 'good faith' efforts to block and screen offensive content." *Fed. Trade Comm'n v. LeadClick Media, LLC*, 838 F.3d 158, 173 (2d Cir. 2016) (quoting 47 U.S.C. § 230(c)). Accordingly, the CDA provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by

[38] Stone also makes a fleeting assertion that WikiLeaks's conduct is protected by the Communications Decency Act, though he does not advance any substantive arguments to support this assertion. *See* Stone Br. 19.

another information content provider" and that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." 47 U.S.C. §§ 230(c)(1), (e)(3). CDA immunity is an affirmative defense that, at the motion to dismiss stage, a defendant must establish is evident from the face of the complaint. *See Ricci v. Teamsters Union Local 456*, 781 F.3d 25, 28 (2d Cir. 2015) (quoting *Klayman v. Zuckerberg*, 753 F.3d 1354 (D.C. Cir. 2014)).

To qualify for protection under the CDA, a defendant must show that it "(1) is a provider or user of an interactive computer service, (2) the claim is based on information provided by another information content provider and (3) the claim would treat [the defendant] as the publisher or speaker of that information." *LeadClick*, 838 F.3d at 173 (internal quotation marks and citation omitted). It is not evident from the face of the Complaint that WikiLeaks satisfies any of these requirements.

To meet the first element, WikiLeaks must show that it is a provider of an interactive computer service, defined under the CDA as "any information service, system or access software provider that provides or enables computer access by multiple users to a computer server." 47 U.S.C. § 230(f)(2). "Courts typically have held that internet service providers, website exchange systems, online message boards, and search engines fall within this definition." *LeadClick*, 838 F.3d at 174. For example, the Second Circuit has noted that GoDaddy, AOL, Craigslist, and Ask.com are interactive computer services. *See id.*

WikiLeaks argues, without any supporting authority or citation to the Complaint, that it is entitled to protection under the CDA because it is similar to "Facebook, Twitter, and WordPress." WikiLeaks 1st Br. 12; *see also* Stone Br. 19. Not so. Unlike WikiLeaks's proffered examples and those set forth by the Second Circuit, WikiLeaks is not a website exchange system that enables

users to post their own content (like GoDaddy, Craigslist, Facebook, Twitter, or WordPress), nor is it an internet service provider (like AOL), a search engine (like Ask.com), or an online message board. *See LeadClick*, 838 F.3d at 174. Rather, it is an organization that itself "publishes leaked or stolen confidential and classified information." ¶ 54. WikiLeaks does not otherwise explain how it "provides or enables computer access by multiple users to a computer server[,]" 47 U.S.C. § 230(f)(2).

To satisfy the second element, WikiLeaks must show that it is not "an 'information content provider' of the content which gives rise to the underlying claim." *LeadClick*, 838 F.3d at 174. An "information content provider" is "any person or entity that is responsible, in whole *or in part*, for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(f)(3) (emphasis added). For example, in *F.T.C. v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009), "a defendant who paid researchers to uncover confidential phone records protected by law, and then provided that information to paying customers, fell within the definition because he did not merely act as a neutral intermediary, but instead 'specifically encourage[d] development of what [was] offensive about the content.'" *LeadClick*, 838 F.3d at 174 (quoting *Accusearch*, 570 F.3d at 1199). Similarly, a website was not protected by the CDA where it "required subscribers to provide information which enabled users of the site to unlawfully discriminate in selecting a roommate" thus "'materially contributing to [the contents'] alleged unlawfulness.'" *Id.* (quoting *Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1167 (9th Cir. 2008)).

Here, the Complaint alleges that WikiLeaks was not simply a "neutral intermediary" passively publishing the content of others; rather, it actively solicited protected DNC data from Russia, and then coordinated with the other Defendants to release the data in a way that caused

maximum damage to Plaintiff and the American democratic system. *See, e.g.*, ¶¶ 17, 149-151, 154, 175. Courts have held that conduct of this nature falls well outside the scope of activities afforded protection by the CDA. *See, e.g.*, *Roommates*, 521 F.3d at 1171-72 (distinguishing between a website that merely provides "neutral tools" that may be used by third parties to post unlawful content and a website that "both elicits the allegedly illegal content and makes aggressive use of it in conducting its business"); *Accusearch*, 570 F.3d at 1199 (defendant not protected under CDA where it "knowingly sought to transform [legally protected] information into a publicly available commodity" and where it "knew that its researchers were obtaining the information through fraud or other illegality").

WikiLeaks does not even attempt to argue that the third element is met here. This is reason alone to reject its CDA argument. *See Ricci*, 781 F.3d at 28 (burden on defendant to establish CDA elements). This omission reflects the fact that the Complaint does not "treat [WikiLeaks] as a publisher or speaker of third-party content." *LeadClick*, 838 F.3d at 175 (quoting *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1101 (9th Cir. 2009)). Rather, it treats WikiLeaks as a participant in a criminal conspiracy. *See id.* (CDA not applicable where the defendant's "liability was premised not on content but on its conduct").

I. Russia Can Be Held Liable for its Misconduct (Responding to: Russia Statement of Immunity 1-10)

In its Statement of Immunity, Russia advances three arguments: (1) that it is entitled to sovereign immunity under the FSIA; (2) that the political question doctrine bars the Court from adjudicating Plaintiff's claims against Russia; and (3) that venue is not proper in this District. Each of Russia's arguments fails.

1. *Russia Is Not Entitled to Sovereign Immunity under the FSIA (Responding to: Russia Statement of Immunity 4-7)*

Under the FSIA, 28 U.S.C. § 1602 *et seq.*, a "'foreign state *shall* be immune from the jurisdiction of the courts of the United States and of the States' unless one of several statutorily defined exceptions applies." *Republic of Argentina v. Weltover, Inc.*, 504 U.S. 607, 610-11 (1992) (quoting 28 U.S.C. § 1604). Two such "statutorily defined exceptions" strip Russia of its sovereign immunity in this case: the non-commercial tort exception, 28 U.S.C. § 1605(a)(5), and the commercial activity exception, 28 U.S.C. § 1605(a)(2).

a. The Non-Commercial Tort Exception Applies Here

The non-commercial tort exception to foreign sovereign immunity applies in cases where

> money damages are sought against a foreign state for personal injury or death, or damage to or loss of property, occurring in the United States and caused by the tortious act or omission of that foreign state or of any official or employee of that foreign state while acting within the scope of his office or employment.

28 U.S.C. § 1605(a)(5). In this case, Plaintiff is seeking "money damages" from Russia for "damage to or loss of property, occurring in the United States and caused by" Russian agents who tortiously trespassed onto the DNC's computer servers and converted the DNC's electronic files "while acting within the scope of [their] office or employment." 28 U.S.C. § 1605(a)(5).

Nevertheless, Russia argues that the non-commercial tort exception is inapplicable because: (1) Plaintiff "primarily alleges that [its] information was disclosed, not that information (or the systems in which it resided) was lost or destroyed"; (2) the Russian officers who interfered with Plaintiff's servers and computer files were exercising a "discretionary function"; and (3) Plaintiff failed to allege that an "entire tort" was committed within the United States. Russia Statement of Immunity 6-7. All three arguments are legally and factually inaccurate.

(1) Plaintiff Alleges Significant Damage to its Computer Servers and Files

First, contrary to Russia's suggestion, Plaintiff alleges that its "information" and the "systems in which it resided" were damaged by Russia's tortious conduct. Russia Statement of Immunity 6. More specifically, Plaintiff alleges that Russia "caused enormous damage to the DNC's computer systems, creating the need to . . . repair and replace all of the DNC's computer hardware and software, telephone and telephone systems, and back-up systems." ¶ 254. Russia cannot escape liability for this damage simply because it *also* harmed Plaintiff in other ways (*e.g.*, by disclosing Plaintiff's information to the public).

(2) The Russian Officers Who Committed the Relevant Torts Were Not Performing Discretionary Functions

The FSIA provides that the non-commercial tort exception is *inapplicable* in cases based upon a foreign official's "exercise or performance or the failure to exercise or perform a discretionary function." 28 U.S.C. § 1605(a)(5)(A). An activity is considered discretionary if it involves "an element of judgment or choice," and "the judgment or choice in question [is] grounded in considerations of public policy or susceptible to policy analysis." *USAA Cas. Ins. Co. v. Permanent Mission of Republic of Namibia*, 681 F.3d 103, 111-12 (2d Cir. 2012). Applying this standard, the GRU operatives who trespassed onto the DNC's servers were not exercising any "judgment or choice." *Id.* at 111-12. Courts have recognized that employees exercise no "judgment or choice" when their actions are "compelled by statute or regulation." *Id.* Employee actions are no more discretionary when they are "compelled by" military orders. And the Complaint alleges that the GRU officers who hacked the DNC's servers "were carrying out military orders that they could not disobey." ¶ 101.

Russia tries to escape this conclusion by noting that the Russian government—as a whole—exercised discretion when it formulated the plan to hack the DNC's servers. Russia Statement of

Immunity 7. But that is irrelevant. Plaintiff is seeking damage for the tortious acts of specific Russian "official[s] or employee[s]," 28 U.S.C. § 1605(a)(5), and those employees were obligated to trespass onto Plaintiff's servers. *USAA Cas. Ins. Co.*, 681 F.3d 103, 111-12 (recognizing that the discretionary function rule is inapplicable when a foreign official is "compelled" to commit a tort by foreign statutes or regulations, even though foreign governments presumably exercise some discretion when crafting those statutes or regulations).

(3) Plaintiff Alleges That Russian Officials Committed an Entire Tort Within the United States.

Finally, Russia argues that the non-commercial tort exception is inapplicable because it did not commit an entire tort within the United States. Russia Statement of Immunity 6. Courts have expanded upon the FSIA's statement that foreign governments can be sued for tortious conduct that causes "loss . . . in the United States." 28 U.S.C. § 1605(a)(5). In *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428 (1989), the Supreme Court held that the exception is not applicable where a foreign sovereign commits a tort abroad, even if that tort results in "loss . . . in the United States." *Id.* at 441. Rather, the exception is only applicable when a foreign sovereign commits a tort "within the territorial jurisdiction of the United States." *Id.* Relying on *Amerada Hess*, several lower courts—including the Second Circuit—have created an "entire tort" doctrine, providing that the non-commercial tort exception is only available in cases where an "entire tort" occurs in the United States. *See, e.g.*, *In re Terrorist Attacks on Sept. 11, 2001*, 714 F.3d 109, 115-16 (2d Cir. 2013); *Cabiri v. Government of Ghana*, 165 F.3d 193, 200 n.3 (2d Cir. 1999); *Asociacion de Reclamantes v. United Mexican States*, 735 F.2d 1517, 1525 (D.C. Cir. 1984); *O'Bryan v. Holy See*, 556 F.3d 361, 382 (6th Cir. 2009); *Olsen by Sheldon v. Government of Mexico*, 729 F.2d 641, 646 (9th Cir. 1984), *abrogated on other grounds as stated in Joseph v. Office of Consulate Gen. of Nigeria*, 830 F.2d 1018, 1026 (9th Cir. 1987).

Courts disagree about the proper scope of the entire tort rule. One D.C. Circuit panel concluded, in dicta, that the entire tort rule would be satisfied if a defendant started a tortious course of conduct abroad, but completed a tortious act and caused a tortious injury within the United States. *See Jerez v. Republic of Cuba*, 775 F.3d 419, 424 (D.C. Cir. 2014). For example, a foreign government could be sued in U.S. courts if one of its agents mailed an "anthrax package or bomb" from foreign soil to the United States, and the bomb caused an injury in the United States. *Id.*

By contrast, other courts—including another D.C. Circuit panel—have concluded that the entire tort rule precludes suits against foreign sovereigns unless a foreign agent *started and completed* both a tortious act and a tortious injury in the United States. *See Doe v. Fed. Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017); *Broidy Capital Mgmt., LLC v. Qatar*, No. 2:18-cv-2421-JFW-E, 2018 WL 6074570 (C.D. Cal. Aug. 8, 2018); *Greenpeace, Inc. v. State of France*, 946 F. Supp. 773, 786 (C.D. Cal. 1996). Applying this stringent entire tort doctrine, the *Doe* court and the *Broidy* court both concluded that foreign sovereigns could not be sued for transnational hacking: *i.e.*, using foreign agents located abroad to hack into computers located in the United States. *Doe*, 851 F.3d at 10; *Broidy*, 2018 WL 6074570 at *4-5. In such transnational hacks, the *Doe* court explained, the tortious act begins abroad, and therefore cannot form the basis for a lawsuit in the United States. *See Doe*, 851 F.3d at 10. Presumably relying on *Doe* and *Broidy*, Russia argues that the non-commercial tort exception is not applicable here.

This Court is not bound by *Doe* or *Broidy* and should not follow the flawed logic of those decisions. As noted above, the "entire tort" rule is a judicial gloss that Courts have placed on the test of the FSIA. *In re Terrorist Attacks on Sept. 11, 2001*, 714 F.3d at 116; *Cabiri*, 165 F.3d at 200 n.3. The apparent purpose of this judicial gloss is to prevent the flood of ligation—and the

strained international relations—that could occur if foreign governments could be sued in the United States for tortious acts that occurred entirely abroad, but had some sort of effect in the United States. *See Jerez*, 775 F.3d at 424 (applying the entire tort rule in a case where defendant was injected with hepatitis C in Cuba, moved to the United States, and then brought suit against Cuba in a U.S. court); *In re Terrorist Attacks on Sept. 11, 2001*, 714 F.3d at 116 (explaining that the entire tort doctrine barred suit in a case where a tortious act was completed on the high seas, but the injured plaintiff brought suit in the United States (citing *Amerada Hess*, 488 U.S. at 428)).

But courts can close the floodgates—and preserve international relations—by construing the "entire tort" doctrine to permit suit when a foreign sovereign *completes* both a tortious act and a tortious injury on U.S. soil (rather than construing the doctrine to permit suit when a foreign sovereign *starts and completes* a tortious act and a tortious injury on U.S. soil). A unanimous D.C. Circuit panel adopted this narrow view of the entire tort doctrine in *Jerez*, when it suggested, in dicta, that a foreign government could be sued in U.S. courts if it mailed an "anthrax package or bomb" from foreign soil to the United States, and the bomb caused an injury in the United States. 775 F.3d at 424. In that scenario, the foreign sovereign's tortious act (*i.e.*, sending the dangerous package) would begin abroad, but it would be completed in the United States and cause injury in the United States; thus, the tort would be committed "entirely in the United States." *Id.* The *Jerez* court's approach is eminently sensible: it protects U.S. residents from foreign sovereigns who target them while they are on U.S. soil, but preserves immunity for torts committed abroad.

Neither *Doe* nor *Broidy* attempted to explain why the *Jerez* court's narrow version of the "entire tort" doctrine is inconsistent with the policies underlying the FSIA. Instead, both decisions seemed to rest on an interpretation of the word "entire" to conclude that the entire tort rule bars suits for transnational torts. *See Doe*, 851 F.3d at 10; *Broidy*, 2018 WL 6074570 at *4-5. That plain

meaning approach would make sense if the word "entire" appeared in the FSIA—or in any other statute—but it does not. As the Second Circuit has recognized, the "entire tort" rule is judicially crafted and judicially named. *In re Terrorist Attacks on Sept. 11, 2001*, 714 F.3d at 116; *Cabiri*, 165 F.3d at 200 n.3. Thus, there is no textual reason to stretch the entire tort rule as far as the *Doe* and *Broidy* courts did; instead, courts should consider the purpose of the doctrine, which is well-served by a rule permitting suit when a foreign sovereign completes a tortious act on U.S. soil.

In any event, even if the Court agrees that *Doe* and *Broidy* correctly described the contours of the entire tort rule, the DNC can still assert claims against Russia and the GRU. The Complaint, unlike the complaints in *Doe* and *Broidy*, alleges that a foreign sovereign is liable for trespass and trespass to chattels. And at least some of the relevant trespasses occurred entirely within the United States.

Crucially, a defendant can commit a trespass in several ways, including: (1) by *sending* something harmful onto someone else's land or chattels; and (2) by *leaving* something harmful on someone else's land or chattels. *See, e.g.*, Restatement (Second) of Torts §§ 161, 217, 221 (1965); *Lacy v. Sutton Place Condo. Ass'n, Inc.*, 684 A.2d 390, 393 (D.C. 1996). Thus, when a defendant sends something damaging onto a plaintiff's land or chattels, and then leaves the damaging object there for a period of time, the plaintiff has at least *two* causes of action against the defendant. *See Gaetan v. Weber*, 729 A.2d 895, 898 (D.C. 1999) ("[T]respass is a continuous tort giving rise to *successive causes of action* until the trespass has ended." (emphasis added)); Restatement (Second) of Torts § 217, cmt. f ("The actor may commit a *new* trespass [to chattles] by continuing an intermeddling which he has already begun . . . ." (emphasis added)); *id.* § 161 (a defendant can commit a trespass by "the continued presence" of something that she "tortiously placed" on the

plaintiff's property). Either form of trespass is a "strict liability offense": "[A] complaint for trespass need not allege any foreseeability, expectation, or anticipation of injury by the defendant." *AES Corp. v. Steadfast Ins. Co.*, 283 Va. 609, 623 n.1 (2012) (Mims, J., concurring).

Applying those principles, the DNC can bring at least two trespass claims against Russia: one for *sending* malware to/installing malware on the DNC's servers, and a second for *leaving* the malware on the servers. Even if the Court follows *Doe and Broidy*, and finds that installing the malware on the DNC's servers was a transnational tort, it is clear that *leaving* the malware on the DNC's servers was a separate tort committed entirely within the United States. This is true even if Russian operatives, like the defendants in *Doe*, formed the intent to commit their crimes abroad (because trespass is a strict liability offense that does not turn on a defendant's intent). *Cf. Doe*, 851 F.3d at 10 (suggesting that the relevant tort did not occur entirely in the United States, in part because the defendants only committed a tort if they intentionally intruded upon the plaintiff's privacy, and "the tortious intent aimed at [the plaintiff] plainly lay abroad").

The DNC Complaint also includes allegations that GRU operatives committed common law conversion by exfiltrating some of the DNC's computer files from servers in Virginia and D.C. to a server in Illinois (before sending the files back to Russia). *See* ¶ 286; *Hartzell Fan, Inc. v. Waco, Inc.*, 256 Va. 294, 301-02 (1998) ("Conversion includes any distinct act of dominion wrongfully exerted over property that is in denial of, or inconsistent with, the owner's rights."). This tort also was committed entirely within the United States, even under the exacting test adopted by the *Doe* court. The tortious act occurred domestically because the files traveled from one server within the United States to a second server in the United States. And there is no need to show that tortious intent occurred domestically because conversion, like trespass, is a strict liability tort. *See Poggi v. Scott*, 167 Cal. 372, 375 (1914) (explaining that, at common law, the "foundation for the

action of conversion rests neither in the knowledge nor the intent of the defendant. It rests upon the unwarranted interference by defendant with the dominion over the property of the plaintiff from which injury to the latter results. Therefore, neither good nor bad faith, neither care nor negligence, neither knowledge nor ignorance, are of the gist of the action.").

b. The Commercial Activity Exception Applies Here

The commercial activity exception to sovereign immunity is also applicable here. The commercial activity exception applies in any case

> based upon a commercial activity carried on in the United States by the foreign state; or upon an act performed in the United States in connection with a commercial activity of the foreign state elsewhere; or upon an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States.

28 U.S.C. § 1605(a)(2). This case is "based upon a commercial activity carried on in the United States."

(1) This Case is Based Upon a Commercial Activity

This case is "based upon a commercial activity"—namely, theft of trade secrets. Whether an activity is "commercial" is "determined by reference to the nature of the course of conduct or particular transaction or act, rather than by reference to its purpose." 28 U.S.C. § 1603(d). Thus, when a court considers whether a particular activity is commercial, "the question is not whether the foreign government is acting with a profit motive or instead with the aim of fulfilling uniquely sovereign objectives. Rather, the issue is whether the particular actions that the foreign state performs (whatever the motive behind them) are the *type* of actions by which a private party engages in trade and traffic or commerce." *Weltover*, 504 U.S. at 614 (internal quotation marks omitted). Applying these principles, the Sixth Circuit has recognized that theft of "trade secrets" can constitute "commercial activity carried on in the United States" because stealing trade secrets is an economic activity in which private parties engage. *Gould, Inc. v. Pechiney Ugine Kuhlmann*,

853 F.2d 445, 453 (6th Cir. 1988), *abrogated on other grounds by Weltover*, 504 U.S. 607. This is so even if the "motive" for sealing the trade secrets is advancing a foreign state's policy objectives, rather than earning a profit or obtaining an economic benefit over a rival. *Weltover*, 504 U.S. at 614.

Russia argues that it was not engaged in a commercial activity when it stole Plaintiff's trade secrets because the theft was carried out by military officers following military orders, ¶ 101, and a military attack is "a quintessential sovereign act." Russia Statement of Immunity 3. Contrary to Russia's suggestion, however, the DNC is not suing Russia for its entire military campaign to influence the 2016 election; instead, it is suing over discrete acts (of theft) taken in furtherance of that operation. And the Supreme Court has recognized that it is permissible to sue a sovereign over discrete military acts if those acts could also be taken by private citizens in a commercial setting. *See Weltover*, 504 U.S. at 614-15 ("[A] contract to buy army boots or even bullets is a 'commercial' activity, because private companies can similarly use sales contracts to acquire goods[.]"); *see also Texas Trading & Mill. Corp. v. Fed. Republic of Nigeria*, 647 F.2d 300, 310 (2d Cir. 1981) ("Nigeria's activity here [contracting to buy cement] is in the nature of a private contract for the purchase of goods. Its purpose to build roads, army barracks, whatever is irrelevant."), *overruled on other grounds by Frontera Res. Azerbaijan Corp. v. State Oil Co. of Azerbaijan Republic*, 582 F.3d 393 (2d Cir. 2009); *Rote v. Zel Custom Mfg. LLC*, 816 F.3d 383, 391 (6th Cir. 2016) (internal citations omitted) ("whether the ammunition [at issue in the case] was used or intended for military purposes is of no consequence."); *UNC Lear Servs., Inc. v. Kingdom of Saudi Arabia*, 581 F.3d 210, 217 (5th Cir. 2009) ("The SPAGE contract for the repair and replacement of goods is a commercial activity, regardless of the product's end use for a military purpose."); *McDonnell Douglas Corp. v. Islamic Republic of Iran*, 758 F.2d 341, 349

(8th Cir. 1985) ("In sum, the language of FSIA, its legislative history and recent case authority all confirm conclusively that the intent of the purchasing sovereign to use the goods for military purposes does not take the transaction outside of the "commercial" exception to sovereign immunity.").

Russia also contends that this case is analogous to *Broidy*, where the court rejected the argument that Qatar was engaged in commercial activity when it hacked into a private computer network. Russia Statement of Immunity 5. But *Broidy*'s analysis on this point is distinguishable. While the *Broidy* plaintiff brought trade secret claims against Qatar, he did not argue that Qatar's theft of trade secrets was commercial activity; instead, he made the broader point that "sophisticated cyber-attack[s] and information campaign[s]" are activities in which private companies engage. *Broidy*, 2018 WL 6074570 at *9 (internal quotation marks omitted). Even if some cyber attacks do not qualify as commercial activity, others clearly do: stealing proprietary software and other trade secrets to gain a leg up on a rival is quintessentially commercial. *See Gould, Inc.*, 853 F.2d at 453.

Finally, Russia contends that "there is no allegation of profit making here." Russia Statement of Immunity 6. The Supreme Court, however, has rejected the suggestion that a sovereign's conduct must be profit making in order to be commercial; to the contrary, it has held that a sovereign's acts may be commercial even if the sovereign does not receive "fair value" or "consideration" for its goods or services. *Weltover*, 504 U.S. at 616.

(2) Russia's Commercial Activity Was Carried on in the United States

Russia's theft of trade secrets was "carried on in the United States." 28 U.S.C. § 1605(a)(2). Commercial activity is carried on in the United states when it "ha[s] substantial contact with the United States." *Id.* § 1603(e). Russia does not dispute that its theft of trade secrets had substantial

contact with the United States. Nor could it reasonably do so: The relevant trade secrets were stolen from servers located in the United States. Thus, the commercial activity exception to sovereign immunity—like the non-commercial tort exception—is squarely applicable here.

2. *The Political Question Doctrine Does Not Apply Here (Responding to: Russia Statement of Immunity 7-9)*

Russia next claims that the political question doctrine bars this Court from considering Plaintiff's claims against Russia. The political question doctrine is a "narrow exception to th[e] rule" that a court has "a responsibility to decide cases properly before it, even those it would gladly avoid." *Zivotofsky ex rel. Zivotofsky v. Clinton*, 566 U.S. 189, 194-95 (2012) (internal quotation marks omitted). Not every "case or controversy which touches foreign relations lies beyond judicial cognizance," and even decisions that "may have significant political overtones" may "present a justiciable controversy." *Japan Whaling Ass'n v. Am. Cetacean Soc'y*, 478 U.S. 221, 229-30 (1986) (quoting *Baker v. Carr*, 369 U.S. 186, 217 (1969)). Only "controversies which revolve around policy choices and value determinations constitutionally committed for resolution to the halls of Congress or the confines of the Executive Branch"—such as controversies requiring the "formulat[ion of] national policies or develop[ment of] standards for matters not legal in nature"—are shielded from judicial review. *New York State v. United States Dep't of Commerce*, 315 F. Supp. 3d 766, 790 (S.D.N.Y. 2018) (quoting *Japan Whaling Ass'n*, 478 U.S. at 230).

As originally articulated in *Baker v. Carr*, the political question doctrine may apply where there is:

> [1] a textually demonstrable constitutional commitment of the issue [at hand] to a coordinate political department; [2] a lack of judicially discoverable and manageable standards for resolving it; [3] the impossibility of deciding without an initial policy determination of a kind clearly for nonjudicial discretion; [4] the impossibility of a court's undertaking independent resolution without expressing lack of the respect due coordinate branches of government; [5] an unusual need for unquestioning adherence to a political decision already made; or [6] the potentiality

> of embarrassment from multifarious pronouncements by various departments on one question.

369 U.S. at 217. "The *Baker* factors are generally viewed as being listed in descending order of importance," with courts placing "a disproportionate emphasis on the first two." *Citizens for Responsibility and Ethics in Washington v. Trump*, 276 F. Supp. 3d 174, 193 (S.D.N.Y. 2017).

Turning to the first factor, this action involves the adjudication of routine racketeering, computer crime, trade secret, and common-law tort claims. "[U]nsurprisingly, [Russia] cite[s] no constitutional text committing these issues to the political branches." *Nn aka v. Federal Republic of Nigeria*, 238 F. Supp. 3d 17, 31 (D.D.C. 2017). Rather, Russia generically recites the Executive's foreign affairs and national security authority, without any explanation of why, in this case, this Executive power must displace the traditional role of courts in adjudicating routine claims. Russia Statement of Immunity 8. By this reasoning, the political question doctrine would bar any case against a foreign sovereign. This is plainly not so: both before and since the enactment of the FSIA, courts have consistently adjudicated cases directly involving the conduct of foreign governments and foreign officials. *See, e.g., BG Group PLC v. Republic of Argentina*, 572 U.S. 25, 45 (2014); *Republic of Mexico v. Hoffman,* 324 U.S. 30, 36 (1945); *de Csepel v. Republic of Hungary*, 714 F.3d 591, 594 (D.C. Cir. 2013); *see also Japan Whaling*, 478 U.S. at 229-30 (it is "error to suppose that every case or controversy which touches foreign relations lies beyond judicial cognizance" (quoting *Baker*, 369 U.S. at 211)). "Indeed, it is more accurate to say that the political branches, through the FSIA, have specifically committed such questions to the courts." *Nn aka*, 238 F. Supp. 3d at 31 (citing *Hourani v. Mirtchey*, 793 F.3d 1, 9 (D.C. Cir. 2015)).

As to the second factor, which considers whether there are standards available to resolve the dispute, and the third factor, which considers whether judicial resolution would require a court to make a policy determination "of a kind clearly for nonjudicial discretion," Russia's argument

that "the Court is not in a position to address a private claim relating to Russian alleged actions" is as confusing as it is wrong. Russia Statement of Immunity 9. The Court is certainly in a position to address Plaintiff's "private" claims concerning the destruction of its own physical and intellectual property. Such claims are the bread and butter of our judicial system. *See Hourani*, 796 F.3d at 8-9 (rejecting application of political question doctrine where "[t]he standards needed to resolve the Houranis' racketeering, extortion, and defamation claims are the workaday tools for decision-making that courts routinely employ"); *Nn aka*, 238 F. Supp. 3d at 31 ("This case involves common law contract, quasi-contract, and tort claims against a foreign sovereign—all of them governed by standards that courts routinely employ." (internal quotation marks omitted)). Russia's argument that the United States is "in the midst" of an "ongoing and evolving response" to Russia's broad election interference scheme is irrelevant. Russia Statement of Immunity 9.[39] Russia does not identify—nor does there exist—any policy determination "of a kind clearly for nonjudicial discretion" the Court would be required to make in adjudicating Plaintiff's claims. *Baker*, 369 U.S. at 217.

Finally, Russia argues in a conclusory manner that the fourth, fifth, and sixth factors warrant invocation of the political question doctrine because (a) "the Executive is already committed to a course of action to combat these actions" and (b) "the Judiciary's involvement in the dispute would undermine the United States' ability to speak with 'one voice' on an issue of foreign affairs and national security." Russia Statement of Immunity 9. Russia does not explain

[39] It is unclear whether Russia refers to some diplomatic activities vis-a-vis the Russian government, the Special Counsel's investigation into Russian interference (which is now complete), or some other "ongoing and evolving response." Regardless, there is no explanation of how or why any of these "diplomatic activities" would be undermined by the Court's resolution of this civil action.

what actions the Executive has supposedly committed to, nor does it explain why the Court's adjudication of routine, civil claims would contradict these Executive actions or undermine the "voice" of another branch. In fact, courts routinely adjudicate civil cases against entities that are also facing criminal charges from the Executive branch. Russia's self-serving speculative concerns do not warrant the invocation of the political question doctrine.

3. *Venue Is Proper in this District (Responding to: Russia Statement of Immunity 9-10)*

Finally, Russia argues that venue does not lie in this judicial district because "virtually all of the alleged U.S.-based conduct took place" in Virginia and D.C. Russia Statement of Immunity 10. Not so. "[A] civil action against a foreign state . . . may be brought . . . in any judicial district in which a substantial part of the events or omissions giving rise to the claim occurred . . . ." 28 U.S.C. § 1391(f). Russia claims that the only events that allegedly occurred in New York are the Trump Tower meeting and a dinner between Manafort and Kilimnik, and concludes that these allegations do not constitute a "a substantial part of the events or omissions." But, just like WikiLeaks, Russia's out-of-hand dismissal of these allegations ignores the centrality of these meetings to Plaintiff's claims.[40] *See supra* Section IV.H.3.a. Thus, "a substantial part of the events" "giving rise to [Plaintiff's] claims" occurred in New York. 28 U.S.C. § 1391(f). Moreover, and independent of the foregoing, venue is proper under 18 U.S.C. § 1965, as explained above at Section IV.H.3.a.

[40] That this conduct does not "constitute acts of [Russia]" is irrelevant, Russia Statement of Immunity 10, because the venue statute does not require an examination of *each* Defendant's acts in the forum. Nevertheless, the Complaint expressly alleges that Russia made an offer of assistance to the Trump Campaign and participated in the Trump Tower meeting in New York through its representatives. ¶ 137.

V. CONCLUSION

For the foregoing reasons, the Court should deny the Motions to Dismiss in their entirety and reject Russia's Statement of Immunity.[41]

April 18, 2019

Respectfully submitted,

/s/ Joseph M. Sellers

Michael Eisenkraft
Cohen Milstein Sellers & Toll PLLC
88 Pine St.
14th Floor
New York, NY 10005
(212) 838-7797

meisenkraft@cohenmilstein.com

Joseph M. Sellers
Geoffrey A. Graber
Julia A. Horwitz
Alison S. Deich
Eric S. Berelovich
Cohen Milstein Sellers & Toll PLLC
1100 New York Ave. NW ● Fifth Floor
Washington, DC 20005
(202) 408-4600

jsellers@cohenmilstein.com
ggraber@cohenmilstein.com
jhorwitz@cohenmilstein.com
adeich@cohenmilstein.com
eberelovich@cohenmilstein.com

Attorneys for Plaintiff

[41] Because leave to amend should be freely given when justice so requires, Fed. R. Civ. P. 15(a)(2), and because the DNC filed the Complaint "before the Court had a chance to address the merits of [its] case," any claims that the Court dismisses should not be dismissed with prejudice. *Cenedella v. Metro. Museum of Art*, 348 F. Supp. 3d 346, 363 (S.D.N.Y. 2018) (Koeltl, J.).

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 2.D. of the Individual Practices of Judge John G. Koeltl, I, Joseph M. Sellers, certify that this memorandum of law complies with the Court's April 15, 2019 Order, ECF No. 240, because it is less than 140 pages, and that this brief complies with the Court's formatting rules.

Dated: April 18, 2019
Washington, D.C.

/s/ Joseph M. Sellers
Joseph M. Sellers

Attorney for Plaintiff