IN THE COURT OF COMMON PLEAS
LANCASTER COUNTY, PENNSYLVANIA

AO ALFA-BANK	
Plaintiff,	Case No.
v.	
JOHN DOE	CIVIL ACTION – LAW **CI-20-04003**
Defendants.	JURY TRIAL DEMANDED

COMPLAINT FOR DAMAGES

1. This is an action arising under the federal Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. § 1961 *et seq.* Plaintiff AO Alfa-Bank ("Alfa Bank") seeks damages for injuries caused by the unknown John Doe defendants' pattern of racketeering activity.

INTRODUCTION

2. Alfa Bank brings this action to seek redress from the unknown actors who perpetrated a sustained series of highly sophisticated cyberattacks against it in 2016 and 2017. This action is in no way related to U.S. or international politics, nor is it an attempt to support or harm, or to align Alfa Bank with, any candidate or political party. As a victim of deliberate, malicious, and damaging cyberactivity, Alfa Bank seeks simply to recoup its losses by identifying the unknown actors who carried out the cyberattacks, obtaining complete relief from those actors, and restoring its global reputation as the leading private bank in Russia.

3. The unknown John Doe defendants ("Defendants") executed a highly sophisticated cyberattacking scheme to fabricate apparent communications between Alfa Bank, one of Russia's

6-12-2020
$173.25 RmD
Ack 656 92533
receipt 123269

largest privately owned commercial banks, and the Trump Organization, President Donald Trump's namesake company, in the months leading up to and immediately following the 2016 U.S. Presidential election. Upon information and belief, Defendants' efforts were part of a broader disinformation campaign aimed at improperly linking Alfa Bank to President Trump's electoral campaign; sowing confusion and polarizing the U.S. public by pitting the predominant political parties against one another; and, ultimately, leading the U.S. public to question the legitimacy of the results of the 2016 election.

4. Upon information and belief, Defendants are members of a group who share a common purpose of using offensive cyber capabilities to develop and execute disinformation campaigns with the intent to disrupt the activities of governments, corporations, and individuals.

5. Upon information and belief, Defendants fraudulently manufactured and manipulated the Domain Name System ("DNS") resolution process, discussed below, to create the false appearance of a covert communication channel between Alfa Bank and the Trump Organization, in at least two separate and distinct ways.

6. First, from at least May 2016 through at least September 2016, Defendants sent "spoofed" emails purporting to come from the Trump Organization to Alfa Bank. Tricked into thinking that the emails were authentic, Alfa Bank's servers responded by sending DNS "lookups" to request information from the Trump Organization server. Observers interpreted the resulting exchange of network traffic between Alfa Bank servers and a Trump Organization server as evidence of secret communications between Alfa Bank employees and members of the Trump Organization. This scheme of cyberattacks involved a series of up to 100 or more separate but related attacks. In this way, Defendants interfered with and deprived Alfa Bank of its exclusive use and control of its servers.

7. As part of this scheme, upon information and belief, computer scientists and researchers who have access to and monitor nonpublic DNS activity "discovered" the manipulated and curated data showing the apparent exchange of DNS data between Alfa Bank and the Trump Organization. Upon information and belief, Defendants alerted these scientists and researchers to the DNS data, with the intent that the scientists and researchers publicize the data. And, indeed, this is precisely what happened. The scientists and researchers who obtained the nonpublic DNS data deliberately leaked portions of that data to other scientists and researchers and, ultimately, to the media. Critically, the DNS data showed Alfa Bank's communication relationships, including the number and frequency of emails between Alfa Bank and unique third parties, and the number and frequency of visits from Alfa Bank to unique websites owned by third parties. This data revealed highly sensitive and confidential information, including Alfa Bank's clients, business partners, suppliers, trade secrets, and unique software used for internal services. Defendants' actions thus proximately caused a data breach that exposed Alfa Bank's confidential business information, thereby depriving Alfa Bank of its property interest in that information.

8. Second, upon information and belief, Defendants carried out an independent but related scheme of cyberattacks in February and March 2017 to further bolster the alleged evidence of covert connections between Alfa Bank and the Trump Organization. On February 18, 2017; March 11, 2017; and March 13, 2017, Defendants sent Alfa Bank over 20,000 DNS requests that appeared to combine a Trump Organization domain name with an Alfa Bank domain name purposefully to create the illusion of secret communications between the two entities. Upon information and belief, Defendants perpetrated these cyberattacks to bolster their disinformation campaign that sought falsely to tie Alfa Bank to President Trump's electoral efforts. Through this

scheme, Defendants interfered with and deprived Alfa Bank of its exclusive use and control of its servers.

9. Beginning in October 2016 and persisting through the present day, media outlets have interpreted the manipulated and curated DNS log data as explosive evidence that Alfa Bank illegally interfered in the 2016 U.S. presidential election on behalf of then-candidate Trump and continued illicit communications with President Trump throughout the presidential transition and the beginning of the new administration. Journalists have pointed to the alleged covert communication channel between Alfa Bank servers and the Trump Organization server as the mechanism through which then-candidate Trump's campaign and the Russian government coordinated their efforts to increase the likelihood that President Trump prevailed in the election.

10. Alfa Bank in fact engaged in no communications with the Trump Organization in 2016 or 2017 beyond the falsely generated and inauthentic DNS queries. Indeed, Alfa Bank has never had any business dealings with the Trump Organization. Three prominent U.S. cybersecurity firms have reviewed all available evidence and found nothing suggesting any intentional or covert communications directed by the Trump Organization and Alfa Bank. The Federal Bureau of Investigation ("FBI"), moreover, investigated supposed links between Alfa Bank and the Trump Organization and ultimately concluded that there were "no such links." Special Counsel Robert S. Mueller, III likewise testified that allegations of ties between Alfa Bank and the Trump Organization were "not true."

11. Nevertheless, despite these definitive findings, the narrative that Alfa Bank communicated with the Trump Organization to coordinate election-interference efforts—falsely created and shaped by Defendants—persists in media circles and the public consciousness. As a direct and reasonably foreseeable result of Defendants' unlawful conduct, Alfa Bank has suffered damage to its business and property. Among other things, Alfa Bank has been forced to hire legal counsel and expend considerable resources to defend itself against the baseless allegations stemming from Defendants' actions, and it has suffered a loss of income through disruption to existing and prospective business transactions caused by Defendants' actions. Alfa Bank seeks to recoup the monetary losses that it has suffered as a direct result of Defendants' unlawful scheme.

PARTIES

12. Plaintiff Alfa Bank is a major banking institution, registered and licensed in the Russian Federation. Its registered office is located at 27 Kalanchevskaya Street, Moscow, Russia 107078. Alfa Bank has a branch network consisting of approximately 750 offices across Russia, as well as a subsidiary bank in the Netherlands and financial subsidiaries in the United Kingdom and Cyprus.

13. Defendants John Doe *et al.* are the unknown persons or entities who are members of the association in fact ("Disinformation Enterprise") that perpetrated cyberattacks against Alfa Bank in 2016 and 2017 designed to produce data purporting to show communications between Alfa Bank and the Trump Organization. Defendants themselves conducted or participated in the Disinformation Enterprise as outlined in this Complaint. Upon information and belief, the Disinformation Enterprise preexisted the events that form the basis of this action and remains in existence to this day. Upon information and belief, the objective of the Disinformation Enterprise is to spread disinformation and disrupt the activities of governments, corporations, and individuals.

14. Alfa Bank has conducted a reasonable search to determine the actual names of Defendants, but Defendants' identities remain unknown to Alfa Bank. The John Doe designation is fictitious and serves as a placeholder until Alfa Bank is able to conduct discovery and uncover the actual names of Defendants.

JURISDICTION AND VENUE

15. This Court has subject-matter jurisdiction over this action because the claims arise under RICO and the amount in controversy exceeds $50,000.00.

16. Upon information and belief, the Court has personal jurisdiction over Defendants pursuant to Chapter 53 of Title 42 of the Pennsylvania Consolidated Statutes.

17. Upon information and belief, venue is proper in this Court pursuant to Pennsylvania Rules of Civil Procedure 1006(a) or 2179 because the cause of action arose in Lancaster County, Pennsylvania, or a transaction or occurrence took place in Lancaster County, Pennsylvania out of which the cause of action arose.

FACTS

I. Network Infrastructure

18. Internet Protocol ("IP") addresses are the bases for communications on the internet. IP addresses are numerical codes (such as 66.216.133.29) that are often assigned and correspond to word-based domain names (such as "trump-email.com"). The DNS serves as a global directory that converts, or "resolves" the domain names (which are more easily used by humans) into an IP address (which are used by machines). The DNS is necessary for facilitating communication on the internet, as it takes the domain name input by a human user and resolves it into the corresponding IP address that is needed to send the communication to the appropriate recipient.

19. When a domain on one server searches for a domain name on another server, there is a "lookup" or "ping" between the two servers indicating that communication was attempted. This lookup (which is referred to as a "DNS request" or "DNS query") does not mean that a substantive communication actually occurred—e.g., that an email was sent and received—but merely that one server was looking for a specific IP address on another server. Domains and domain names are hosted by DNS servers. The appropriate DNS server fields the lookup and tries to resolve the DNS request by locating the correct IP address.

20. Critically, data logs of these DNS requests can reveal highly sensitive and confidential information. A reviewer with knowledge of DNS data can take the raw data from DNS logs and extract meaningful, substantive information. With respect to a business like Alfa Bank, for instance, an elementary analysis of raw DNS data could reveal a company's website traffic, email traffic, business partners, suppliers, trade secrets, and other similarly sensitive information. A reviewer could use the data to identify a company's communication relationships, including the number and frequency of emails between a company and unique third parties, and the number and frequency of visits from the company to unique websites owned by third parties. DNS data also could reveal software used by a company for various internal services.

21. In each of the two schemes, Defendants improperly manipulated and fabricated DNS lookups between Alfa Bank servers (located in Russia) and a Trump Organization server (located in Lancaster County, Pennsylvania).

22. Cendyn, LLC ("Cendyn") is a Florida–based marketing company that administered the Trump Organization domain that allegedly communicated with Alfa Bank servers—i.e., "trump-email.com." In June 2007, the Trump Organization retained Cendyn as its "exclusive marketing agency." (Ex. 1, *Cendyn is Tapped for Interactive Marketing Services by the Trump Organization*, Cision PRWeb (June 21, 2007), https://www.prweb.com/releases/2007/06/prweb535089.htm (last visited June 11, 2020).) In this capacity, among other tasks, Cendyn distributed marketing emails. Prior to its announcement of a business relationship with the Trump Organization, Cendyn had registered the generic domain "contact-client[.]com" in its own name. (Ex. 2, Ankura Consulting Group, *Covert Channel*

Allegation: New Data Analysis Results (Apr. 2020) at 4 (hereinafter "Ankura Report"); Ex. 3, Mandiant, *Alfa-Bank Investigation Report* (Nov. 4, 2016) at 9 (hereinafter "Mandiant Report").) In August 2009, Cendyn registered the domain "trump-email.com" in the Trump Organization's name but listed itself as the administrator. (Ex. 3, Mandiant Report at 6–8.) Two months later, Cendyn coordinated the hosting of two related domains ("trump1.client-contact.com," which was a subdomain of "contact-client.com," and "mail1.trump-email.com," which was a subdomain of "trump-email.com") on a server with the IP address 66.216.133.29. (Ex. 2, Ankura Report at 5.) GoDaddy, Inc. ("GoDaddy") hosted both parent domains and their corresponding subdomains.

23. GoDaddy used three DNS servers ("ns1.cdservices.com," "ns2.cdservices.com," and "ns3.cdservices.com") to process DNS requests. (Ex. 3, Mandiant Report at 3.) Each time any computer on the internet (including those connected to Alfa Bank's servers) sent a DNS request to try to resolve the IP address for those Trump Organization domains, the actual network traffic was directed by GoDaddy to one of the three DNS servers.

24. Cendyn contracted certain marketing functions to Listrak, a Lancaster County, Pennsylvania–based company that provides digital marketing platforms and that distributed marketing emails on behalf of Trump Hotels. Listrak owned the server with the IP address 66.216.133.29, which housed the Trump Organization domains registered and administered by Cendyn. That server is located in Lititz, Pennsylvania. Reports indicate that the Listrak server continued to "reverse resolve[] the IP address 66.216.133.29 as 'mail1.trump-email.com'" through and following the last known cyberattack committed by Defendants against Alfa Bank. (Ex. 4, Robert Graham, *Pranksters gonna prank*, Errata Security at 2 (Mar. 19, 2017) https://blog.erratasec.com/2017/03/pranksters-gonna-prank.html#.XpjCWKhKiUn (last visited June 11, 2020).) Thus, at all relevant times, DNS requests to the Trump Organization server—

including those that Defendants fraudulently generated from Alfa Bank servers—were received in Lititz, Pennsylvania.

25. Although the Trump Organization retained Serenata CRM (a German firm now doing business as NextGuest Technologies) to perform its marketing services in March 2016, the business relationship between Cendyn and the Trump Organization continued for another year. Specifically, on June 29, 2016, Cendyn extended the registration for the "trump-email.com" domain for one year and remained the administrator of that domain until March 8, 2017, when it transferred the domain to the Trump Organization. (Ex. 2, Ankura Report at 10.) At least one team of researchers, moreover, identified "thousands of e-mails between Trump and Cendyn through the entire period that Alfa Bank was looking up the Trump server," such that the business relationship persisted throughout the duration of Defendants' cyberattacks. (Ex. 5, Dexter Filkins, *Was There a Connection Between a Russian Bank and the Trump Campaign?*, THE NEW YORKER, Oct. 8, 2018, https://www.newyorker.com/magazine/2018/10/15/was-there-a-connection-between-a-russian-bank-and-the-trump-campaign (hereinafter "Oct. 8, 2018 *New Yorker* article").)

26. Notably, one of the cybersecurity expert firms that reviewed the evidence related to the cyberattacks concluded that the manner in which Cendyn configured the Trump Organization domains made them vulnerable to manipulation. Specifically, the expert concluded that the domains "trump-email.com" and "contact-client.com" were set up in such a way that "a threat actor could send spoofed emails or inauthentic DNS queries masquerading as these domains" to other domains, such as those hosted on Alfa Bank servers. (Ex. 2, Ankura Report at 4.) "As a result, this inauthentic activity could force Alfa-Bank servers to repeatedly query DNS records for both of these domains even if Alfa-Bank never received a legitimate marketing email" or other communication. (*Id.*) As explained further below, Defendants exploited this vulnerability to fabricate "evidence" of a purported secret communication channel between Alfa Bank and the Trump Organization.

II. Defendants' Cyberattacks Against Alfa Bank

27. Defendants orchestrated a coordinated series of cyberattacks against Alfa Bank that took place over the course of at least ten months, and potentially longer. Upon information and belief, Defendants perpetrated these cyberattacks as part of a disinformation campaign aimed at falsely linking Alfa Bank to President Trump's electoral campaign, thereby pitting the predominant political parties against one another, leading the U.S. public to question the legitimacy of the results of the election, and undermining trust in the U.S. democratic system.

28. Upon information and belief, the Disinformation Enterprise is a highly skilled group with robust cyber offensive capabilities, as highlighted by the sophisticated nature of the attacks and the manipulation of the specialized DNS infrastructure. Indeed, only a subset of malicious cyber actors would have been capable of funding, organizing, and carrying out the attacks on Alfa Bank. Executing the cyberattacks against Alfa Bank would have required understanding precisely how the Alfa Bank servers were constructed and demanded a concerted effort over a significant amount of time. Upon information and belief, Defendants are part of a well-trained and well-funded group that existed before the cyberattacks committed against Alfa Bank, continues to exist today, and carries out cyberattacks against a range of targets. It is likely that Defendants and the Disinformation Enterprise will continue their efforts to spread disinformation and undermine U.S. institutions, including through cyber campaigns aimed at disrupting the upcoming 2020 U.S. Presidential election.

29. Upon information and belief, Defendants exploited the DNS request process to manufacture the purported connection between Alfa Bank and the Trump Organization for multiple reasons. Because DNS data is a reliable indicator of communications between two sources, upon information and belief, Defendants knew that third parties would interpret the fraudulent DNS data as highly compelling evidence that Alfa Bank in fact communicated with the Trump Organization, thereby posing particularly acute risks to Alfa Bank's business and reputation. Upon information and belief, moreover, Defendants sought to take advantage of the inherent complexities and difficulties of collecting and interpreting historic DNS data. To take just one example, different sources of DNS records often contradict each other in material ways such that focusing on a "single point of collections or DNS historical data" can lead to overlooking "clarifying context." (Ex. 2, Ankura Report at 5, 7.) Thus, upon information and belief, Defendants expected that no observers would be able to detect their manipulations, which produced the DNS activity falsely evidencing communications between Alfa Bank and the Trump Organization, until well after the 2016 U.S. Presidential election, if ever. In the meantime, Defendants anticipated that at least some individuals who reviewed the data would promote Defendants' concocted narrative of illicit communications because they would be expected to "miss[], ignore[]," or lack "access to a complete record of DNS history." (*See id.* at 19.)

A. The 2016 Cyberattack Scheme

30. As Ankura Consulting Group ("Ankura"), one of the cybersecurity experts who studied the evidence, concluded, a "likely scenario" is that Defendants "artificially created DNS activity to make it appear as though a connection" between Alfa Bank servers and a Trump Organization server "existed, for 'discovery' later." (Ex. 2, Ankura Report at 3.) Indeed, from at least May 4, 2016 until September 21, 2016, Defendants improperly connected to server networks and manipulated data on a regular basis to fool Alfa Bank's servers into looking up a domain registered to the Trump Organization—when, in the absence of this activity, Alfa Bank's servers would not have done so. Through this scheme, Defendants caused traffic on U.S.-based computer servers and networks and created the illusion of two-way communication between Alfa Bank and the Trump Organization.

31. Applying their sophistication and deep knowledge of arcane DNS infrastructure, Defendants exploited a vulnerability in the configuration of the Trump Organization server located in Lancaster County, Pennsylvania and operated by Cendyn and Listrak. In the normal course, an "SPF TXT record" accompanies an email when that email is sent. An SPF TXT record is used to confirm that emails actually have been sent by the identified sender, and not by someone falsely claiming to be the sender. An SPF TXT record performs this authentication by "specifying which hostnames, IP addresses, and/or IP ranges are permitted to send emails on behalf of a domain." (Ex. 2, Ankura Report at 13.) In the case of the Trump Organization domains, the SPF TXT records contained a list of IP ranges that it deemed legitimate, all of which are associated with hotel and hospitality companies. (*Id.* at 13–16.) Critically, however, these SPF TXT records ended with an "~all flag," which directed the recipient of an email from the "trump-email.com" domain that originated from an IP address *not* included in the verified TXT record to "identify [the email] as spam but allow it at" the recipient's direction. (*Id.* at 13, 15.) In other words, recipients did not necessarily reject emails that claimed to be from one of the Trump-related domains but originated from IP addresses not associated with those domains. This "~all flag" gateway thus allowed emails from non-Trump-related domains to appear as though they were from Trump-related IP addresses when they actually were not. Accordingly, the configuration "could . . . [have] allow[ed] an attacker"—such as Defendants—"to bypass spam identification and deliver ma[illegible] organization" as though the mail originated from the Trump Organization. (*Id.* at 13.)

32. And Defendants in fact exploited this vulnerability to manufacture purported communications between Alfa Bank and the Trump Organization, "essentially tricking" Alfa Bank servers "to perform a DNS query for a domain [they] never visited or received a legitimate email from." (Ex. 2, Ankura Report at 18.) Ankura concluded that the DNS traffic patterns that formed the basis for alleging that Alfa Bank servers had been communicating with a Trump Organization server could have been caused by Defendants' sending "spoofed emails masquerading as trump1.contact-client[.]com to Alfa-Bank," in which case "these spoofed emails would force Alfa Bank's email servers to request SPF records from contact-client[.]com." (*Id.*) When Alfa Bank's servers requested these records, the network traffic was received by the Trump Organization server in Lititz, Pennsylvania. These original spoofed emails sent by Defendants to Alfa Bank, when combined with DNS requests sent by Alfa Bank servers to a Trump Organization server, created the false illusion of secret communications between Alfa Bank and the Trump Organization.

33. Defendants' first cyberattack scheme took place over the span of nearly five months in 2016, from at least May through September. As experts have concluded, the varied timing and volume of DNS lookups suggest that they were the product of human action, not automation. (*See, e.g.*, Ex. 6, Franklin Foer, *Was a Trump Server Communicating with Russia*, SLATE, Oct. 31, 2016, at 8, http://www.slate.com/articles/news_and_politics/cover_story/2016/10/was_a_server_registered_to_the_trump_organization_communicating_with_russia.html (hereinafter "Oct. 31 2016 *Slate* article").) Defendants would have needed to sustain this scheme with near-daily manual lookups to create this pattern of activity. In other words, the 2016 scheme of cyberattacks in fact comprised a series of up to 100 or more separate but related attacks.

34. Upon information and belief, Defendants intended that computer scientists and researchers "discover" the DNS data purportedly showing communications between Alfa Bank and the Trump Organization, monitor the traffic themselves, and then publicize that data to create a narrative that Alfa Bank was illegally coordinating with President Trump's campaign and interfering in the 2016 election. Some computer scientists and researchers have access to nonpublic DNS data for purposes of cybersecurity research and monitoring, although the data remains under the exclusive control of its owner (in this case, Alfa Bank). Upon information and belief, Defendants alerted one or more of these scientists or researchers to DNS data showing the manufactured exchange of network traffic between Alfa Bank servers and Trump Organization servers, with the expectation that these scientists or researchers would publicly disclose this data and its purported significance as alleged evidence of a covert communication channel between Alfa Bank and the Trump Organization.

35. Through this scheme, Defendants deprived Alfa Bank of its property interest in its DNS data, which Alfa Bank has the exclusive right to control. Upon information and belief, Defendants caused third parties to obtain, analyze, distribute, and publicize Alfa Bank's DNS data. Alfa Bank's DNS data, in turn, contained confidential business information, including information related to Alfa Bank's business partners, suppliers, trade secrets, and unique software used for internal services. The DNS data, more broadly, revealed Alfa Bank's communication relationships, including the number and frequency of emails between Alfa Bank and unique third parties, and the number and frequency of visits from Alfa Bank to unique websites owned by third parties.

36. Defendants likewise deprived Alfa Bank of its property interest in its servers and DNS data logs by fraudulently causing Alfa Bank's servers to send lookup requests to the Trump

Organization server and manipulating the resulting records of DNS data. Alfa Bank has the exclusive right to use and control its servers. By manipulating those servers to generate fraudulent DNS requests, Defendants deprived Alfa Bank of its property interest in the servers. And, indeed, Alfa Bank's exclusive control of its servers was necessary to Defendants' scheme, as it enabled Defendants to foster the false narrative that Alfa Bank, and only Alfa Bank, could have sent DNS requests from its servers to the Trump Organization server.

B. The 2017 Cyberattack Scheme

37. Defendants carried out a separate campaign of cyberattacks against Alfa Bank over three days in 2017. As with the 2016 cyberattacks, this scheme also was designed to create the false impression of illicit communications between Alfa Bank and the Trump Organization. Upon information and belief, these attacks were intended to bolster Defendants' disinformation efforts by linking Alfa Bank with President Trump's campaign, pitting the predominant political parties against one another, delegitimizing the results of the 2016 presidential election, and undermining faith in U.S. democracy.

38. In separate attacks on February 18, 2017; March 11, 2017; and March 13, 2017, Defendants manufactured and sent over 20,000 DNS requests for invalid domain names to Alfa Bank. (Ex. 7, Stroz Friedberg LLC, *Summary of Cyber Incident Investigation* (Jul. 19, 2017) at 1 (hereinafter "Stroz Friedberg Report"); Ex. 8, *Press Statement Alfa Bank confirms it has sought help from U.S. authorities, and discloses new cyberattacks linked to Trump hoax* (Mar. 17, 2017), at 3, https://alfabank.com/news/press-statement-alfa-bank-confirms-it-has-sought-help-from-u-s-authorities-and-discloses-new-cyberattacks-linked-to-trump-hoax/ (last visited June 11, 2020) (hereinafter "Mar. 17, 2017 Alfa Bank Press Release").) Those invalid domain names appeared to combine a purported Trump Organization domain name with a purported Alfa Bank domain name. (Ex. 7, Stroz Friedberg Report at 1.) When Alfa Bank's servers sent DNS requests in response to these queries, the network traffic was received by the Trump Organization server in Lititz, Pennsylvania.

39. On February 18, 2017, Defendants sent Alfa Bank at least sixteen suspicious DNS queries. Specifically, Defendants queried the domain name "mail.trump-email.com.MOSCow.AlFaintRa.nEt" from external IP addresses. (Ex. 7, Stroz Friedberg Report at 1.) This invalid domain name combines two valid domain names associated with the Trump Organization and Alfa Bank, "mail.trump-email.com" and "moscow.alfaintra.net." Defendants intended that these DNS queries create the impression of an exchange of communications between Alfa Bank and the Trump Organization. Notably, these lookups were virtually identical to unverified DNS data that L. Jean Camp, a computer science professor at Indiana University, posted on her website in early November 2016. (Ex. 9, L. Jean Camp, "Intra Net DNS Leakage," http://ljean.com/NetworkRecords/intranet/index.html (last visited June 11, 2020).)

40. On March 11 and March 13, 2017, Defendants sent 20,000 more of these DNS requests for the same domain name. (Ex. 7, Stroz Friedberg Report at 1; Ex. 8, Mar. 17, 2017 Alfa Bank Press Release at 3.) Significantly, this exponential uptick in attacks began the day after CNN published an article stating that the FBI continued to investigate an "'odd' computer link between [a] Russian bank and [the] Trump Organization." (*See* Ex. 10, Pamela Brown & Jose Pagliery, *Sources: FBI investigation continues into 'odd' computer link between Russian bank and Trump Organization*, CNN (Mar. 10, 2017), https://www.cnn.com/2017/03/09/politics/fbi-investigation-continues-into-odd-computer-link-between-russian-bank-and-trump-organization/index.html (last visited June 11, 2020).)

41. Through this scheme, Defendants deprived Alfa Bank of its property interest in its servers and DNS data logs by fraudulently causing Alfa Bank's servers to send lookup requests to the Trump Organization server and manipulating the resulting records of DNS data. Alfa Bank has the exclusive right to use and control its servers. By manipulating those servers to generate fraudulent DNS requests, Defendants deprived Alfa Bank of its property interest in the servers. And, indeed, Alfa Bank's exclusive control of its servers was necessary to Defendants' scheme, as it enabled Defendants to foster the false narrative that Alfa Bank, and only Alfa Bank, could have sent DNS requests from its servers to the Trump Organization server. Defendants similarly deprived Alfa Bank of its exclusive control of its DNS data by fraudulently generating DNS data, thereby impairing Alfa Bank's property rights.

42. An expert retained by Alfa Bank to review evidence related to the 2017 cyberattacks, Stroz Friedberg LLC ("Stroz Friedberg"), concluded that the data was consistent with DNS traffic produced by cyberattackers. (Ex. 7, Stroz Friedberg Report at 3.)

III. "Discovery" of Defendants' Manufactured Data

43. As Defendants intended, computer scientists "discovered" Defendants' fabricated DNS data in the summer of 2016.

44. After the publication of news reports in June 2016 that Russian hackers had infiltrated the Democratic National Committee's ("DNC") computer network and looted the DNC's opposition research on then-candidate Trump, a "tightly knit community of computer scientists" worked together to uncover evidence of other network intrusions related to the upcoming U.S. Presidential election. (Ex. 6, Oct. 31, 2016 *Slate* article at 2; Ex. 5, Oct. 8, 2018 *New Yorker* article at 2.) This group, which has been described as a "Union of Concerned Nerds" or an "elite group of malware hunters," includes both academics and professionals, some of whom

reportedly worked at cybersecurity firms with close ties to federal agencies and accordingly had unparalleled access to "nearly comprehensive logs of communications between servers." (Ex. 6, Oct. 31, 2016 *Slate* article at 2–3.)

45. In late July 2016, one member of this group, who has identified himself using the pseudonym "Tea Leaves," uncovered what he initially thought was malware emanating from Russia destined for a domain with "Trump" in the domain name. Thereafter, to augment this data, Tea Leaves "began carefully keeping logs of the Trump server's DNS activity" and periodically circulated the data to the other group members. (Ex. 6, Oct. 31, 2016 *Slate* article at 3.) At least six of these computer scientists, including Tea Leaves and another member who uses the pseudonym "Max," started to comb through the data looking for abnormalities. (*Id.*; Ex. 5, Oct. 8, 2018 *New Yorker* article at 4.) The identities of these researchers, including Tea Leaves and Max, remain a mystery.

46. The researchers ultimately collected what they claimed were portions of Alfa Bank's historical DNS records spanning approximately five months, presumably using commercial databases available to them because of the nature of their employment and expertise. The researchers subsequently distributed, first among their group and later to the press, Alfa Bank's DNS logs, which allegedly showed two servers belonging to Alfa Bank pinging a hostname, "mail1.trump-email.com," that was registered to the Trump Organization and associated with the IP address 66.216.133.29. The nonpublic DNS data, which includes approximately 2800 DNS logs dated from May 4, 2016 to September 23, 2016, was circulated in a text file, the source of which was never verified. (Ex. 6, Oct. 31, 2016 *Slate* article at 8.)

47. The researchers asserted that "[t]he irregular pattern of server lookups actually resembled the pattern of human conversation—conversations that began during office hours in

New York and continued during office hours in Moscow." (*Id.* at 4.) They theorized that the pattern of activity "wasn't an attack, but a sustained relationship between a server registered to the Trump Organization and two servers registered to an entity called Alfa Bank." (*Id.*)

48. The researchers sought to bolster their theory that the DNS data evidenced a covert communication channel between Alfa Bank and the Trump Organization. First, they plotted the DNS logs against a timeline of campaign events and concluded that there were upticks in the number of pings during significant campaign events, such as the party conventions. (Ex. 6, Oct. 31, 2016 *Slate* article at 10.) Second, the researchers claimed that the Trump server was disabled after two journalists from *The New York Times* met with Alfa Bank representatives on September 21, 2016 to discuss the server allegations. (*Id.* at 11.) According to the researchers, the Trump Organization shut down the server after Alfa Bank informed it that journalists had discovered the connection between the servers. (*Id.*) Third, the researchers determined that on September 27, 2016, the Trump Organization had established a new host name, trump1.client-contact.com, that used the same IP address as the mail1.trump-email.com host name, and that an Alfa Bank server was the first to look up the new host name—an act that one journalist reported is "never random." (*Id.*)

49. Upon information and belief, Defendants flagged the fabricated DNS data for one or more of the researchers. It is unlikely that the researchers could have identified the data without knowing to look for it, given the sheer volume of DNS data. (*See, e.g.*, Ex. 6, Oct. 31, 2016 *Slate article* at 3 (describing discovery of the data as "pure happenstance—a surprising needle in a large haystack of DNS lookups").) Indeed, Max, one of Tea Leaves' colleagues, provided a forensic team with the 37 million DNS logs that the researchers had at their disposal. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 8.) Particularly given that only 2800 of the 37 million logs showed the alleged communications between Alfa Bank servers and Trump Organization servers, it is likely that Defendants pointed Tea Leaves or other researchers in the direction of the planted evidence.

IV. Publication of Defendants' Manufactured Data

50. Just as Defendants had intended, the researchers who "discovered" the fabricated data allegedly showing communications between Alfa Bank and the Trump Organization promptly moved to disclose that data to other researchers and journalists.

51. Notably, the DNS log data that the researchers reviewed is not public information. Rather, some companies, after de-duplicating the raw data and removing critical details, amass the processed DNS logs in databases that they offer commercially on a subscription basis. Other specialized entities collect and review the raw DNS data to ensure that the DNS process works effectively. Researchers and cybersecurity professionals use this nonpublic data to look for evidence of misconfigurations, outages, manipulation, malicious activity, and surveillance. At all times, the data remains under the exclusive control of the owner of that data, which has the right to decide how to use the data and whether to publicize it. As Ankura explained with specific reference to Alfa Bank, "only entities with specialized and non-public access to DNS infrastructure would know that Alfa-Bank . . . [was] sending repeated DNS queries to Trump associated domains." (Ex. 2, Ankura Report at 11.)

52. Despite the nonpublic nature of DNS data and Alfa Bank's exclusive ownership of its DNS data, the researchers disclosed excerpts of their underlying data to news media outlets, including *The New York Times*, *Washington Post*, *Reuters*, *Daily Beast*, *Vice*, *The Intercept*, and *Slate*. (Ex. 11, Sam Biddle, Lee Fang, et al., *Here's the Problem with the Story Connecting Russia to Donald Trump's Email Server*, THE INTERCEPT (Nov. 1, 2016), at 1–3, https://theintercept.com/2016/11/01/heres-the-problem-with-the-story-connecting-russia-to-donald-trumps-email-server/ (last visited June 11, 2020) (hereinafter "Nov. 1, 2016 *The Intercept* article"); Ex. 6, Oct. 31, 2016 *Slate* article at 4.) Specifically, the researchers provided each media outlet with three documents: (i) an "academia-style white paper" about the so-called Trump server; (ii) an analysis of the white paper; and (iii) a "sprawling dossier on Alfa Bank," described as having been "compiled with the exhaustive detail of a political oppo[sition] team, not a university researcher." (Ex. 11, Nov. 1, 2016 *The Intercept* article at 4.) Tea Leaves himself reportedly posted data on the dark web, *id.* at 6, and an unnamed researcher using the handle "LeavesTeaLeaves" posted the data in a Reddit thread. (Ex. 6, Oct. 31, 2016 *Slate* article at 11.) Then, on October 5, "leavestea" created a post on a WordPress blog that indicated that then-candidate Trump and Russia's largest bank communicated via a "hidden server." (Ex. 12, *Trump's Russian Bank Account*, WordPress (Oct. 5, 2016), https://gdd53.wordpress.com/2016/10/05/first-blog-post/.) *Slate* published Franklin Foer's explosive, yet false story of secret server communication on October 31, 2016—eight days before the Presidential election. Scores of additional news outlets subsequently reported that same story, making Alfa Bank a household name across the U.S. population, synonymous with Russian election interference.

53. Foer's article relied on interviews with Tea Leaves and two unnamed accomplices, as well as the opinions of well-known experts in the cybersecurity field who had received and examined the logs. Among these experts was L. Jean Camp, a computer science professor at Indiana University. Camp had access to the researchers' DNS log data and reportedly knows the identity of Tea Leaves and the author of the so-called Alfa Bank dossier. (Ex. 6, Oct. 31, 2016 *Slate* article at 4; Ex. 11, Nov. 1, 2016 *The Intercept* article at 3.) Since the publication of the *Slate* story, Camp has spoken out in support of the threat actors' theory of secret server communication and the authenticity of the source data. (*See, e.g.*, Ex. 13, Franklin Foer, *Trump's Server, Revisited,* SLATE (Nov. 2, 2016), at 5, https://slate.com/news-and-politics/2016/11/the-trump-server-evaluating-new-evidence-and-countertheories.html (last visited June 11, 2020).) On November 2, 2016, shortly after the publication of Foer's article and in the wake of ensuing criticism, Camp posted the DNS logs that she had in her possession to her personal website. (Ex. 14, *Some Network Data*, Transparent Network Data, http://ljean.com/NetworkData.php (last visited June 11, 2020).) In addition to Camp, Foer relied on the opinions of cybersecurity experts Paul Vixie (who also received the nonpublic DNS logs directly from the researchers), Richard Clayton, Christopher Davis, and Nicholas Weaver. (Ex. 6, Oct. 31, 2016 *Slate* article at 5, 7–8.)

54. News articles relying on the fabricated DNS data to link Alfa Bank to illegal efforts to interfere in the 2016 U.S. Presidential election continued unchecked for years—and, indeed, persist to this day. To take one particularly notable example, Dexter Filkins published a lengthy exposé on the server allegations in *The New Yorker* in October 2018. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 3.) Similar stories continue to surface with the effect of dredging up the false and discredited narrative that Alfa Bank maintained a secret communication channel with the Trump Organization in 2016 and 2017.

V. Initiation of Investigations Into Alfa Bank

55. After receiving purported leads from several sources, the FBI began investigating allegations of a secret communication channel between Alfa Bank and the Trump Organization in August and September 2016. In particular, at least three primary sources provided the FBI with information underpinning its investigation.

56. First, Max's attorney contacted the FBI in September 2016 to alert officials to a potential upcoming story in *The New York Times* about the server allegations. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 3.)

57. Second, also in September 2016, Michael Sussmann, an attorney representing the DNC and Hillary Clinton's campaign, gave FBI General Counsel James Baker information about a purported "surreptitious channel of communications" between a part of then-candidate Trump's business and a Russian organization allegedly associated with the Russian government. (Ex. 15, House Comm. on Judiciary & Comm. on Gov't Reform & Oversight, U.S. H.R., Interview of James A. Baker, 105 Cong., at 119–23 (Oct. 18, 2018).) Sussmann similarly delivered a briefing and supporting documents to an intelligence agency. (Ex. 16, Permanent Select Comm. on Intelligence, U.S. H.R., Interview of Michael Sussmann, at 28–30, 52–54, 60–61 (Dec. 18, 2017).) Sussman obtained this information in the summer of 2016 from an unidentified client. (*Id.* at 53–56, 60–61.)

58. Third, Glenn Simpson, co-founder of Fusion GPS ("Fusion"), a commercial research and strategic intelligence firm in Washington, DC, provided information that ultimately was shared with the FBI. The DNC had engaged Fusion to conduct opposition research on then-candidate Trump. Fusion, in turn, retained Christopher Steele and Steele's company, Orbis Business Intelligence Ltd., who shared information with Simpson that related to purported communications between Alfa Bank servers and the Trump Organization server. Steele discussed the server allegations with Bruce Ohr, a senior official at the U.S. Department of Justice ("DOJ"), on September 23, 2016. (Ex. 17, Office of Inspector Gen., U.S. Dep't of Justice, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation*, Oversight and Review Division Report 20-012 (Dec. 2019), at 274–75 (hereinafter "OIG Report").) Simpson later indicated that "people" had given his group "information" that he described as "a bunch of data" "beyond [his] competence." (Ex. 18, Sen. Judiciary Comm., U.S. S. Interview of Glenn Simpson at 304:21–305:13 (Oct. 18, 2018).)

59. On September 19, 2016, Steele provided election reporting to the FBI. (Ex. 17, OIG Report at vi (finding that Steele's reporting "playėd a central and essential role in the FBI's and [DOJ's] decision to seek the FISA order").) Thereafter, in October 2016, Steele met with two officials at the U.S. Department of State: Kathleen Kavalec, Deputy Assistant Secretary in the Bureau of European and Eurasian Affairs; and Jonathan Winer, Deputy Assistant Secretary in the Bureau of International Narcotics and Law Enforcement Affairs. (*Id.* at 117.) In her notes from that meeting, Kavalec recounted that "Peter [sic] Aven of Alfa Bank has been the conduit for secret communications between the Kremlin and Manafort; messages are encrypted via TOR software and run between a hidden server managed by Alfa Bank." (Ex. 19, Rowan Scarborough, *Dossier author Christopher Steele breaks silence with IG report rebuttal*, WASH. TIMES (Dec. 19, 2019), at 5, https://www.washingtontimes.com/news/2019/dec/16/christopher-steele-trump-dossier-author-rebuts-ig-/ (last visited June 11, 2020) (hereinafter "Dec. 16, 2019 *Washington Times* article"); Ex. 17, OIG Report at 117.) On October 13, 2016, Kavalec reportedly downloaded Steele's summary of the server allegations from a private cloud storage service and transmitted it to FBI section chief Stephen Laycock. (Ex. 20, John Solomon, *Christopher Steele's nugget of fool's gold was easily disproven — but FBI didn't blink an eye*, THE HILL (May 21, 2019), at 2, https://thehill.com/opinion/white-house/444884-christopher-steeles-nugget-of-fools-gold-was-easily-disproven-but-fbi (last visited June 11, 2020); Ex. 17, OIG Report at 119.) In addition, Simpson reportedly met with Ohr and shared information regarding the alleged server link in December 2016. (Ex. 19, Dec. 16, 2019 *Washington Times* article at 5; Ex. 21, John Solomon, *Move over 'grassy knoll,' the Trump-Russia bank tale joins unproven conspiracies list*, THE HILL (Oct. 14, 2018) at 2, https://thehill.com/opinion/white-house/411209-move-over-grassy-knoll-the-trump-russia-bank-tale-joins-unproven (last visited June 11, 2020).) Simpson also pitched the false server story to multiple journalists.

60. The FBI reportedly used these sources of information to seek a warrant from the Foreign Intelligence Surveillance Court authorizing it to wiretap the server in Trump Tower for the purpose of investigating Alfa Bank and another Russian bank, including those banks' possible connections to the Trump campaign. The court granted the FBI's request in October 2016. (*See generally* Ex. 17, OIG Report, at i–xix; *see also* Ex. 22, Louise Mensch, *EXCLUSIVE: FBI 'Granted FISA Warrant' Covering Trump Camp's Ties to Russia*, HEAT STREET (Nov. 7, 2016), at 1–2, https://archive.is/xFqPB (last visited June 11, 2020).)

61. At around the same time, FBI agents visited Listrak's offices in Lititz, Pennsylvania to obtain information from the company. (Ex. 23, Tim Mekeel, *FBI gets Lititz firm's help in probe of Russian bank's 'odd' interest in Trump Hotels marketing emails*, LANCASTER ONLINE (Mar. 10, 2017), at 1, https://lancasteronline.com/news/local/fbi-gets-lititz-firm-s-help-in-probe-of-russian/article_ef5d5ed0-05ae-11e7-a003-471e5543b26a.html (last visited June 11, 2020); Ex. 5, Oct. 8, 2018 *New Yorker* article at 7.) Ross Kramer, Listrak's CEO, told reporters that he "gave them everything they asked for." (Ex. 5, Oct. 8, 2018 *New Yorker* article at 7.)

62. The FBI's investigation continued into 2017. In March 2017, for instance, FBI agents met with Daniel Jones, the president of the Penn Quarter Group and a former FBI investigator and Senate aide. (Ex. 24, Rowan Scarborough, *FBI refuses to say if it has received Daniel Jones' anti-Trump research*, WASH. TIMES (May 8, 2019), at 2, https://www.washingtontimes.com/news/2019/may/8/fbi-refuses-reveal-if-daniel-jones-alfa-bank-serve/ (last visited June 11, 2020).) Jones reportedly told the FBI that the Penn Quarter Group was funded by seven to ten wealthy donors in New York and California and had retained

Steele and Fusion GPS to explore alleged Russian interference in the 2016 election. (*Id.*) Jones and the Penn Quarter Group planned to share any information that they obtained with policymakers on Capitol Hill, the mainstream media, and the FBI. (*Id.* at 3.) At the same time that he was assisting the FBI, Jones assembled a team of computer scientists to review the computer data compiled by Max's group, which an unnamed Democratic Senator disclosed to Jones and requested him to analyze. Jones assembled two teams of computer scientists, both of which consulted with Camp and Max. (Ex. 5, Oct. 8, 2018 *New Yorker* article at 7.) The findings of those teams were the backbone of the October 8, 2018 article in *The New Yorker* that concluded that the DNS data in fact was evidence of a covert communication channel between Alfa Bank and the Trump Organization.

VI. Exoneration of Alfa Bank

63. Law enforcement officials and cybersecurity experts who reviewed all available evidence of purported communications between Alfa Bank and the Trump Organization concluded that there were no such communications. These officials and experts determined that Alfa Bank did not communicate with the Trump Organization in 2016 and 2017 through their respective servers or otherwise.

64. In September 2016, Alfa Bank engaged Mandiant, a preeminent U.S. cybersecurity consulting firm, to investigate the allegations that recently had surfaced. Mandiant determined that there was no evidence of communications between Alfa Bank and the Trump Organization. (Ex. 3, Mandiant Report.)

65. In the wake of the 2017 cyberattacks, Alfa Bank retained a second elite cybersecurity expert group, Stroz Friedberg, to review evidence related to those attacks. Stroz Friedberg concluded that its investigation had "revealed no actual connections or communications between Alfa-Bank and President Trump or the Trump Organization." (Ex. 7, Stroz Friedberg Report at 3; *accord id.* at 2 ("find[ing] no evidence of any connections or communications between Alfa-Bank and the Trump Organization occurring in 2017").) Stroz Friedberg further determined that the server traffic from February and March 2017 was "consistent with the type of traffic often seen coming from . . . attackers checking or testing a company's security." (*Id.* ("[I]t is likely that the suspicious queries came from researchers and/or would-be attackers . . . .").)

66. Most recently, Alfa Bank retained a third cybersecurity consulting firm, Ankura, to review all of the evidence related to the purported communications between Alfa Bank and the Trump Organization. As described above, Ankura found no "support whatsoever for the allegation of a 'secret server' or covert 'cyber links' between Alfa Bank and the Trump Organization." (Ex. 2, Ankura Report at 3.) Instead, Ankura concluded that malicious actors likely manipulated DNS traffic to create the false illusion of communications between Alfa Bank and the Trump Organization. (*Id.*)

67. The Special Counsel's Office, whose mandate included investigating Russian efforts to interfere in the 2016 U.S. Presidential election, also reviewed allegations that Alfa Bank and the Trump Organization had orchestrated a secret communication channel through the use of their servers. Special Counsel Robert Mueller testified before Congress that his "belief at this point" was that the server allegations were "not true." (Ex. 25, *Former Special Counsel Robert S. Mueller III on the Investigation into Russian Interference in the 2016 Presidential Election,* U.S. H.R., Permanent Select Comm. on Intelligence, 116 Cong. (July 24, 2019) at 64.)

68. In December 2019, the Office of the Inspector General of the DOJ released its review into the FBI's investigation into Russian efforts to interfere in the 2016 election. The final report noted that "[t]he FBI investigated whether there were cyber links between the Trump

Organization and Alfa Bank, but had concluded by early February 2017 that there were no such links." (Ex. 17, OIG Report at 119 n.259.)

CAUSES OF ACTION

I. Count One: Federal Racketeer Influenced and Corrupt Organizations Act (Primary Violation) (18 U.S.C. § 1961 *et al.*)

69. All preceding paragraphs are repeated, re-alleged, and incorporated as if fully set forth herein.

70. RICO provides that "[i]t shall be unlawful for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity or collection of unlawful debt." 18 U.S.C. § 1962(c). The statute further provides a private right of action to "[a]ny person injured in his business or property by reason of a violation of section 1962." *Id.* § 1964(c).

71. Defendants are employed by or associated with the Disinformation Enterprise. 18 U.S.C. § 1962(c). The Disinformation Enterprise is a partnership, corporation, association, or other legal entity, or a union or group of individuals associated in fact although not a legal entity. *Id.* § 1961(4). Upon information and belief, Defendants are members of the Disinformation Enterprise, an ongoing organization whose various associates function as a continuing unit. Upon information and belief, Defendants have associated together and with others to form a group with the common purpose of orchestrating and executing disinformation campaigns to disrupt the activities of governments, corporations, and individuals. Upon information and belief, the Disinformation Enterprise preexisted the perpetration of cyberattacks against Alfa Bank in 2016 and 2017 and continues to exist. Upon information and belief, the Disinformation Enterprise engages in interstate or foreign commerce, or the activities of the Disinformation Enterprise affect interstate or foreign commerce, because the Disinformation Enterprise used and uses the internet, including networks and servers in multiple states in the United States and in Russia.

72. Defendants conducted or participated, directly or indirectly, in the conduct of the Disinformation Enterprise's affairs. 18 U.S.C. § 1962(c). Defendants, separately and collectively, participated in the operation or management of the Disinformation Enterprise itself. Specifically, Defendants developed and executed, in whole or in part, the 2016 and 2017 cyberattacks directed at Alfa Bank.

73. Defendants conducted or participated, directly or indirectly, in the conduct of the Disinformation Enterprise's affairs through "racketeering activity." 18 U.S.C. § 1962(c). From at least May 2016 through March 2017, Defendants committed acts indictable under 18 U.S.C. § 1343 (relating to wire fraud). *Id.* § 1961(1)(B). Defendants, as outlined above, devised a scheme or artifice to defraud, or to obtain money or property by means of false or fraudulent pretenses, representations, or promises, and transmitted or caused to be transmitted by means of wire, radio, or television communications in interstate or foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice. *Id.* § 1343. Defendants, acting knowingly and with fraudulent intent, devised and executed a deliberate plan of action or course of conduct by which they intended to deceive or cheat Alfa Bank or by which they intended to deprive Alfa Bank of something of value. Defendants used the internet for the purpose of executing the scheme to defraud.

74. Defendants conducted or participated, directly or indirectly, in the conduct of the Disinformation Enterprise's affairs through a "pattern" of racketeering activity, as defined in the preceding paragraphs. 18 U.S.C. § 1962(c). Defendants' cyberattacks against Alfa Bank in 2016

and 2017 qualify as at least two acts of racketeering activity that are related and amount to or pose a threat of continued criminal activity. *Id.* § 1961(5).

75. As the direct and proximate result of Defendants' unlawful acts, Alfa Bank was injured in its business or property in an amount to be proven at trial.

II. Count Two: Federal Racketeer Influenced and Corrupt Organizations Act (Conspiracy) (18 U.S.C. § 1961 *et al.*)

76. Paragraphs 1–68 are repeated, re-alleged, and incorporated as if fully set forth herein.

77. RICO provides that "[i]t shall be unlawful for any person to conspire to violate any of the provisions of subsection (a), (b), or (c)" of Section 1962. 18 U.S.C. § 1962(d). The statute further provides a private right of action to "[a]ny person injured in his business or property by reason of a violation of section 1962." *Id.* § 1964(c).

78. Defendants are employed by or associated with the Disinformation Enterprise. 18 U.S.C. § 1962(c). The Disinformation Enterprise is a partnership, corporation, association, or other legal entity, or a union or group of individuals associated in fact although not a legal entity. *Id.* § 1961(4). Upon information and belief, Defendants are members of the Disinformation Enterprise, an ongoing organization whose various associates function as a continuing unit. Upon information and belief, Defendants have associated together and with others to form a group with the common purpose of orchestrating and executing disinformation campaigns to disrupt the activities of governments, corporations, and individuals. Upon information and belief, the Disinformation Enterprise preexisted the perpetration of cyberattacks against Alfa Bank in 2016 and 2017 and continues to exist. Upon information and belief, the Disinformation Enterprise engages in interstate or foreign commerce, or the activities of the Disinformation Enterprise affect interstate or foreign commerce, because the Disinformation Enterprise used and uses the [illegible] including networks and servers in multiple states in the United States and in Russia.

79. Defendants conspired to conduct or participate, directly or indirectly, in the conduct of the Disinformation Enterprise's affairs. 18 U.S.C. § 1962(c). Defendants, separately and collectively, conspired to participate in the operation or management of the Disinformation Enterprise itself. Specifically, Defendants conspired to develop and execute, in whole or in part, the 2016 and 2017 cyberattacks directed at Alfa Bank. Defendants knew of the overall objectives of the Disinformation Enterprise and agreed to further its purpose or, alternatively, committed at least two predicate acts of criminal activity themselves.

80. Defendants conspired to conduct or participate, directly or indirectly, in the conduct of the Disinformation Enterprise's affairs through "racketeering activity." 18 U.S.C. § 1962(c). From at least May 2016 through March 2017, Defendants conspired to commit acts indictable under 18 U.S.C. § 1343 (relating to wire fraud). *Id.* § 1961(1)(B). Defendants, as outlined above, conspired to devise a scheme or artifice to defraud, or to obtain money or property by means of false or fraudulent pretenses, representations, or promises, and conspired to transmit or cause to be transmitted by means of wire, radio, or television communications in interstate or foreign commerce, writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice. *Id.* § 1343. Defendants, acting knowingly and with fraudulent intent, conspired to devise and execute a deliberate plan of action or course of conduct by which they intended to deceive or cheat Alfa Bank or by which they intended to deprive Alfa Bank of something of value. Defendants conspired to use the internet for the purpose of executing the scheme to defraud.

81. Defendants conspired to conduct or participate, directly or indirectly, in the conduct of the Disinformation Enterprise's affairs through a "pattern" of racketeering activity, as defined in the preceding paragraphs. 18 U.S.C. § 1962(c). Defendants' conspiracies to commit the cyberattacks against Alfa Bank in 2016 and 2017 qualify as at least two acts of racketeering activity that are related and amount to or pose a threat of continued criminal activity. *Id.* § 1961(5).

82. As the direct and proximate result of Defendants' unlawful acts, Alfa Bank was injured in its business or property in an amount to be proven at trial.

RELIEF REQUESTED

WHEREFORE, Alfa Bank respectfully prays that this Court enter judgment against Defendants for the following:

1. Treble monetary damages in excess of the amount requiring compulsory arbitration to be proven at trial;

2. Costs and attorneys' fees incurred in this action;

3. Pre- and post-judgment interest to the extent permitted by law; and

4. Such other relief as the Court may deem just and proper.

Dated: June 11, 2020

Respectfully submitted,

/s/ Jeffrey B. Rettig
Jeffrey B. Rettig
JOHNSON, DUFFIE, STEWART & WEIDNER
301 Market Street
P.O. Box 109
Lemoyne, PA 17043
(717) 761-4540
JRettig@JohnsonDuffie.com

Margaret E. Krawiec
Michael A. McIntosh
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
1440 New York Ave. NW
Washington, DC 20005
(202) 371-7000
margaret.krawiec@skadden.com
michael.mcintosh@skadden.com

VERIFICATION

I, Yakovlev Aleksandr Vladimirovich, depose and state that I am Head of Network Infrastructure Department for Plaintiff AO Alfa-Bank. I have reviewed the Complaint for Damages and verify that the statements made in the aforementioned document are true and correct to the best of my knowledge, information, and belief. This statement and verification are made subject to the penalties of 18 Pa. C.S. § 4904 relating to unsworn falsification to authorities, which provides that if I make knowingly false averments, I may be subject to criminal penalties.

Dated: June 11, 2020

/s/ Yakovlev Aleksandr Vladimirovich
Yakovlev Aleksandr Vladimirovich
Head of Network Infrastructure Department, AO Alfa-Bank