IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. ARTEM MIKHAYLOVICH LIFSHITS, Defendant.	Case No. 1:20-mj-256

AFFIDAVIT IN SUPPORT OF
A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Heather Turner, being duly sworn under oath, do hereby depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since July 2015. I have a number of different duties, including being responsible for investigating violations of the federal code, including wire fraud and aggravated identity theft. As a Special Agent, I have received specialized training and instruction in the field of financial crimes and fraud investigations.

2. This affidavit is submitted in support of a criminal complaint and arrest warrant charging the defendant, ARTEM MIKHAYLOVICH LIFSHITS (Лифшиц Артём Михайлович) ("LIFSHITS"), with conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349.

3. The facts and information contained in this Affidavit are based on my training and experience, on information provided to me by other members of USSS and other law enforcement officers, court records and documents, business records, interviews, publicly available information, and my review of physical and documentary evidence. I have personally

participated in the investigation of the offense set forth below and, because of my participation and review of evidence gathered in the case, I am familiar with the facts and circumstances of this investigation. Because this Affidavit is limited in purpose, I am not including all facts known to law enforcement concerning this investigation.

4. Below, I will explain the relevant statutes and the technical aspects of the investigation. I will then briefly describe Project Lakhta's past and continuing efforts to influence the United States political system. I will summarize an indictment obtained in the District of Columbia and a criminal complaint obtained in the Eastern District of Virginia, which charged several Project Lakhta members for their role in conspiring to defraud the United States and in using the means of identification of United States persons to open bank accounts, PayPal accounts, and cryptocurrency accounts.

5. I will also explain the USSS's more recent investigation into Project Lakhta members' use of the means of identification of United States persons to open cryptocurrency accounts. The remainder of the Affidavit will focus on LIFSHITS, who has been a manager in Project Lakhta's Translator Department since at least January 2017. The evidence below establishes that LIFSHITS was a manager in a unit responsible for much of Project Lakhta's influence operations and that these operations are ongoing. The evidence also establishes that LIFSHITS operated cryptocurrency accounts opened in the name of United States identity theft victims for personal gain.

RELEVANT STATUTES AND BACKGROUND

6. *Wire Fraud and Conspiracy to Commit Wire Fraud.* Title 18, United States Code, Section 1343 provides, in relevant part, that whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or

fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be guilty of a federal offense. Title 18, United States Code, Section 1349 provides, in relevant part, that whoever attempts or conspires to commit wire fraud shall be guilty of a federal offense.

7. *Aggravated Identity Theft*. Title 18, United States Code, Section 1028A provides, in relevant part, that whomever, knowingly and unlawfully transferred, possessed, or used a means of identification of another person during and in relation to an enumerated felony in Sections 1028A(c) or 2332b(g)(5)(B), shall be guilty of a federal felony. Wire fraud and conspiracy to commit wire fraud, are both enumerated felonies in Section 1028A(c).

TECHNICAL BACKGROUND

8. *Bitcoin*. Bitcoin is a cryptocurrency, which is a specific type of decentralized digital currency for which transactions are effected via cryptography. Bitcoin is often used in e-commerce or in the purchase of goods or services from online merchants. Each Bitcoin address is controlled through the use of a unique, corresponding private key — that is, a cryptographic password needed to access the address. Only the holder of the private key (or keys) for an address can authorize any transfers of Bitcoin from that address to other Bitcoin addresses. Bitcoin addresses are often stored alongside their corresponding private keys in digital "wallets." No identifying information about the payor or payee is transmitted in a Bitcoin transaction, as generally only the Bitcoin addresses of the parties are needed for the transaction. However, all Bitcoin transactions are recorded on a digital blockchain, which is a publicly available ledger that, among other things, records the source wallet address, the receiving wallet address, and the amount transacted for every Bitcoin transaction. Accordingly, as a general

matter, the Bitcoin blockchain contains a certain and verifiable public record of every single Bitcoin transaction ever made.[1] Moreover, because the blockchain is distributed among thousands of computers, it is effectively impossible to edit or delete the blockchain's record of completed transactions.

9. *Bitcoin exchanges*. A user typically acquires Bitcoin from a Bitcoin exchange. Bitcoin exchanges generally accept payments of conventional currency, and, for a fee, transfer a corresponding number of Bitcoin to the customer or convert Bitcoin back into fiat currency. Bitcoin exchanges can also provide Bitcoin wallet services, although an individual can obtain a wallet from a number of sources, such as downloading software from the internet. United States law requires Bitcoin exchanges operating within the United States to register with the Financial Crimes Enforcement Network ("FinCEN"), an arm of the Department of the Treasury, and as such, are required to follow certain money transmitter regulations.[2]

10. *Regulation of Bitcoin exchanges*. Based on my research and experience, the types of Bitcoin exchanges can vary from large, established, and licensed businesses that operate under and follow strict know-your-customer ("KYC") and Anti-Money Laundering ("AML") policies to unlicensed individuals operating without regard to the United States federal regulations governing virtual currency exchanges. Individuals involved in criminal activity often prefer to use unregulated and unlicensed exchanges to purchase Bitcoin with unlawful proceeds or cash out Bitcoin acquired through illegal activity, precisely because these exchanges do not request and store the type of information required under KYC and AML guidelines. Though operating

[1] There are third-party services that can obfuscate the wallets involved in transactions; however, these methods are not relevant to this case because the transactions discussed in this Affidavit were identified on the public blockchain.

[2] *See* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering (accessed August 27, 2020).

independently of the larger, more established exchange companies, the independent exchanges will often have active accounts with these larger companies due to the convenience and amount of resources (i.e., Bitcoin and fiat currency) available to their customers.

11. *Blockchain analysis*. Though Bitcoin affords a significant degree of anonymity to its users, there are a number of investigative tools exists that law enforcement can use to track the flow and location of Bitcoin, including blockchain analysis (also referred to as "Bitcoin tracing"). Blockchain analysis or Bitcoin tracing is a process whereby those wishing to do so can use the blockchain to follow Bitcoin transactions from Bitcoin addresses to Bitcoin address. This enables the public to, among other things, identify a point of entry—that is, the Bitcoin address in which Bitcoin purchased from fiat currency is first stored—and the point of exit—that is, the Bitcoin address out of which Bitcoin is exchanged for cash.

PROBABLE CAUSE

A. Background on Project Lakhta and Efforts to Interfere with United States Political System

12. Since at least 2014, known and unknown individuals, operating as part of a broader Russian effort known as "Project Lakhta," have engaged in political and electoral interference operations targeting populations within the Russian Federation and in various other countries, including, but not limited to, the United States, members of the European Union, Ukraine, and Africa. Since at least May 2014, Project Lakhta's stated goal in the United States was to disrupt the democratic process and to spread distrust towards candidates for political office and the political system in general.

13. Beginning in or around mid-2014 and continuing to the present, Project Lakhta obscured its conduct by operating through a number of Russian entities, including, but not limited to, the Internet Research Agency LLC, Internet Research LLC, MediaSintez LLC,

GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC (a/k/a "NevNov"), Economy Today LLC, National News LLC, Federal News Agency LLC (a/k/a "FAN"), and International News Agency LLC (a/k/a "MAN"). These entities employed hundreds of individuals in support of Project Lakhta's operations with an annual global budget of millions of United States dollars.

14. In furtherance of its goals, Project Lakhta members traveled to the United States to collect intelligence; established United States computer infrastructure; and built the capacity to reach millions of United States citizens through social media accounts operated under fictitious personas, including through the use of political advertisements. Further, Project Lakhta members acquired fake identification documents (such as driver's licenses) to further their operations and used stolen United States identities to open accounts with banks and cryptocurrency exchanges.

B. Overview of the Wire Fraud Conspiracy and LIFSHITS' Role in the Conspiracy

15. During the course of the investigation into Russian interference in the United States political system, law enforcement obtained evidence establishing that Project Lakhta members purchased the means of identification of United States persons. Project Lakhta members then used these means of identification to open bank accounts, PayPal accounts, and cryptocurrency accounts. The United States persons did not provide permission for their means of identification to be sold or used for such purposes. Further, and as explained below, the fraudulently opened accounts deprived the banks, PayPal, and the cryptocurrency exchanges of the right to control their property and exposed the entities to potential economic losses.

16. LIFSHITS applied for a job with Project Lakhta in and around July 2015. By in and around January 2017, LIFSHITS served as the head of Project Lakhta's Translator Department.[3]

17. From in and around April 2014, Project Lakhta's Translator Department focused on influencing the United States population. The Translator Department conducted operations on social media platforms, such as YouTube, Facebook, Instagram, and Twitter. The Translator Department's primary goal was to sow discord in the United States political system, incite civil unrest, and polarize Americans by promoting socially divisive issues, with particular emphasis on racial divisions and inequality in the United States

18. The evidence outlined below establishes that LIFSHITS accessed a cryptocurrency account that was opened using the means of identification of a real United States person. This cryptocurrency account was setup with a United States-based cryptocurrency exchange ("Exchange 1"). This United States person did not provide LIFSHITS or any other person permission to use his means of identification for this purpose. Then, on at least one occasion, LIFSHITS sent a payment of Bitcoin from this account to his personal account with Exchange 3, which is another United States-based cryptocurrency exchange. In accessing and using the fraudulently opened cryptocurrency account, LIFSHITS and his co-conspirators deprived Exchange 1 of its right to control its property and exposed Exchange 1 to potential economic losses.

[3] This is a translation from Russian, and it could be referred to as a Department, Unit, or Project. The USAO-DC Indictment, which is discussed in Section C, refers to it as the Translator Project.

C. The District of Columbia Indictment and Elena Khusyaynova Criminal Complaint in the Eastern District of Virginia

19. On February 16, 2018, a grand jury in the District of Columbia returned an Indictment charging thirteen Russian nationals and three Russian companies, including the Internet Research Agency, with committing federal crimes, while seeking to interfere with United States elections and political processes, including the 2016 presidential election. Indictment, *United States v. Internet Research Agency, et al.*, 1:18-CR-32 (DLF) (D.D.C. Feb. 16, 2018) (hereinafter the "USAO-DC Indictment"). *See* Attachment A. As of the filing of this Complaint, only Concord Management and Consulting LLC, which was one of three Russian companies indicted, had appeared in United States courts to defend itself.[4]

20. The USAO-DC Indictment charged certain of the Project Lakhta[5] defendants with committing aggravated identity theft and conspiring to commit wire fraud. The United States charged these co-conspirators, in part, because they used the stolen identities of real United States persons to open bank accounts, PayPal accounts, and cryptocurrency accounts. Co-conspirators used some of these accounts to further the conspiracy to interfere in the United States political system and other accounts for self-enrichment.

[4] On March 16, 2020, the United States dismissed Concord Management and Consulting LLC from the Indictment. Concord "availed itself of the Court's jurisdiction to obtain discovery from the United States . . . while positioning itself to evade any real obligations or responsibility," even refusing to produce a corporate representative despite "appearing" through counsel. Mot. to Dismiss Concord Defs., 2, 6, *United States v. Internet Research Agency, et. al*, 1:18-cr-32 (DLF) (D.D.C. Mar. 16, 2020). In light of the defendant's conduct, the United States dismissed these parties from the Indictment, stating substantial federal interests were no longer served by continuing the proceedings against them. *See id.* at 9. The Indictment remains pending and active as to thirteen named individual defendants and the IRA. *Id.*

[5] While the co-conspirators worked for Project Lakhta and were thus its employees, it is also true that some, if not all, employees were paid through other business entities.

21. On September 28, 2018, Elena Alekseyevna Khusyaynova ("Khusyaynova") was charged by criminal complaint in the Eastern District of Virginia (the "Khusyaynova Complaint") for participating in a conspiracy to defraud the United States, in violation of Title 18, United States Code, Section 371. *See* Attachment B. Between April 2014 and at least September 2018, Khusyaynova, as the Chief Accountant in Project Lakhta's finance department, managed the financing of substantially all aspects of Project Lakhta's operations, which included media and influence activities directed at the United States, the European Union, and Ukraine, as well as the Russian Federation. In that role, she oversaw the budgets of various Project Lakhta entities. The affidavit in support of the Khusyaynova Complaint documents her overt acts in furtherance of Project Lakhta's goals of interfering in the United States political system, including, but not limited to, her completion and submission of detailed budgets that included funding for political advertisements on Facebook, Instagram, and other social media outlets.

22. I submit that the factual allegations in the USAO-DC Indictment and the affidavit in support of the Khusyaynova Complaint provide further probable cause to believe that LIFSHITS has conspired to commit wire fraud and committed aggravated identity theft. Both the USAO-DC Indictment and affidavit in support of the Khusyaynova Complaint are attached hereto and incorporated by reference.

D. Project Lakhta's Political Interference Activities from late December 2016 to Present in the United States

23. Between in or around December 2016 and in or around May 2018, as part of the effort to sow discord in the United States political system, Project Lakhta members used social media and other internet platforms to inflame passions on a wide variety of topics, including immigration, gun control and the Second Amendment; the Confederate flag; race relations; Lesbian, Gay, Bisexual, and Transgender ("LGBT") issues; the Women's March; and the

National Football League national anthem debate. Project Lakhta members took advantage of specific events in the United States to anchor their themes, including the shootings of church employees in Charleston, South Carolina, and concert attendees in Las Vegas, Nevada; the Charlottesville "Unite the Right" rally and associated violence; police shootings of African-American men; and the current United States administration's personnel and policy decisions.

24. Below I detail only a small portion of the overt acts committed in furtherance of the conspiracy to defraud the United States. More overt acts are thoroughly discussed in the Khusyaynova Complaint, which is incorporated by reference and is attached to this Affidavit.

25. According to evidence gathered by law enforcement, Project Lakhta leadership directed its members to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements." Project Lakhta members also sought, in the words of one employee, to "effectively aggravate the conflict between minorities and the rest of the population."

26. Project Lakhta members did not exclusively adopt one ideological viewpoint; rather, they wrote on topics from varied and sometimes opposing perspectives. Project Lakhta members also developed strategies and guidance to target audiences with conservative and liberal viewpoints, as well as particular social groups. For example, one Project Lakhta member directed his fellow co-conspirator in or around October 2017 that "if you write posts in a liberal group, . . . you must not use Breitbart titles. On the contrary, if you write posts in a conservative group, do not use Washington Post or BuzzFeed's titles." Using the example of individuals of color who are also employees of the LGBT community, one Project Lakhta member offered the following guidance on how to target the group:

> Colored LGBT are less sophisticated than white; therefore, complicated phrases and messages do not work. Be careful dealing with racial content. Just like ordinary Blacks,

> Latinos, and Native Americans, colored LGBT people are very sensitive towards #whiteprivilege and they react to posts and pictures that favor white people. . . . Unlike with conservatives, infographics works well among LGBT and their liberal allies, and it does work very well. However, the content must be simple to understand consisting of short text in large font and a colorful picture.

(Preliminary translation of Russian text)

27. Project Lakhta members also developed detailed analysis of timely news articles and guidance for how to describe the articles in social media posts in order to interfere with the United States political process. For example, in or around early August 2017, one co-conspirator, working under the guise of the Facebook group "Secured Borders," analyzed a large quantity of United States news articles, summarized the substance of the articles, and outlined ways for the conspiracy to promote them. Specifically, one or more co-conspirators described each article and categorized its theme, provided a strategic response with a particular focus on how to target United States audiences, and then noted approval to use the strategic response. The strategic response was referred to as "Tasking Specifics," which appeared to include an assignment to certain Project Lakhta members to disseminate the message on social media platforms.

28. For instance, citing an online news article titled "Paul Ryan Opposes Trump's Immigration Cuts, Wants Struggling American Workers to Stay Poor," from on or about August 5, 2017, a Project Lakhta member directed his fellow co-conspirator to message the article in the following way:

> Brand Paul Ryan a complete and absolute nobody incapable of any decisiveness. Emphasize that while serving as Speaker, this two-faced loudmouth has not accomplished anything good for America or for American citizens. State that the only way to get rid of Ryan from Congress, provided he wins in the 2018 primaries, is to vote in favor of Randy Brice, an American veteran and an iron worker and a Democrat.

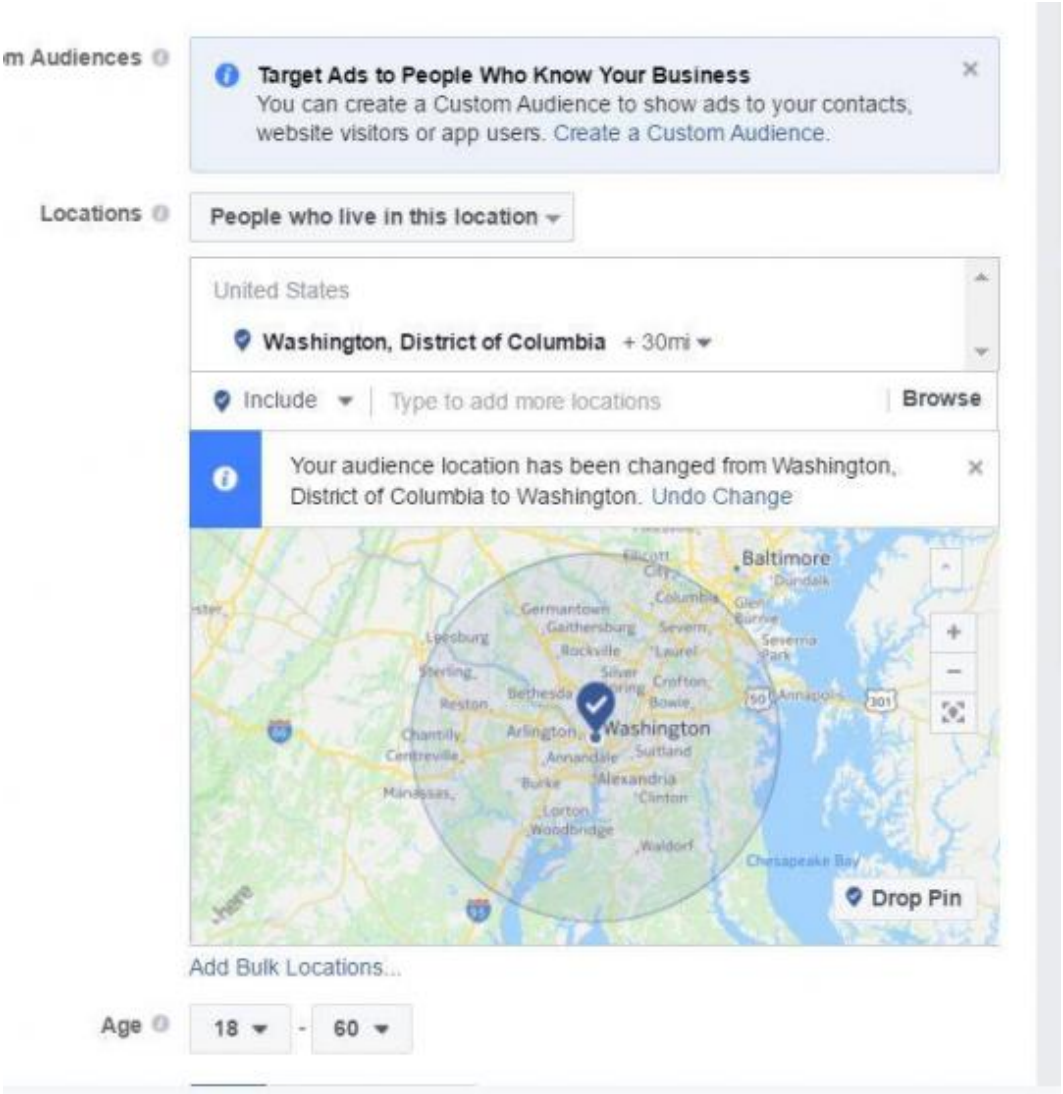
(Preliminary translation of Russian text)

29. In another example, citing an online news article titled "CNN's Pro-Jeb! Republican: Trump White House Like a 'Brothel,'" from on or about August 7, 2017, a Project Lakhta member directed his fellow co-conspirator to message the article in the following way:

> CNN commentator "RINO" likened the Trump administration to a "brothel." Mass News Media Criticism! Accuse CNN of yet another lie. State that during past elections, namely, this mainstream media, which supported Hillary Clinton's candidacy for United States President almost 100%, disseminated fake news, insulting statements, and lies about Donald Trump and his supporters. This continues now. This is precisely why such news sources as the New York Times, Washington Post, CNN, CBS, Time, and Huffington Post must not be taken seriously, for they are the main propaganda channels that are screwing with the heads of American citizens. Remind readers that each of the above-mentioned media resources supported Hillary Clinton and received funds from her election fund. They produced fake social study research results at polls predicting a Clinton win with a 10-15% lead over Trump and tried hard to insult and discredit Trump. Summarize with a statement that CNN long ago lost its reputation as a trusted source and that its reputation is still declining.

(Preliminary translation of Russian text)

30. Further, on or about July 2, 2017, a Project Lakhta member used the "Helen Christopherson" Facebook account, which is a fake United States persona, to send a United States organization a proposal to purchase advertising targeted at individuals within 30 miles of Washington, DC, including significant portions of the Eastern District of Virginia, as depicted below:



The proposed advertisements had an estimated reach of 29,000 to 58,000 individuals.

Subsequently, the United States organization agreed to make the "Helen Christopherson" Facebook account a co-organizer of the event on Facebook.

31. On or about March 22, 2018, a Project Lakhta member used the Twitter account "@johncopper16" to post the following tweet about the 2018 midterm election:

> Just a friendly reminder to get involved in the 2018 Midterms. They are motivated They hate you They hate your morals They hate your 1A and 2A rights They hate the Police They hate the Military They hate YOUR President

32. In or around July 2019, a Project Lakhta member founded Eliminating Barriers for the Liberation of Africa ("EBLA") in Accra, Ghana. EBLA employed approximately sixteen Ghanians and received direction from the Project Lakhta member. EBLA members established social media accounts on Facebook and Twitter. The EBLA members designed the accounts to look like the users were located in the United States. EBLA members used these accounts to post about racial issues in the United States. For example, one Twitter account, @africamustwake posted the following message:

> YOU POLICE BEEN KILLING BLACKS SINCE YA RAGGEDY MOMMAS GAVE BIRTH TO U. HAPPY MLK DAY TO U HYPOCRITES.

33. On or about January 25, 2020, an EBLA employee created an EBLA company page on LinkedIn and subsequently advertised a job posting seeking a chapter coordinator in Charleston, South Carolina. The advertisement described EBLA as "a network of strong advocates of human rights…we as young activists and human rights advocates envisage a better world were POC live freely, thus our call to join hands with our brothers and sisters world-wide, especially in the United States where POC are mostly subjected to all forms of Brutality." This advertisement was also posted to at least six other internet websites in late January and early February 2020. Law enforcement have identified approximately 90 social media accounts with known or suspected links to EBLA.

34. According to a CNN interview with a former EBLA employee, employees were given United States news articles to read and topics to post. The EBLA employee stated: "So you get stories about LGBT, you get stories about police brutality, depends on what you are working." The employee said that she and other employees were told that the best time to tweet and post was late afternoon and at night in Ghana, which are times when a United States audience would have been active.

35. Project Lakhta members continue to use social media platforms in furtherance of its efforts to sow discord in the United States. Further, members are using sophisticated methods to obfuscate the origins of their social media activity, including the use of virtual private servers, software enabling anonymous communications, and single use or "burner" email accounts linked to social media accounts. Law enforcement have identified social media accounts used by Project Lakhta members since August 2019 up until the present to post about a wide range of topics, including, but not limited to, the Second Amendment, Black Lives Matters, and LGBTQ issues. As previously stated, Project Lakhta members have posted about these issues for several years. The accounts associated with these posts used virtual servers located in Ghana, Cameroon, Central African Republic, Germany, Ukraine, Estonia, United States, and elsewhere.

E. Background on USSS Investigation into Project Lakhta's Use of Cryptocurrency Accounts

36. In and around October 2018, USSS began investigating Russian efforts to interfere in United States elections and democratic processes. Specifically, USSS examined how Project Lakhta members used and continue to use cryptocurrency accounts to further the objects of the conspiracy to interfere with the United States political system; and how Project Lakhta members used and continue to use accounts created using the stolen identities of real United States persons for personal enrichment.

37. In an effort to uncover the identities and activities of Project Lakhta members, USSS identified multiple cryptocurrency accounts registered to email accounts known to be used by co-conspirators. The USAO-DC Indictment identified many of these email accounts. *See* Attachment A. As set forth in the USAO-DC Indictment, Project Lakhta members used these email accounts to open fraudulent accounts with banks, cryptocurrency exchanges, and PayPal. Based on a review of the information provided in response to subpoena requests, USSS

identified several cryptocurrency accounts to be of "high interest" due to registered identifiers, transactional activity, and/or Internet Protocol ("IP") address logs on file.

38. One of the initial accounts that USSS identified was hosted at Exchange 1. The Exchange 1 account was registered to a known Project Lakhta email account, x[T.W.]x@gmail.com[6] (hereinafter the "T.W. Exchange 1 Account"). The T.W. Exchange 1 Account reflected debits to several beneficiaries, including accounts registered to LIFSHITS and another known Project Lakhta member ("Co-Conspirator 1"). The IP activity associated with the T.W. Exchange 1 Account also matched the IP address activity of cryptocurrency accounts registered to LIFSHITS and Vladimir Venkov, who is charged in the USAO-DC Indictment.

39. Law enforcement conducted a voluntary interview of T.W. T.W. confirmed that he had never purchased, owned, or possessed any cryptocurrency or virtual currency, such as those outlined in this Complaint. T.W. stated that he never authorized another person to use or sell his personally identifiable information to any other individual or organization. T.W. stated that he did not establish or use the email x[T.W.]x@gmail.com or email handle "x[T.W.]x." Thus, LIFSHITS and his co-conspirators did not have lawful authority to use T.W.'s means of identification.

40. USSS identified a second account, which was hosted at another United States cryptocurrency exchange ("Exchange 2"). The Exchange 2 account was registered to a known Project Lakhta email account, allforusa@yahoo.com (hereinafter the "AllforUSA Exchange 2 Account").[7] Project Lakhta members opened the AllforUSA Exchange 2 Account using the

[6] Here, I use T.W. instead of the actual email account in order to protect the identity of the victim. T.W. is one of the identity theft victims listed in Count 2 of the USAO-DC indictment.

[7] The USAO-DC Indictment alleges that the allforusa@yahoo.com email account was used by co-conspirators to, among other things, open fraudulent bank accounts as part of the underlying conspiracy to interfere with U.S. elections.

identifiers of T.B. According to Exchange 2's records, Project Lakhta members solely funded the AllforUSA Exchange 2 Account with an incoming credit from an account also in the name of T.B. at a United States-based financial institution. This credit was used exclusively to fund outgoing payments to a Blockchain wallet[8] that USSS investigators determined was controlled by Co-Conspirator 1. Additionally, the IP activity of the AllforUSA Exchange 2 Account again matched the IP activity of accounts registered to LIFSHITS and Venkov.

41. Law enforcement conducted a voluntary interview of T.B. T.B. confirmed that he had never purchased, owned, or possessed any cryptocurrency or virtual currency, such as those outlined in this Complaint. T.B. stated that he never authorized another person to use or sell his personally identifiable information to any other individual or organization. T.B. confirmed that he did not provide another person permission to open the accounts at issue in this Complaint. Thus, LIFSHITS and his co-conspirators did not have lawful authority to use T.B.'s means of identification.[9]

F. Identification of Accounts Used to Purchase United States Persons' Personally Identifying Information

42. Law enforcement obtained a search warrant for the contents of the email account allforusa@yahoo.com, which as stated above is associated with a cryptocurrency account linked to both LIFSHITS and Co-Conspirator 1. During a review of the emails, law enforcement located "Order Confirmation" emails received from an online criminal marketplace that sells fraudulent passports and similar identification documents (the "Criminal Marketplace"). These

[8] Blockchain is a wallet service provider ostensibly based in Luxembourg. Blockchain provides encrypted non-custodial wallet services and claims that legal process served upon Blockchain will not yield any relevant information regarding the specific user or associated transaction activity of a given wallet.

[9] T.B. is another of the identity theft victims listed in Count 2 of the USAO-DC indictment.

emails corresponded to purchases of United States driver licenses that reflected the real names, addresses, and dates of birth of United States identity theft victims. This type of personally identifiable information is a "means of identification" as defined in Title 18, United States Code, Section 1028(d)(7).

43. Project Lakhta members thus used the allforusa@yahoo.com account to, among other things, create an account with the Criminal Marketplace. Project Lakhta members then used this account to purchase fraudulent documents reflecting the identifiers of real United States persons, including T.B. The relevant order confirmations related to United States identity theft victims noted in this Complaint are listed below. I have redacted the real identifiers and the personally identifiable information of the United States persons.

Order Date	**May 4, 2017**
Order Number	12261
Total Price	$45
Payment Method	Bitcoin
Billing Address	"T.B."
Customer Details	allforusa@yahoo.com
Product	Driver's License
Identifiers	"T.B."[Real Address Redacted] [Real Date of Birth Redacted]

Order Date	**May 11, 2017**
Order Number	12373
Total Price	$30
Payment Method	Bitcoin
Billing Address	"T.B."
Customer Details	allforusa@yahoo.com
Product	Driver's License
Identifiers	"J.W." [Real Address Redacted] [Real Date of Birth Redacted]

Order Date	**July 4, 2017**
Order Number	13228
Total Price	$210
Payment Method	Bitcoin
Billing Address	"T.B."
Customer Details	allforusa@yahoo.com
Product	Driver's License

Identifiers	"T.C." [Real Address Redacted] [Real Date of Birth Redacted]

G. LIFSHITS' Connections to and Role in Project Lakhta

44. During the course of this investigation, law enforcement obtained a search warrant for an email account belonging to a known Project Lakhta member. During a review of the contents of this email account, law enforcement identified Project Lakhta rosters from January and September 2017, which identify members by department and position. The rosters also reflect the fact that Project Lakhta hid its activities by paying its members through different companies including, but not limited to, Azimut LLC. As detailed in the USAO-DC Indictment, Azimut LLC is one of several entities that Project Lakhta used to obscure its conduct.

45. LIFSHITS is listed in the Project Lakhta rosters. One spreadsheet titled "Roster of employees of Project Lakhta as of January 18, 2017," listed an "Artem Mikhaylovich Lifshits" as a "Task Manager" in "Translator Department No. 2" with a monthly salary of 70,000 rubles. A second spreadsheet titled "Roster of employees of Project Lakhta as of October 26, 2017," listed "Artem Mikhaylovich Lifshits" as a "Task Manager" in "Translator Department No. 1" with a monthly salary of 80,000 rubles. In addition, another roster dated September 2017, listed "Artem Mikhaylovich Lifshits" as "Task Manager No. 2."

46. As described more fully above, LIFSHITS, as a manager in the Project Lakhta's Translator Department, would have been directly involved in social media messages and other messages directed at and intended to influence the United States population.

47. During the course of the investigation into Project Lakhta, law enforcement obtained information indicating that LIFSHITS applied to Project Lakhta in and around July 2015. More specifically, law enforcement obtained a search warrant for an email account belonging to another known Project Lakhta member. Based on the review of emails obtained

pursuant to the search warrant, law enforcement located an email from July 2015 from LIFSHITS' known email account with a resume attached. The resume belonged to "Artem Mikhaylovich Lifshits," born December [redacted], 1992, and reported a phone number ending in 4982. These identifiers for LIFSHITS all match the information on file with Exchange 3.

H. LIFSHITS Use of Cryptocurrency Accounts and IP Addresses Known To Be Used by Project Lakhta Members

1. USSS Identification of LIFSHITS

48. While conducting a forensic transactional analysis on the T.W. Exchange 1 Account as discussed above, USSS identified LIFSHITS as a transactional counterparty. Specifically, the transactional activity of the T.W. Exchange 1 Account reflected an outgoing payment to a Bitcoin address [redacted]. Valid legal process confirmed this as an address hosted at an exchange operating in the United States ("Exchange 3") and assigned to LIFSHITS, whose full identifiers were on file with Exchange 3. These identifiers included LIFSHITS' Russian passport, email account, and telephone number.

49. During the course of this investigation, law enforcement obtained other information to corroborate that the information used to establish LIFSHITS' account with Exchange 3 is actually associated with LIFSHITS.

50. For instance, a September 2012 publication of Monok'e, which is a student magazine associated with the Faculty of Economics at Saint Petersburg State University, included a photograph of LIFSHITS and noted him to be "head" of the publication's "information committee." LIFSHITS' contact information included the phone number ending in 4982, which he used to setup his Exchange 3 account. In addition, I note that LIFSHITS' resume, which he sent to the known Project Lakhta member in 2015, listed Saint Petersburg State University in the education section.

51. In a post on Russian social networking platform VK from March 2010, user "artemous" listed a photograph, date of birth, and Russia as his country. The date of birth supplied by "artemous" matches LIFSHITS' date of birth supplied to Exchange 3. Further, LIFSHITS' passport photo supplied to Exchange 3 and the photograph of "artemous" appear to be the same person.

52. Finally, during the course of this investigation, law enforcement obtained search warrants for email accounts belonging to two known Project Lakhta members. The address books of both of these individuals included LIFSHITS' phone number ending in 4982, and referenced it as associated with "Artemka Boss" and "Troll Face."

53. Based on the above, I submit that there is at least probable cause to believe that LIFSHITS established and uses the Exchange 3 account that is registered in his name.

54. A forensic transactional review of LIFSHITS' Exchange 3 account resulted in the identification of an account registered to LIFSHITS at another exchange operating in the United States ("Exchange 4"). The account was opened using the same email account that LIFSHITS used to open his Exchange 3 account. Exchange 4 had no additional identifiers for the account. However, this email account, as well as the IP address activity associated with the account, match the registered email account and IP address activity of LIFSHITS' Exchange 3 account. As a result, I submit that there is at least probable cause to support that LIFSHITS also operates the Exchange 4 account registered in his name.

2. LIFSHITS' Use of Project Lakhta-Controlled IP Addresses

55. During the course of the investigation into Project Lakhta, law enforcement determined Project Lakhta members used Russian IP address XX.XX.XXX.218 ("Russian IP Address 1") to access a significant number of social media accounts used to develop fictitious

personas and to engage with Americans on social and political issues. LIFSHITS' account at Exchange 3 reflected over 30 instances of activity from this IP address. Further, LIFSHITS' account at Exchange 4 reflects four instances of activity from this IP address.

56. In addition, Project Lakhta members used United States IP address XX.XXX.XXX.67 ("United States IP Address 1") to access cryptocurrency accounts setup in the name of United States identity theft victims, as well as an account Project Lakhta members used to procure United States victim identifiers from the Criminal Marketplace. LIFSHITS' account at Exchange 3 reflected six instances of activity from this IP address. LIFSHITS' account at Exchange 4 reflected four instances of activity from this IP.

57. Further, the T.W. Exchange 1 Account, which as discussed above is registered to a United States identity theft victim, reflected multiple instances of activity from United States IP address XXX.XXX.XXX.22 ("United States IP Address 2"). LIFSHITS' account at Exchange 3 reflected six instances of activity from this same IP address.

58. Below is a visual representation of this activity.

United States IP Address 1

ACCOUNT LOGINS LINKED BY IP ADDRESS				
Date Range	**IP Instances**	**Account**	**(Project Lakhta) Registration Email**	**US Person Identity**
6/28/2016	11	Exchange 2	allforusa@yahoo.com	T.B.
8/9/2016	10	Exchange 2	wemakeweather@gmail.com	T.B.
8/9/2016	13	Exchange 2	mightytyrone7@gmail.com	T.C.
8/9/2016 – 9/13/2016	6	[Foreign Exchange 2]	mightytyrone7@gmail.com	T.C.
6/7/2017 – 1/14/2018	23	Exchange 1	X[T.W.]x@gmail.com	T.W.
6/9/2017 – 10/1/2017	43	[Foreign Exchange 1]	ihatecrime1@gmail.com	J.W.
8/12/2016 – 9/16/2017	99	[Foreign Exchange 1]	wokeaztec@outlook.com	A.S.
3/20/2017 – 12/29/2017	6	Exchange 3	mycryptodeals@yandex.ru	N/A – LIFSHITS
1/11/2018	4	Exchange 4	mycryptodeals@yandex.ru	N/A – LIFSHITS

United States IP Address 2

ACCOUNT LOGINS LINKED BY IP ADDRESS				
Date Range	**IP Instances**	**Account**	**(Project Lakhta) Registration Email**	**US Person Identity**
12/26/2017-12/29/2017	4	Exchange 3	mycryptodeals@yandex.ru	N/A – LIFSHITS
01/29/2017	2	Exchange 1	X[T.W.]x@gmail.com	T.W.

Russian IP Address 1

ACCOUNT LOGINS LINKED BY IP ADDRESS				
Date Range	**IP Instances**	**Account**	**(Project Lakhta) Registration Email**	**US Person Identity**
12/21/2017 – 6/6/2018	33	Exchange 3	mycryptodeals@yandex.ru	N/A – LIFSHITS
1/12/2018	5	Exchange 2	X[T.W.]x@gmail.com	T.W.
2/9/2018 – 6/6/2018	3	Exchange 4	mycryptodeals@yandex.ru	N/A – LIFSHITS

59. I submit that LIFSHITS' appearance in the Project Lakhta employee rosters, the fact that he sent his resume to a known Project Lakhta member, and his use of Project Lakhta-controlled IP addresses to access his own accounts, establishes probable cause to believe that LIFSHITS works for Project Lakhta and uses Project Lakhta-controlled IP addresses to access his Exchange 3 account.

I. LIFSHITS' Use of the T.W. Exchange 1 Account for Personal Gain

60. On or about December 29, 2017, LIFSHITS accessed and used the T.W. Exchange 1 Account to conduct an electronic transfer of funds from the T.W. Exchange 1 Account to his personal Exchange 3 account. This transaction is publicly viewable on the Bitcoin blockchain and USSS confirmed its existence through other investigative means.

61. On or about December 29, 2017, LIFSHITS used United States IP Address 1 at 15:35 UTC to access his Exchange 3 account. Then, three minutes later, he used the same IP address to access the T.W. Exchange 1 Account. This is on the same day that the T.W. Exchange 1 Account sent an electronic funds transfer to LIFSHITS' Exchange 3 account.

62. With this transaction, LIFSHITS (1) intentionally and voluntarily devised or participated in a scheme to defraud — as evidenced by controlling and using a fraudulent

cryptocurrency account, and (2) used interstate wire communications to further the fraud — as evidenced by the online cryptocurrency transactions.

1. Noteworthy Overlaps in IP Activity between the LIFSHITS and T.W. Accounts

63. Between December 26, 2017 and January 12, 2018, LIFSHITS' personal accounts at Exchange 3 and Exchange 4 reflected activity from United States IP Addresses 1 and 2. During that same time, including on the same day and within several minutes of one another, the T.W. Exchange 1 Account reflected activity from the same IP addresses.

64. The below table summarizes the IP address activity for LIFSHITS' accounts and the T.W. Exchange 1 Account. For ease of reference, I have highlighted where the LIFSHITS' account and the T.W. Exchange 1 Account were accessed from the same IP address within a few minutes of each other.

UTC Timestamp	IP	IP Activity Type	Account
12/26/2017 11:37:12	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/27/2017 7:51:34	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/28/2017 8:01:51	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/29/2017 7:58:07	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/29/2017 14:43:33	United States IP Address 2	Unknown IP login BEFORE 2FA	T.W. – Exchange 1
12/29/2017 14:44:23	United States IP Address 2	Unknown IP login	T.W. – Exchange 1
12/29/2017 15:31:34	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
12/29/2017 15:31:54	United States IP Address 1	Login	T.W. – Exchange 1
12/29/2017 15:35:40	United States IP Address 1	Login	LIFSHITS – Exchange 3
12/29/2017 15:38:43	United States IP Address 1	Withdrawal 2FA Success[10]	T.W. – Exchange 1
12/29/2017 15:41:24	United States IP Address 1	Logoff	T.W. – Exchange 1
12/29/2017 20:56:07	United States IP Address 1	Login before 2FA	T.W. – Exchange 1

[10] "2FA Success" refers to 2 factor authentication.

UTC Timestamp	IP	IP Activity Type	Account
12/29/2017 20:56:24	United States IP Address 1	Login	T.W. – Exchange 1
12/29/2017 21:01:31	United States IP Address 1	Withdrawal 2FA Success	T.W. – Exchange 1
1/10/2018 16:28:17	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
1/10/2018 16:28:44	United States IP Address 1	Login	T.W. – Exchange 1
1/11/2018 12:23:52	United States IP Address 1	User registration	LIFSHITS – Exchange 4
1/11/2018 12:36:35	United States IP Address 1	Email verification	LIFSHITS – Exchange 4
1/11/2018 12:37:27	United States IP Address 1	User forgot password	LIFSHITS – Exchange 4
1/11/2018 13:49:57	United States IP Address 1	User forgot password	LIFSHITS – Exchange 4
1/12/2018 2:37:29	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
1/12/2018 2:37:43	United States IP Address 1	Login	T.W. – Exchange 1
1/12/2018 2:39:48	United States IP Address 1	Withdrawal 2FA Success	T.W. – Exchange 1

2. Focus on December 29, 2017 Transaction from the T.W. Exchange 1 Account to LIFSHITS' Exchange 3 Account

65. The IP logs of the T.W. Exchange 1 and LIFSHITS' Exchange 3 accounts reflect the following activity on December 29, 2017. This activity indicates that LIFSHITS logged in to his account at Exchange 3 at the same time and from the same IP address as the T.W. Exchange 1 Account, when the latter engaged in a login and subsequent withdrawal of funds:

UTC Timestamp	IP	IP Activity Type	Account
12/29/2017 7:58:07	United States IP Address 2	Login	LIFSHITS – Exchange 3
12/29/2017 14:43:33	United States IP Address 2	Unknown IP login before 2FA	T.W. – Exchange 1
12/29/2017 14:44:23	United States IP Address 2	Unknown IP login	T.W. – Exchange 1
12/29/2017 15:31:34	United States IP Address 1	Login before 2FA	T.W. – Exchange 1
12/29/2017 15:31:54	United States IP Address 1	Login	T.W. – Exchange 1
12/29/2017 15:35:40	United States IP Address 1	Login	LIFSHITS – Exchange 3
12/29/2017 15:38:43	United States IP Address 1	Withdrawal 2FA Success	T.W. – Exchange 1
12/29/2017 15:41:24	United States IP Address 1	Logoff	T.W. – Exchange 1

66. The "Withdrawal 2FA Success" field indicates that on December 29, 2017, at 15:38:43 UTC, the T.W. Exchange 1 Account successfully authorized a withdrawal of funds from the account. The transactional activity of the T.W. Exchange 1 Account confirmed that this withdrawal pertained to the following transaction:

> Withdrawal Amount: BTC 0.00938398
> Destination Address: [redacted]
> Transaction
> Hash: [redacted]
> Withdrawal Date: 12/29/2017
> Withdrawal Time: 15:38:43 (UTC)

67. As noted elsewhere in this Complaint, Exchange 3 records confirm that Destination Address [redacted] is hosted at Exchange 3 and is assigned to LIFSHITS. A review of the transactional activity within LIFSHITS' Exchange 3 account confirmed that the following transaction occurred:

> Deposit Amount: BTC 0.00938398
> Deposit Address: [redacted]
> Transaction
> Hash: [redacted]
> Deposit Date: 12/29/2017
> Deposit Time: 15:57:27 (UTC)

68. Thus, the particular deposit to LIFSHITS' personal Exchange 3 account originated from the T.W. Exchange 1 Account. As established above, Project Lakhta members created the T.W. Exchange 1 Account using a known Project Lakhta email account and the stolen identifiers of T.W., who is a real United States person. Further, in the minutes prior to the transaction, the T.W. Exchange 1 Account reflected an active login session from United States IP Address 1 at the same time that LIFSHITS logged into his personal Exchange 3 account from that same IP address. Several minutes later, the T.W. Exchange 1 Account, using United States IP Address 1, facilitated a transfer of Bitcoin to LIFSHITS' personal Exchange 3 account.

69. I therefore submit that this evidence alone establishes probable cause to believe that LIFSHITS had control of and accessed the T.W. Exchange 1 Account. It also establishes probable cause to believe that LIFSHITS caused the electronic transfer of funds from the T.W. Exchange 1 Account to his (LIFSHITS') own personal account at Exchange 3.

3. Noteworthy Overlaps in User Agent Strings between the LIFSHITS and T.W. Accounts

70. A web browser corresponding to a single user agent string generated the above IP activity at United States IP Addresses 1 and 2, associated with LIFSHITS' Exchange 3 and Exchange 4 accounts between December 26, 2017 and January 11, 2018. With the exception of activity on January 10, 2018, the IP activity associated with the T.W. Exchange 1 Account during that same period was also generated via a browser corresponding to the same user agent string. This means that the internet web browser and version used to access the T.W. Exchange 1 Account and LIFTSHITS' Exchange 3 and Exchange 4 accounts was the same. I submit that when coupled with the fact that the same IP address was used to access the T.W. Exchange 1 Account and LIFSHITS' Exchange 3 account within minutes of each other, the identical user agent strings are further evidence that LIFSHITS used the T.W. Exchange 1 Account to fund his Exchange 3 account.

71. The below table summarizes the IP activity and user agent strings for LIFSHITS' accounts and the T.W. Exchange 1 Account. For ease of reference, I have highlighted the transaction on December 29, 2017.

UTC Timestamp	IP	IP Activity – User Agent String	Account
12/26/2017 11:37:12	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/27/2017 7:51:34	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/28/2017 8:01:51	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/29/2017 7:58:07	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/29/2017 14:43:33	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 14:44:23	United States IP Address 2	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:31:34	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:31:54	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:35:40	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 3
12/29/2017 15:38:43	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 15:41:24	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 20:56:07	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 20:56:24	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
12/29/2017 21:01:31	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
1/10/2018 16:28:17	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/10/2018 16:28:44	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/11/2018 12:23:52	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/11/2018 12:36:35	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/11/2018 12:37:27	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/11/2018 13:49:57	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	LIFSHITS – Exchange 4
1/12/2018 2:37:29	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1
1/12/2018 2:37:43	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0	T.W. – Exchange 1

72. As previously stated, a different user agent string was generated on January 10, 2018, when accessing the T.W. Exchange 1 Account. Importantly, this same user agent string appears when LIFSHITS used a Russian IP address to access his Exchange 3 and Exchange 4

accounts during the same time period that the T.W. Exchange 1 Account reflected activity from this user agent string:

UTC Timestamp	IP	IP Activity – User Agent String	Account
1/9/2018 12:19:14	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/10/2018 16:28:17	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/10/2018 16:28:44	United States IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	T.W. – Exchange 1
1/19/2018 13:30:38	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/23/2018 14:44:23	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/26/2018 13:04:24	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
1/29/2018 13:59:34	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/6/2018 15:14:00	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/9/2018 18:20:11	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 4
2/15/2018 15:52:57	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/19/2018 14:56:38	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/21/2018 14:08:22	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3
2/22/2018 12:59:00	Russian IP Address 1	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36	LIFSHITS – Exchange 3

73. I submit the use of the same Mozilla user agent string to access both LIFSHITS' Exchange 3 account and the T.W. Exchange 1 Account, during the same time period, provides further supports that LIFSHITS controlled and accessed both accounts.

J. Use of IP Addresses Associated with Computers Located in the Eastern District of Virginia

74. Since 2015, Exchange 2 has used Amazon Web Services ("AWS") for its cloud computing and Application Programming Interface ("API") infrastructure. As part of the conspiracy to commit wire fraud, the conspirators opened three different accounts with Exchange 2 using the means of identification of United States persons, including T.W. The conspirators interacted with and relied upon Exchange 2's AWS infrastructure in order to create, access, and use the Exchange 2 accounts in question. For example, the conspirators used the stolen identifiers of T.W. to create an account with Exchange 2 on March 3, 2017. As part of the account creation process, Exchange 2 used an AWS-controlled IP address in order to deliver a confirmation email to the conspirators so that the latter could complete the account creation by clicking on the email in question. This IP address is associated with a computer located in and operated by AWS from a data center in the Eastern District of Virginia.

75. The conspirators caused Exchange 2 to use IP addresses associated with a computer located in and operated by AWS from its data center(s) in the Eastern District of Virginia on other occasions including, but not limited to, the following:

a. On or about June 28, 2016, Exchange 2 used an AWS-controlled IP address to deliver an account creation verification for an account created using the name of a United States identity theft victim. Further, the conspirators caused Exchange 2 to use IP addresses located in the Eastern District of Virginia on other occasions. For instance, the conspirators linked a United States bank account to this fraudulently obtained Exchange 2 account. This action resulted in Exchange 2 using the AWS infrastructure located in the Eastern District of Virginia to respond to the customer's account activity.

b. On or about August 9, 2016, Exchange 2 used AWS-controlled IP address to deliver an account creation verification for an account set up in the name of a United States identity theft victim. Further, the conspirators caused Exchange 2 to use IP addresses associated with a computer located in the Eastern District of Virginia on other occasions.

c. On or about August 9, 2016, Exchange 2 used a computer associated with an AWS-controlled IP address to deliver an account creation verification for an account set up in the name of a United States identity theft victim. Further, the conspirators caused Exchange 2 to use a computer associated with IP addresses located in the Eastern District of Virginia on other occasions.

K. LIFSHITS and Co-Conspirators Deprived Exchange 1 of its Property

76. Law enforcement spoke with compliance personnel at Exchange 1. Compliance personnel stated that in order to comply with federal law and regulations, Exchange 1 is required to identify its customers. For that purpose, Exchange 1 collects personally identifiable information from account applicants. Exchange 1 then directs applicants to a third-party service provider that requires the applicant to upload a photo of their government-issued photo identification, as well as a photo of themselves. The third-party service provider then examines these documents and photos for authenticity and signs of tampering. Compliance personnel stated that Exchange 1 does this to comply both with law and regulations and to prevent fraud on their platform.

77. Exchange 1 compliance personnel stated that Exchange 1 would not open an account if it knew that an applicant used fraudulent identifiers or a fraudulent identity document to register an account. Compliance personnel stated that regulatory fines could be levied against

the company, and that "fraudsters" operating on the Exchange 1 platform could expose the company to civil liability. Compliance personnel stated that individuals using false identifications to establish Exchange 1 accounts are likely using the accounts for other unlawful activity, which exposes the company to even greater regulatory penalties, including possible fines. Indeed, Exchange 1 also holds financial institution licenses in several states, and states could levy their own penalties. For these reasons, Exchange 1 considers itself a victim of fraud whenever a user opens or uses an account — including, specifically, the T.W. Exchange 1 account used by LIFSHITS — that is predicated on fraudulent or stolen identity information.

78. Thus, by opening and using the T.W. Exchange 1 Account, which was setup using the stolen identifiers of a real United States person, LIFSHITS and his co-conspirators through their fraudulent misrepresentations deprived Exchange 1 of its right to control its assets. According to Exchange 1 compliance personnel, the misrepresentations that were made in opening the T.W. Exchange 1 Account could cause tangible economic harm, which is why Exchange 1 does not knowingly permit customers to use stolen identifiers to open accounts. *See, e.g., United States v. Lebedev*, 932 F.3d 40, 48-49 (2d Cir. 2019) (holding that financial institutions were deprived of their right to control their assets when a defendant disguised that he operated an illegal money service business); *see also United States v. Finazzo*, 850 F.3d 94, 110-11 (2d Cir. 2017) (holding that misrepresentations or nondisclosure of information may support mail or wire fraud conviction under "right to control" theory if misrepresentations or nondisclosures can or do result in tangible economic harm); *United States v. Binday*, 804 F.3d 587, 571 (2d Cir. 2015) (holding cognizable harm occurs under mail and wire fraud statutes where defendant misrepresentations deprive a victim of potentially valuable economic information).

L. LIFSHITS and his Co-Conspirators Conspired to Commit Aggravated Identity Theft

79. As described in the previous section, on December 29, 2017, LIFSHITS accessed the T.W. Exchange 1 Account to transfer funds to his personal Exchange 3 account. By doing so, LIFSHITS knowingly possessed and used the identification of United States individual, T.W., in order to transact the wire scheme in transferring funds between cryptocurrency accounts. In particular, he accessed T.W.'s name, date of birth, and address. This type of personally identifiable information is a "means of identification" as defined in Title 18, United States Code, Section 1028(d)(7).

80. Moreover, based on Exchange 1's thorough account verification features, LIFSHITS and his co-conspirators had every reason to believe that the personally identifiable information used to open the T.W. Exchange 1 Account belonged to a real United States person.

81. Based on the forensic cryptocurrency analysis, the IP address usage, Exchange 1's verification procedures, and the statements made by the victim, when LIFSHITS accessed the T.W. Exchange 1 Account and then proceeded to transfer funds from that account to his Exchange 3 accounts, LIFSHITS knowingly and unlawfully used T.W.'s means of identification in furtherance of the scheme to defraud Exchange 1 of its property. I therefore submit that there is probable cause to believe that LIFSHITS committed and conspired to commit aggravated identity theft, in violation of Title 18, United States Code, Section 1028A.

CONCLUSION

82. Based on the facts set forth above, I submit there is probable cause to believe that from a date unknown, but by at least in and around January 2017 to the present, the exact dates being unknown, in the Eastern District of Virginia and elsewhere, the defendant, ARTEM MIKHAYLOVICH LIFSHITS, unlawfully and knowingly combined, conspired, confederated, and agreed with others, both known and unknown, to execute and attempt to execute a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and did transmit or caused to be transmitted by means of wire communication in interstate commerce, any writings, signs, signals, pictures, and sounds for the purpose of executing such scheme or artifice, in violation of Title 18, United States Code, Section 1343, all in violation of Title 18, United States Code, Section 1349.

Heather Turner
Special Agent
United States Secret Service

Reviewed by AUSAs Carina A. Cuellar and Jay V. Prabhu.

Subscribed and sworn to before me via telephone this 10th day of September 2020.

Digitally signed by Theresa Carroll Buchanan
Date: 2020.09.10 11:10:57 -04'00'

The Honorable Theresa Carroll Buchanan
United States Magistrate Judge

Attachment A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	*	
	*	CRIMINAL NO.
v.	*	
	*	(18 U.S.C. §§ 2, 371, 1349, 1028A)
INTERNET RESEARCH AGENCY LLC A/K/A MEDIASINTEZ LLC A/K/A GLAVSET LLC A/K/A MIXINFO LLC A/K/A AZIMUT LLC A/K/A NOVINFO LLC,	*	
CONCORD MANAGEMENT AND CONSULTING LLC,	*	
CONCORD CATERING,	*	
YEVGENIY VIKTOROVICH PRIGOZHIN,	*	
MIKHAIL IVANOVICH BYSTROV,	*	
MIKHAIL LEONIDOVICH BURCHIK A/K/A MIKHAIL ABRAMOV,	*	
ALEKSANDRA YURYEVNA KRYLOVA,	*	
ANNA VLADISLAVOVNA BOGACHEVA,	*	
SERGEY PAVLOVICH POLOZOV,	*	
MARIA ANATOLYEVNA BOVDA A/K/A MARIA ANATOLYEVNA BELYAEVA,	*	
ROBERT SERGEYEVICH BOVDA,	*	
DZHEYKHUN NASIMI OGLY ASLANOV A/K/A JAYHOON ASLANOV A/K/A JAY ASLANOV,	*	
VADIM VLADIMIROVICH PODKOPAEV,	*	
GLEB IGOREVICH VASILCHENKO,	*	
IRINA VIKTOROVNA KAVERZINA,	*	
and	*	
VLADIMIR VENKOV.	*******	

Defendants.

INDICTMENT

The Grand Jury for the District of Columbia charges:

Introduction

1. The United States of America, through its departments and agencies, regulates the activities of foreign individuals and entities in and affecting the United States in order to prevent, disclose, and counteract improper foreign influence on U.S. elections and on the U.S. political system. U.S. law bans foreign nationals from making certain expenditures or financial disbursements for the purpose of influencing federal elections. U.S. law also bars agents of any foreign entity from engaging in political activities within the United States without first registering with the Attorney General. And U.S. law requires certain foreign nationals seeking entry to the United States to obtain a visa by providing truthful and accurate information to the government. Various federal agencies, including the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State, are charged with enforcing these laws.

2. Defendant INTERNET RESEARCH AGENCY LLC ("ORGANIZATION") is a Russian organization engaged in operations to interfere with elections and political processes. Defendants MIKHAIL IVANOVICH BYSTROV, MIKHAIL LEONIDOVICH BURCHIK, ALEKSANDRA YURYEVNA KRYLOVA, ANNA VLADISLAVOVNA BOGACHEVA, SERGEY PAVLOVICH POLOZOV, MARIA ANATOLYEVNA BOVDA, ROBERT SERGEYEVICH BOVDA, DZHEYKHUN NASIMI OGLY ASLANOV, VADIM VLADIMIROVICH PODKOPAEV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV worked in various capacities to carry out Defendant ORGANIZATION's interference operations targeting the United States. From in or around 2014 to the present, Defendants knowingly and intentionally conspired with each other (and with persons known and unknown to

the Grand Jury) to defraud the United States by impairing, obstructing, and defeating the lawful functions of the government through fraud and deceit for the purpose of interfering with the U.S. political and electoral processes, including the presidential election of 2016.

3. Beginning as early as 2014, Defendant ORGANIZATION began operations to interfere with the U.S. political system, including the 2016 U.S. presidential election. Defendant ORGANIZATION received funding for its operations from Defendant YEVGENIY VIKTOROVICH PRIGOZHIN and companies he controlled, including Defendants CONCORD MANAGEMENT AND CONSULTING LLC and CONCORD CATERING (collectively "CONCORD"). Defendants CONCORD and PRIGOZHIN spent significant funds to further the ORGANIZATION's operations and to pay the remaining Defendants, along with other uncharged ORGANIZATION employees, salaries and bonuses for their work at the ORGANIZATION.

4. Defendants, posing as U.S. persons and creating false U.S. personas, operated social media pages and groups designed to attract U.S. audiences. These groups and pages, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by Defendants. Defendants also used the stolen identities of real U.S. persons to post on ORGANIZATION-controlled social media accounts. Over time, these social media accounts became Defendants' means to reach significant numbers of Americans for purposes of interfering with the U.S. political system, including the presidential election of 2016.

5. Certain Defendants traveled to the United States under false pretenses for the purpose of collecting intelligence to inform Defendants' operations. Defendants also procured and used computer infrastructure, based partly in the United States, to hide the Russian origin of their activities and to avoid detection by U.S. regulators and law enforcement.

6. Defendant ORGANIZATION had a strategic goal to sow discord in the U.S. political system, including the 2016 U.S. presidential election. Defendants posted derogatory information about a number of candidates, and by early to mid-2016, Defendants' operations included supporting the presidential campaign of then-candidate Donald J. Trump ("Trump Campaign") and disparaging Hillary Clinton. Defendants made various expenditures to carry out those activities, including buying political advertisements on social media in the names of U.S. persons and entities. Defendants also staged political rallies inside the United States, and while posing as U.S. grassroots entities and U.S. persons, and without revealing their Russian identities and ORGANIZATION affiliation, solicited and compensated real U.S. persons to promote or disparage candidates. Some Defendants, posing as U.S. persons and without revealing their Russian association, communicated with unwitting individuals associated with the Trump Campaign and with other political activists to seek to coordinate political activities.

7. In order to carry out their activities to interfere in U.S. political and electoral processes without detection of their Russian affiliation, Defendants conspired to obstruct the lawful functions of the United States government through fraud and deceit, including by making expenditures in connection with the 2016 U.S. presidential election without proper regulatory disclosure; failing to register as foreign agents carrying out political activities within the United States; and obtaining visas through false and fraudulent statements.

COUNT ONE

(Conspiracy to Defraud the United States)

8. Paragraphs 1 through 7 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

9. From in or around 2014 to the present, in the District of Columbia and elsewhere,

Defendants, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to defraud the United States by impairing, obstructing, and defeating the lawful functions of the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State in administering federal requirements for disclosure of foreign involvement in certain domestic activities.

Defendants

10. Defendant INTERNET RESEARCH AGENCY LLC (Агентство Интернет Исследований) is a Russian organization engaged in political and electoral interference operations. In or around July 2013, the ORGANIZATION registered with the Russian government as a Russian corporate entity. Beginning in or around June 2014, the ORGANIZATION obscured its conduct by operating through a number of Russian entities, including Internet Research LLC, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, and NovInfo LLC. Starting in or around 2014, the ORGANIZATION occupied an office at 55 Savushkina Street in St. Petersburg, Russia. That location became one of the ORGANIZATION's operational hubs from which Defendants and other co-conspirators carried out their activities to interfere in the U.S. political system, including the 2016 U.S. presidential election.

a. The ORGANIZATION employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The ORGANIZATION's annual budget totaled the equivalent of millions of U.S. dollars.

b. The ORGANIZATION was headed by a management group and organized into departments, including: a graphics department; a data analysis department; a search-engine optimization ("SEO") department; an information-technology ("IT")

department to maintain the digital infrastructure used in the ORGANIZATION's operations; and a finance department to budget and allocate funding.

c. The ORGANIZATION sought, in part, to conduct what it called "information warfare against the United States of America" through fictitious U.S. personas on social media platforms and other Internet-based media.

d. By in or around April 2014, the ORGANIZATION formed a department that went by various names but was at times referred to as the "translator project." This project focused on the U.S. population and conducted operations on social media platforms such as YouTube, Facebook, Instagram, and Twitter. By approximately July 2016, more than eighty ORGANIZATION employees were assigned to the translator project.

e. By in or around May 2014, the ORGANIZATION's strategy included interfering with the 2016 U.S. presidential election, with the stated goal of "spread[ing] distrust towards the candidates and the political system in general."

11. Defendants CONCORD MANAGEMENT AND CONSULTING LLC (Конкорд Менеджмент и Консалтинг) and CONCORD CATERING are related Russian entities with various Russian government contracts. CONCORD was the ORGANIZATION's primary source of funding for its interference operations. CONCORD controlled funding, recommended personnel, and oversaw ORGANIZATION activities through reporting and interaction with ORGANIZATION management.

a. CONCORD funded the ORGANIZATION as part of a larger CONCORD-funded interference operation that it referred to as "Project Lakhta." Project Lakhta had multiple components, some involving domestic audiences within the Russian

Federation and others targeting foreign audiences in various countries, including the United States.

b. By in or around September 2016, the ORGANIZATION's monthly budget for Project Lakhta submitted to CONCORD exceeded 73 million Russian rubles (over 1,250,000 U.S. dollars), including approximately one million rubles in bonus payments.

c. To conceal its involvement, CONCORD labeled the monies paid to the ORGANIZATION for Project Lakhta as payments related to software support and development. To further conceal the source of funds, CONCORD distributed monies to the ORGANIZATION through approximately fourteen bank accounts held in the names of CONCORD affiliates, including Glavnaya Liniya LLC, Merkuriy LLC, Obshchepit LLC, Potentsial LLC, RSP LLC, ASP LLC, MTTs LLC, Kompleksservis LLC, SPb Kulinariya LLC, Almira LLC, Pishchevik LLC, Galant LLC, Rayteks LLC, and Standart LLC.

12. Defendant YEVGENIY VIKTOROVICH PRIGOZHIN (Пригожин Евгений Викторович) is a Russian national who controlled CONCORD.

a. PRIGOZHIN approved and supported the ORGANIZATION's operations, and Defendants and their co-conspirators were aware of PRIGOZHIN's role.

b. For example, on or about May 29, 2016, Defendants and their co-conspirators, through an ORGANIZATION-controlled social media account, arranged for a real U.S. person to stand in front of the White House in the District of Columbia under false pretenses to hold a sign that read "Happy 55th Birthday Dear Boss." Defendants and their co-conspirators informed the real U.S. person that the sign

was for someone who "is a leader here and our boss . . . our funder." PRIGOZHIN's Russian passport identifies his date of birth as June 1, 1961.

13. Defendant MIKHAIL IVANOVICH BYSTROV (Быстров Михаил Иванович) joined the ORGANIZATION by at least in or around February 2014.

a. By approximately April 2014, BYSTROV was the general director, the ORGANIZATION's highest-ranking position. BYSTROV subsequently served as the head of various other entities used by the ORGANIZATION to mask its activities, including, for example, Glavset LLC, where he was listed as that entity's general director.

b. In or around 2015 and 2016, BYSTROV frequently communicated with PRIGOZHIN about Project Lakhta's overall operations, including through regularly scheduled in-person meetings.

14. Defendant MIKHAIL LEONIDOVICH BURCHIK (Бурчик Михаил Леонидович) A/K/A MIKHAIL ABRAMOV joined the ORGANIZATION by at least in or around October 2013. By approximately March 2014, BURCHIK was the executive director, the ORGANIZATION's second-highest ranking position. Throughout the ORGANIZATION's operations to interfere in the U.S political system, including the 2016 U.S. presidential election, BURCHIK was a manager involved in operational planning, infrastructure, and personnel. In or around 2016, BURCHIK also had in-person meetings with PRIGOZHIN.

15. Defendant ALEKSANDRA YURYEVNA KRYLOVA (Крылова Александра Юрьевна) worked for the ORGANIZATION from at least in or around September 2013 to at least in or around November 2014. By approximately April 2014, KRYLOVA served as director and was the ORGANIZATION's third-highest ranking employee. In 2014, KRYLOVA traveled to the United

States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations.

16. Defendant SERGEY PAVLOVICH POLOZOV (Полозов Сергей Павлович) worked for the ORGANIZATION from at least in or around April 2014 to at least in or around October 2016. POLOZOV served as the manager of the IT department and oversaw the procurement of U.S. servers and other computer infrastructure that masked the ORGANIZATION's Russian location when conducting operations within the United States.

17. Defendant ANNA VLADISLAVOVNA BOGACHEVA (Богачева Анна Владиславовна) worked for the ORGANIZATION from at least in or around April 2014 to at least in or around July 2014. BOGACHEVA served on the translator project and oversaw the project's data analysis group. BOGACHEVA also traveled to the United States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations.

18. Defendant MARIA ANATOLYEVNA BOVDA (Бовда Мария Анатольевна) A/K/A MARIA ANATOLYEVNA BELYAEVA ("M. BOVDA") worked for the ORGANIZATION from at least in or around November 2013 to at least in or around October 2014. M. BOVDA served as the head of the translator project, among other positions.

19. Defendant ROBERT SERGEYEVICH BOVDA (Бовда Роберт Сергеевич) ("R. BOVDA") worked for the ORGANIZATION from at least in or around November 2013 to at least in or around October 2014. R. BOVDA served as the deputy head of the translator project, among other positions. R. BOVDA attempted to travel to the United States under false pretenses for the purpose of collecting intelligence to inform the ORGANIZATION's operations but could not obtain the necessary visa.

20. Defendant DZHEYKHUN NASIMI OGLY ASLANOV (Асланов Джейхун Насими Оглы) A/K/A JAYHOON ASLANOV A/K/A JAY ASLANOV joined the ORGANIZATION by at least in or around September 2014. ASLANOV served as head of the translator project and oversaw many of the operations targeting the 2016 U.S. presidential election. ASLANOV was also listed as the general director of Azimut LLC, an entity used to move funds from CONCORD to the ORGANIZATION.

21. Defendant VADIM VLADIMIROVICH PODKOPAEV (Подкопаев Вадим Владимирович) joined the ORGANIZATION by at least in or around June 2014. PODKOPAEV served as an analyst on the translator project and was responsible for conducting U.S.-focused research and drafting social media content for the ORGANIZATION.

22. Defendant GLEB IGOREVICH VASILCHENKO (Васильченко Глеб Игоревич) worked for the ORGANIZATION from at least in or around August 2014 to at least in or around September 2016. VASILCHENKO was responsible for posting, monitoring, and updating the social media content of many ORGANIZATION-controlled accounts while posing as U.S. persons or U.S. grassroots organizations. VASILCHENKO later served as the head of two sub-groups focused on operations to interfere in the U.S. political system, including the 2016 U.S. presidential election.

23. Defendant IRINA VIKTOROVNA KAVERZINA (Каверзина Ирина Викторовна) joined the ORGANIZATION by at least in or around October 2014. KAVERZINA served on the translator project and operated multiple U.S. personas that she used to post, monitor, and update social media content for the ORGANIZATION.

24. Defendant VLADIMIR VENKOV (Венков Владимир) joined the ORGANIZATION by at least in or around March 2015. VENKOV served on the translator project and operated multiple

U.S. personas, which he used to post, monitor, and update social media content for the ORGANIZATION.

Federal Regulatory Agencies

25. The Federal Election Commission is a federal agency that administers the Federal Election Campaign Act ("FECA"). Among other things, FECA prohibits foreign nationals from making any contributions, expenditures, independent expenditures, or disbursements for electioneering communications. FECA also requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission. The reporting requirements permit the Federal Election Commission to fulfill its statutory duties of providing the American public with accurate data about the financial activities of individuals and entities supporting federal candidates, and enforcing FECA's limits and prohibitions, including the ban on foreign expenditures.

26. The U.S. Department of Justice administers the Foreign Agent Registration Act ("FARA"). FARA establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law. FARA requires, among other things, that persons subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them. Disclosure of the required information allows the federal government and the American people to evaluate the statements and activities of such persons in light of their function as foreign agents.

27. The U.S. Department of State is the federal agency responsible for the issuance of non-immigrant visas to foreign individuals who need a visa to enter the United States. Foreign

individuals who are required to obtain a visa must, among other things, provide truthful information in response to questions on the visa application form, including information about their employment and the purpose of their visit to the United States.

Object of the Conspiracy

28. The conspiracy had as its object impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable the Defendants to interfere with U.S. political and electoral processes, including the 2016 U.S. presidential election.

Manner and Means of the Conspiracy

Intelligence-Gathering to Inform U.S. Operations

29. Starting at least in or around 2014, Defendants and their co-conspirators began to track and study groups on U.S. social media sites dedicated to U.S. politics and social issues. In order to gauge the performance of various groups on social media sites, the ORGANIZATION tracked certain metrics like the group's size, the frequency of content placed by the group, and the level of audience engagement with that content, such as the average number of comments or responses to a post.

30. Defendants and their co-conspirators also traveled, and attempted to travel, to the United States under false pretenses in order to collect intelligence for their interference operations.

a. KRYLOVA and BOGACHEVA, together with other Defendants and co-conspirators, planned travel itineraries, purchased equipment (such as cameras, SIM cards, and drop phones), and discussed security measures (including "evacuation scenarios") for Defendants who traveled to the United States.

b. To enter the United States, KRYLOVA, BOGACHEVA, R. BOVDA, and another co-conspirator applied to the U.S. Department of State for visas to travel. During

their application process, KRYLOVA, BOGACHEVA, R. BOVDA, and their co-conspirator falsely claimed they were traveling for personal reasons and did not fully disclose their place of employment to hide the fact that they worked for the ORGANIZATION.

c. Only KRYLOVA and BOGACHEVA received visas, and from approximately June 4, 2014 through June 26, 2014, KRYLOVA and BOGACHEVA traveled in and around the United States, including stops in Nevada, California, New Mexico, Colorado, Illinois, Michigan, Louisiana, Texas, and New York to gather intelligence. After the trip, KRYLOVA and BURCHIK exchanged an intelligence report regarding the trip.

d. Another co-conspirator who worked for the ORGANIZATION traveled to Atlanta, Georgia from approximately November 26, 2014 through November 30, 2014. Following the trip, the co-conspirator provided POLOZOV a summary of his trip's itinerary and expenses.

31. In order to collect additional intelligence, Defendants and their co-conspirators posed as U.S. persons and contacted U.S. political and social activists. For example, starting in or around June 2016, Defendants and their co-conspirators, posing online as U.S. persons, communicated with a real U.S. person affiliated with a Texas-based grassroots organization. During the exchange, Defendants and their co-conspirators learned from the real U.S. person that they should focus their activities on "purple states like Colorado, Virginia & Florida." After that exchange, Defendants and their co-conspirators commonly referred to targeting "purple states" in directing their efforts.

Use of U.S. Social Media Platforms

32. Defendants and their co-conspirators, through fraud and deceit, created hundreds of social media accounts and used them to develop certain fictitious U.S. personas into "leader[s] of public opinion" in the United States.

33. ORGANIZATION employees, referred to as "specialists," were tasked to create social media accounts that appeared to be operated by U.S. persons. The specialists were divided into day-shift and night-shift hours and instructed to make posts in accordance with the appropriate U.S. time zone. The ORGANIZATION also circulated lists of U.S. holidays so that specialists could develop and post appropriate account activity. Specialists were instructed to write about topics germane to the United States such as U.S. foreign policy and U.S. economic issues. Specialists were directed to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements."

34. Defendants and their co-conspirators also created thematic group pages on social media sites, particularly on the social media platforms Facebook and Instagram. ORGANIZATION-controlled pages addressed a range of issues, including: immigration (with group names including "Secured Borders"); the Black Lives Matter movement (with group names including "Blacktivist"); religion (with group names including "United Muslims of America" and "Army of Jesus"); and certain geographic regions within the United States (with group names including "South United" and "Heart of Texas"). By 2016, the size of many ORGANIZATION-controlled groups had grown to hundreds of thousands of online followers.

35. Starting at least in or around 2015, Defendants and their co-conspirators began to purchase advertisements on online social media sites to promote ORGANIZATION-controlled social media groups, spending thousands of U.S. dollars every month. These expenditures were included in the budgets the ORGANIZATION submitted to CONCORD.

36. Defendants and their co-conspirators also created and controlled numerous Twitter accounts designed to appear as if U.S. persons or groups controlled them. For example, the ORGANIZATION created and controlled the Twitter account "Tennessee GOP," which used the handle @TEN_GOP. The @TEN_GOP account falsely claimed to be controlled by a U.S. state political party. Over time, the @TEN_GOP account attracted more than 100,000 online followers.

37. To measure the impact of their online social media operations, Defendants and their co-conspirators tracked the performance of content they posted over social media. They tracked the size of the online U.S. audiences reached through posts, different types of engagement with the posts (such as likes, comments, and reposts), changes in audience size, and other metrics. Defendants and their co-conspirators received and maintained metrics reports on certain group pages and individualized posts.

38. Defendants and their co-conspirators also regularly evaluated the content posted by specialists (sometimes referred to as "content analysis") to ensure they appeared authentic—as if operated by U.S. persons. Specialists received feedback and directions to improve the quality of their posts. Defendants and their co-conspirators issued or received guidance on: ratios of text, graphics, and video to use in posts; the number of accounts to operate; and the role of each account (for example, differentiating a main account from which to post information and auxiliary accounts to promote a main account through links and reposts).

Use of U.S. Computer Infrastructure

39. To hide their Russian identities and ORGANIZATION affiliation, Defendants and their co-conspirators—particularly POLOZOV and the ORGANIZATION's IT department—purchased space on computer servers located inside the United States in order to set up virtual private networks ("VPNs"). Defendants and their co-conspirators connected from Russia to the U.S.-

based infrastructure by way of these VPNs and conducted activity inside the United States—including accessing online social media accounts, opening new accounts, and communicating with real U.S. persons—while masking the Russian origin and control of the activity.

40. Defendants and their co-conspirators also registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names so as to appear to be U.S. persons and groups. From these accounts, Defendants and their co-conspirators registered or linked to online social media accounts in order to monitor them; posed as U.S. persons when requesting assistance from real U.S. persons; contacted media outlets in order to promote activities inside the United States; and conducted other operations, such as those set forth below.

Use of Stolen U.S. Identities

41. In or around 2016, Defendants and their co-conspirators also used, possessed, and transferred, without lawful authority, the social security numbers and dates of birth of real U.S. persons without those persons' knowledge or consent. Using these means of identification, Defendants and their co-conspirators opened accounts at PayPal, a digital payment service provider; created false means of identification, including fake driver's licenses; and posted on ORGANIZATION-controlled social media accounts using the identities of these U.S. victims. Defendants and their co-conspirators also obtained, and attempted to obtain, false identification documents to use as proof of identity in connection with maintaining accounts and purchasing advertisements on social media sites.

Actions Targeting the 2016 U.S. Presidential Election

42. By approximately May 2014, Defendants and their co-conspirators discussed efforts to interfere in the 2016 U.S. presidential election. Defendants and their co-conspirators began to monitor U.S. social media accounts and other sources of information about the 2016 U.S. presidential election.

43. By 2016, Defendants and their co-conspirators used their fictitious online personas to interfere with the 2016 U.S. presidential election. They engaged in operations primarily intended to communicate derogatory information about Hillary Clinton, to denigrate other candidates such as Ted Cruz and Marco Rubio, and to support Bernie Sanders and then-candidate Donald Trump.

a. On or about February 10, 2016, Defendants and their co-conspirators internally circulated an outline of themes for future content to be posted to ORGANIZATION-controlled social media accounts. Specialists were instructed to post content that focused on "politics in the USA" and to "use any opportunity to criticize Hillary and the rest (except Sanders and Trump—we support them)."

b. On or about September 14, 2016, in an internal review of an ORGANIZATION-created and controlled Facebook group called "Secured Borders," the account specialist was criticized for having a "low number of posts dedicated to criticizing Hillary Clinton" and was told "it is imperative to intensify criticizing Hillary Clinton" in future posts.

44. Certain ORGANIZATION-produced materials about the 2016 U.S. presidential election used election-related hashtags, including: "#Trump2016," "#TrumpTrain," "#MAGA," "#IWontProtectHillary," and "#Hillary4Prison." Defendants and their co-conspirators also established additional online social media accounts dedicated to the 2016 U.S. presidential election, including the Twitter account "March for Trump" and Facebook accounts "Clinton FRAUDation" and "Trumpsters United."

45. Defendants and their co-conspirators also used false U.S. personas to communicate with unwitting members, volunteers, and supporters of the Trump Campaign involved in local community outreach, as well as grassroots groups that supported then-candidate Trump. These

individuals and entities at times distributed the ORGANIZATION's materials through their own accounts via retweets, reposts, and similar means. Defendants and their co-conspirators then monitored the propagation of content through such participants.

46. In or around the latter half of 2016, Defendants and their co-conspirators, through their ORGANIZATION-controlled personas, began to encourage U.S. minority groups not to vote in the 2016 U.S. presidential election or to vote for a third-party U.S. presidential candidate.

a. On or about October 16, 2016, Defendants and their co-conspirators used the ORGANIZATION-controlled Instagram account "Woke Blacks" to post the following message: "[A] particular hype and hatred for Trump is misleading the people and forcing Blacks to vote Killary. We cannot resort to the lesser of two devils. Then we'd surely be better off without voting AT ALL."

b. On or about November 3, 2016, Defendants and their co-conspirators purchased an advertisement to promote a post on the ORGANIZATION-controlled Instagram account "Blacktivist" that read in part: "Choose peace and vote for Jill Stein. Trust me, it's not a wasted vote."

c. By in or around early November 2016, Defendants and their co-conspirators used the ORGANIZATION-controlled "United Muslims of America" social media accounts to post anti-vote messages such as: "American Muslims [are] boycotting elections today, most of the American Muslim voters refuse to vote for Hillary Clinton because she wants to continue the war on Muslims in the middle east and voted yes for invading Iraq."

47. Starting in or around the summer of 2016, Defendants and their co-conspirators also began to promote allegations of voter fraud by the Democratic Party through their fictitious U.S. personas

and groups on social media. Defendants and their co-conspirators purchased advertisements on Facebook to further promote the allegations.

a. On or about August 4, 2016, Defendants and their co-conspirators began purchasing advertisements that promoted a post on the ORGANIZATION-controlled Facebook account "Stop A.I." The post alleged that "Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus."

b. On or about August 11, 2016, Defendants and their co-conspirators posted that allegations of voter fraud were being investigated in North Carolina on the ORGANIZATION-controlled Twitter account @TEN_GOP.

c. On or about November 2, 2016, Defendants and their co-conspirators used the same account to post allegations of "#VoterFraud by counting tens of thousands of ineligible mail in Hillary votes being reported in Broward County, Florida."

Political Advertisements

48. From at least April 2016 through November 2016, Defendants and their co-conspirators, while concealing their Russian identities and ORGANIZATION affiliation through false personas, began to produce, purchase, and post advertisements on U.S. social media and other online sites expressly advocating for the election of then-candidate Trump or expressly opposing Clinton. Defendants and their co-conspirators did not report their expenditures to the Federal Election Commission, or register as foreign agents with the U.S. Department of Justice.

49. To pay for the political advertisements, Defendants and their co-conspirators established various Russian bank accounts and credit cards, often registered in the names of fictitious U.S. personas created and used by the ORGANIZATION on social media. Defendants and their co-conspirators also paid for other political advertisements using PayPal accounts.

50. The political advertisements included the following:

Approximate Date	Excerpt of Advertisement
April 6, 2016	"You know, a great number of black people support us saying that #HillaryClintonIsNotMyPresident"
April 7, 2016	"I say no to Hillary Clinton / I say no to manipulation"
April 19, 2016	"JOIN our #HillaryClintonForPrison2016"
May 10, 2016	"Donald wants to defeat terrorism . . . Hillary wants to sponsor it"
May 19, 2016	"Vote Republican, vote Trump, and support the Second Amendment!"
May 24, 2016	"Hillary Clinton Doesn't Deserve the Black Vote"
June 7, 2016	"Trump is our only hope for a better future!"
June 30, 2016	"#NeverHillary #HillaryForPrison #Hillary4Prison #HillaryForPrison2016 #Trump2016 #Trump #Trump4President"
July 20, 2016	"Ohio Wants Hillary 4 Prison"
August 4, 2016	"Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus."
August 10, 2016	"We cannot trust Hillary to take care of our veterans!"
October 14, 2016	"Among all the candidates Donald Trump is the one and only who can defend the police from terrorists."
October 19, 2016	"Hillary is a Satan, and her crimes and lies had proved just how evil she is."

Staging U.S. Political Rallies in the United States

51. Starting in approximately June 2016, Defendants and their co-conspirators organized and coordinated political rallies in the United States. To conceal the fact that they were based in Russia, Defendants and their co-conspirators promoted these rallies while pretending to be U.S. grassroots activists who were located in the United States but unable to meet or participate in person.

Defendants and their co-conspirators did not register as foreign agents with the U.S. Department of Justice.

52. In order to build attendance for the rallies, Defendants and their co-conspirators promoted the events through public posts on their false U.S. persona social media accounts. In addition, Defendants and their co-conspirators contacted administrators of large social media groups focused on U.S. politics and requested that they advertise the rallies.

53. In or around late June 2016, Defendants and their co-conspirators used the Facebook group "United Muslims of America" to promote a rally called "Support Hillary. Save American Muslims" held on July 9, 2016 in the District of Columbia. Defendants and their co-conspirators recruited a real U.S. person to hold a sign depicting Clinton and a quote attributed to her stating "I think Sharia Law will be a powerful new direction of freedom." Within three weeks, on or about July 26, 2016, Defendants and their co-conspirators posted on the same Facebook page that Muslim voters were "between Hillary Clinton and a hard place."

54. In or around June and July 2016, Defendants and their co-conspirators used the Facebook group "Being Patriotic," the Twitter account @March_for_Trump, and other ORGANIZATION accounts to organize two political rallies in New York. The first rally was called "March for Trump" and held on June 25, 2016. The second rally was called "Down with Hillary" and held on July 23, 2016.

a. In or around June through July 2016, Defendants and their co-conspirators purchased advertisements on Facebook to promote the "March for Trump" and "Down with Hillary" rallies.

b. Defendants and their co-conspirators used false U.S. personas to send individualized messages to real U.S. persons to request that they participate in and

help organize the rally. To assist their efforts, Defendants and their co-conspirators, through false U.S. personas, offered money to certain U.S. persons to cover rally expenses.

c. On or about June 5, 2016, Defendants and their co-conspirators, while posing as a U.S. grassroots activist, used the account @March_for_Trump to contact a volunteer for the Trump Campaign in New York. The volunteer agreed to provide signs for the "March for Trump" rally.

55. In or around late July 2016, Defendants and their co-conspirators used the Facebook group "Being Patriotic," the Twitter account @March_for_Trump, and other false U.S. personas to organize a series of coordinated rallies in Florida. The rallies were collectively referred to as "Florida Goes Trump" and held on August 20, 2016.

a. In or around August 2016, Defendants and their co-conspirators used false U.S. personas to communicate with Trump Campaign staff involved in local community outreach about the "Florida Goes Trump" rallies.

b. Defendants and their co-conspirators purchased advertisements on Facebook and Instagram to promote the "Florida Goes Trump" rallies.

c. Defendants and their co-conspirators also used false U.S. personas to contact multiple grassroots groups supporting then-candidate Trump in an unofficial capacity. Many of these groups agreed to participate in the "Florida Goes Trump" rallies and serve as local coordinators.

d. Defendants and their co-conspirators also used false U.S. personas to ask real U.S. persons to participate in the "Florida Goes Trump" rallies. Defendants and their co-conspirators asked certain of these individuals to perform tasks at the rallies.

For example, Defendants and their co-conspirators asked one U.S. person to build a cage on a flatbed truck and another U.S. person to wear a costume portraying Clinton in a prison uniform. Defendants and their co-conspirators paid these individuals to complete the requests.

56. After the rallies in Florida, Defendants and their co-conspirators used false U.S. personas to organize and coordinate U.S. political rallies supporting then-candidate Trump in New York and Pennsylvania. Defendants and their co-conspirators used the same techniques to build and promote these rallies as they had in Florida, including: buying Facebook advertisements; paying U.S. persons to participate in, or perform certain tasks at, the rallies; and communicating with real U.S. persons and grassroots organizations supporting then-candidate Trump.

57. After the election of Donald Trump in or around November 2016, Defendants and their co-conspirators used false U.S. personas to organize and coordinate U.S. political rallies in support of then president-elect Trump, while simultaneously using other false U.S. personas to organize and coordinate U.S. political rallies protesting the results of the 2016 U.S. presidential election. For example, in or around November 2016, Defendants and their co-conspirators organized a rally in New York through one ORGANIZATION-controlled group designed to "show your support for President-Elect Donald Trump" held on or about November 12, 2016. At the same time, Defendants and their co-conspirators, through another ORGANIZATION-controlled group, organized a rally in New York called "Trump is NOT my President" held on or about November 12, 2016. Similarly, Defendants and their co-conspirators organized a rally entitled "Charlotte Against Trump" in Charlotte, North Carolina, held on or about November 19, 2016.

Destruction of Evidence

58. In order to avoid detection and impede investigation by U.S. authorities of Defendants' operations, Defendants and their co-conspirators deleted and destroyed data, including emails, social media accounts, and other evidence of their activities.

a. Beginning in or around June 2014, and continuing into June 2015, public reporting began to identify operations conducted by the ORGANIZATION in the United States. In response, Defendants and their co-conspirators deleted email accounts used to conduct their operations.

b. Beginning in or around September 2017, U.S. social media companies, starting with Facebook, publicly reported that they had identified Russian expenditures on their platforms to fund political and social advertisements. Facebook's initial disclosure of the Russian purchases occurred on or about September 6, 2017, and included a statement that Facebook had "shared [its] findings with US authorities investigating these issues."

c. Media reporting on or about the same day as Facebook's disclosure referred to Facebook working with investigators for the Special Counsel's Office of the U.S. Department of Justice, which had been charged with investigating the Russian government's efforts to interfere in the 2016 presidential election.

d. Defendants and their co-conspirators thereafter destroyed evidence for the purpose of impeding the investigation. On or about September 13, 2017, KAVERZINA wrote in an email to a family member: "We had a slight crisis here at work: the FBI busted our activity (not a joke). So, I got preoccupied with covering tracks together with the colleagues." KAVERZINA further wrote, "I created all these pictures and posts, and the Americans believed that it was written by their people."

Overt Acts

59. In furtherance of the Conspiracy and to effect its illegal object, Defendants and their co-conspirators committed the following overt acts in connection with the staging of U.S. political rallies, as well as those as set forth in paragraphs 1 through 7, 9 through 27, and 29 through 58, which are re-alleged and incorporated by reference as though fully set forth herein.

60. On or about June 1, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for their "March for Trump" rally.

61. On or about June 4, 2016, Defendants and their co-conspirators used allforusa@yahoo.com, the email address of a false U.S. persona, to send out press releases for the "March for Trump" rally to New York media outlets.

62. On or about June 23, 2016, Defendants and their co-conspirators used the Facebook account registered under a false U.S. persona "Matt Skiber" to contact a real U.S. person to serve as a recruiter for the "March for Trump" rally, offering to "give you money to print posters and get a megaphone."

63. On or about June 24, 2016, Defendants and their co-conspirators purchased advertisements on Facebook to promote the "Support Hillary. Save American Muslims" rally.

64. On or about July 5, 2016, Defendants and their co-conspirators ordered posters for the "Support Hillary. Save American Muslims" rally, including the poster with the quote attributed to Clinton that read "I think Sharia Law will be a powerful new direction of freedom."

65. On or about July 8, 2016, Defendants and their co-conspirators communicated with a real U.S. person about the posters they had ordered for the "Support Hillary. Save American Muslims" rally.

66. On or about July 12, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for the "Down With Hillary" rally in New York.

67. On or about July 23, 2016, Defendants and their co-conspirators used the email address of a false U.S. persona, joshmilton024@gmail.com, to send out press releases to over thirty media outlets promoting the "Down With Hillary" rally at Trump Tower in New York City.

68. On or about July 28, 2016, Defendants and their co-conspirators posted a series of tweets through the false U.S. persona account @March_for_Trump stating that "[w]e're currently planning a series of rallies across the state of Florida" and seeking volunteers to assist.

69. On or about August 2, 2016, Defendants and their co-conspirators used the false U.S. persona "Matt Skiber" Facebook account to send a private message to a real Facebook account, "Florida for Trump," set up to assist then-candidate Trump in the state of Florida. In the first message, Defendants and their co-conspirators wrote:

> Hi there! I'm a member of Being Patriotic online community. Listen, we've got an idea. Florida is still a purple state and we need to paint it red. If we lose Florida, we lose America. We can't let it happen, right? What about organizing a YUGE pro-Trump flash mob in every Florida town? We are currently reaching out to local activists and we've got the folks who are okay to be in charge of organizing their events almost everywhere in FL. However, we still need your support. What do you think about that? Are you in?

70. On or about August 2, 2016, and August 3, 2016, Defendants and their co-conspirators, through the use of a stolen identity of a real U.S. person, T.W., sent emails to certain grassroots groups located in Florida that stated in part:

> My name is [T.W.] and I represent a conservative patriot community named as "Being Patriotic." . . . So we're gonna organize a flash mob across Florida to support Mr. Trump. We clearly understand that the elections winner will be predestined by purple states. And we must win Florida. . . . We got a lot of volunteers in ~25 locations and it's just the beginning. We're currently choosing venues for each

> location and recruiting more activists. This is why we ask you to spread this info and participate in the flash mob.

71. On or about August 4, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for the "Florida Goes Trump" rally. The advertisements reached over 59,000 Facebook users in Florida, and over 8,300 Facebook users responded to the advertisements by clicking on it, which routed users to the ORGANIZATION's "Being Patriotic" page.

72. Beginning on or about August 5, 2016, Defendants and their co-conspirators used the false U.S. persona @March_for_Trump Twitter account to recruit and later pay a real U.S. person to wear a costume portraying Clinton in a prison uniform at a rally in West Palm Beach.

73. Beginning on or about August 11, 2016, Defendants and their co-conspirators used the false U.S. persona "Matt Skiber" Facebook account to recruit a real U.S. person to acquire signs and a costume depicting Clinton in a prison uniform.

74. On or about August 15, 2016, Defendants and their co-conspirators received an email at one of their false U.S. persona accounts from a real U.S. person, a Florida-based political activist identified as the "Chair for the Trump Campaign" in a particular Florida county. The activist identified two additional sites in Florida for possible rallies. Defendants and their co-conspirators subsequently used their false U.S. persona accounts to communicate with the activist about logistics and an additional rally in Florida.

75. On or about August 16, 2016, Defendants and their co-conspirators used a false U.S. persona Instagram account connected to the ORGANIZATION-created group "Tea Party News" to purchase advertisements for the "Florida Goes Trump" rally.

76. On or about August 18, 2016, the real "Florida for Trump" Facebook account responded to the false U.S. persona "Matt Skiber" account with instructions to contact a member of the Trump Campaign ("Campaign Official 1") involved in the campaign's Florida operations and provided

Campaign Official 1's email address at the campaign domain donaldtrump.com. On approximately the same day, Defendants and their co-conspirators used the email address of a false U.S. persona, joshmilton024@gmail.com, to send an email to Campaign Official 1 at that donaldtrump.com email account, which read in part:

> Hello [Campaign Official 1], [w]e are organizing a state-wide event in Florida on August, 20 to support Mr. Trump. Let us introduce ourselves first. "Being Patriotic" is a grassroots conservative online movement trying to unite people offline. . . . [W]e gained a huge lot of followers and decided to somehow help Mr. Trump get elected. You know, simple yelling on the Internet is not enough. There should be real action. We organized rallies in New York before. Now we're focusing on purple states such as Florida.

The email also identified thirteen "confirmed locations" in Florida for the rallies and requested the campaign provide "assistance in each location."

77. On or about August 18, 2016, Defendants and their co-conspirators sent money via interstate wire to another real U.S. person recruited by the ORGANIZATION, using one of their false U.S. personas, to build a cage large enough to hold an actress depicting Clinton in a prison uniform.

78. On or about August 19, 2016, a supporter of the Trump Campaign sent a message to the ORGANIZATION-controlled "March for Trump" Twitter account about a member of the Trump Campaign ("Campaign Official 2") who was involved in the campaign's Florida operations and provided Campaign Official 2's email address at the domain donaldtrump.com. On or about the same day, Defendants and their co-conspirators used the false U.S. persona joshmilton024@gmail.com account to send an email to Campaign Official 2 at that donaldtrump.com email account.

79. On or about August 19, 2016, the real "Florida for Trump" Facebook account sent another message to the false U.S. persona "Matt Skiber" account to contact a member of the Trump

Campaign ("Campaign Official 3") involved in the campaign's Florida operations. On or about August 20, 2016, Defendants and their co-conspirators used the "Matt Skiber" Facebook account to contact Campaign Official 3.

80. On or about August 19, 2016, Defendants and their co-conspirators used the false U.S. persona "Matt Skiber" account to write to the real U.S. person affiliated with a Texas-based grassroots organization who previously had advised the false persona to focus on "purple states like Colorado, Virginia & Florida." Defendants and their co-conspirators told that U.S. person, "We were thinking about your recommendation to focus on purple states and this is what we're organizing in FL." Defendants and their co-conspirators then sent a link to the Facebook event page for the Florida rallies and asked that person to send the information to Tea Party members in Florida. The real U.S. person stated that he/she would share among his/her own social media contacts, who would pass on the information.

81. On or about August 24, 2016, Defendants and their co-conspirators updated an internal ORGANIZATION list of over 100 real U.S. persons contacted through ORGANIZATION-controlled false U.S. persona accounts and tracked to monitor recruitment efforts and requests. The list included contact information for the U.S. persons, a summary of their political views, and activities they had been asked to perform by Defendants and their co-conspirators.

82. On or about August 31, 2016, Defendants and their co-conspirators, using a U.S. persona, spoke by telephone with a real U.S. person affiliated with a grassroots group in Florida. That individual requested assistance in organizing a rally in Miami, Florida. On or about September 9, 2016, Defendants and their co-conspirators sent the group an interstate wire to pay for materials needed for the Florida rally on or about September 11, 2016.

83. On or about August 31, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for a rally they organized and scheduled in New York for September 11, 2016.

84. On or about September 9, 2016, Defendants and their co-conspirators, through a false U.S. persona, contacted the real U.S. person who had impersonated Clinton at the West Palm Beach rally. Defendants and their co-conspirators sent that U.S. person money via interstate wire as an inducement to travel from Florida to New York and to dress in costume at another rally they organized.

85. On or about September 22, 2016, Defendants and their co-conspirators created and purchased Facebook advertisements for a series of rallies they organized in Pennsylvania called "Miners for Trump" and scheduled for October 2, 2016.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO

(Conspiracy to Commit Wire Fraud and Bank Fraud)

86. Paragraphs 1 through 7, 9 through 27, and 29 through 85 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

87. From in or around 2016 through present, in the District of Columbia and elsewhere, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, and GLEB IGOREVICH VASILCHENKO, together with others known and unknown to the Grand Jury, knowingly and intentionally conspired to commit certain offenses against the United States, to wit:

a. to knowingly, having devised and intending to devise a scheme and artifice to defraud, and to obtain money and property by means of false and fraudulent

pretenses, representations, and promises, transmit and cause to be transmitted, by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purposes of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343; and

b. to knowingly execute and attempt to execute a scheme and artifice to defraud a federally insured financial institution, and to obtain monies, funds, credits, assets, securities and other property from said financial institution by means of false and fraudulent pretenses, representations, and promises, all in violation of Title 18, United States Code, Section 1344.

Object of the Conspiracy

88. The conspiracy had as its object the opening of accounts under false names at U.S. financial institutions and a digital payments company in order to receive and send money into and out of the United States to support the ORGANIZATION's operations in the United States and for self-enrichment.

Manner and Means of the Conspiracy

89. Beginning in at least 2016, Defendants and their co-conspirators used, without lawful authority, the social security numbers, home addresses, and birth dates of real U.S. persons without their knowledge or consent. Using these means of stolen identification, Defendants and their co-conspirators opened accounts at a federally insured U.S. financial institution ("Bank 1"), including the following accounts:

Approximate Date	Account Name	Means of Identification
June 16, 2016	T.B.	Social Security Number Date of Birth
July 21, 2016	A.R.	Social Security Number Date of Birth
July 27, 2016	T.C.	Social Security Number Date of Birth
August 2, 2016	T.W.	Social Security Number Date of Birth

90. Defendants and their co-conspirators also used, without lawful authority, the social security numbers, home addresses, and birth dates of real U.S. persons to open accounts at PayPal, a digital payments company, including the following accounts:

Approximate Date	Initials of Identity Theft Victim	Means of Identification
June 16, 2016	T.B.	Social Security Number Date of Birth
July 21, 2016	A.R.	Social Security Number Date of Birth
August 2, 2016	T.W.	Social Security Number Date of Birth
November 11, 2016	J.W.	Home Address
January 18, 2017	V.S.	Social Security Number

Defendants and their co-conspirators also established other accounts at PayPal in the names of false and fictitious U.S. personas. Some personas used to register PayPal accounts were the same as the false U.S. personas used in connection with the ORGANIZATION's social media accounts.

91. Defendants and their co-conspirators purchased credit card and bank account numbers from online sellers for the unlawful purpose of evading security measures at PayPal, which used account numbers to verify a user's identity. Many of the bank account numbers purchased by Defendants

and their co-conspirators were created using the stolen identities of real U.S. persons. After purchasing the accounts, Defendants and their co-conspirators submitted these bank account numbers to PayPal.

92. On or about the dates identified below, Defendants and their co-conspirators obtained and used the following fraudulent bank account numbers for the purpose of evading PayPal's security measures:

Approximate Date	Card/Bank Account Number	Financial Institution	Email Used to Acquire Account Number
June 13, 2016	xxxxxxxxx8902	Bank 2	wemakeweather@gmail.com
June 16, 2016	xxxxxx8731	Bank 1	allforusa@yahoo.com
July 21, 2016	xxxxxx2215	Bank 3	antwan_8@yahoo.com
August 2, 2016	xxxxxx5707	Bank 1	xtimwaltersx@gmail.com
October 18, 2016	xxxxxxxxx5792	Bank 4	unitedvetsofamerica@gmail.com
October 18, 2016	xxxxxxxxx4743	Bank 4	patriototus@gmail.com
November 11, 2016	xxxxxxxxx2427	Bank 4	beautifullelly@gmail.com
November 11, 2016	xxxxxxxxx7587	Bank 5	staceyredneck@gmail.com
November 11, 2016	xxxxxxxx7590	Bank 5	ihatecrime1@gmail.com
November 11, 2016	xxxxxxxx1780	Bank 6	staceyredneck@gmail.com
November 11, 2016	xxxxxxxx1762	Bank 6	ihatecrime1@gmail.com
December 13, 2016	xxxxxxxx6168	Bank 6	thetaylorbrooks@aol.com
March 30, 2017	xxxxxxxxx6316	Bank 3	wokeaztec@outlook.com
March 30, 2017	xxxxxx9512	Bank 3	wokeaztec@outlook.com

93. Additionally, and in order to maintain their accounts at PayPal and elsewhere, including online cryptocurrency exchanges, Defendants and their co-conspirators purchased and obtained false identification documents, including fake U.S. driver's licenses. Some false identification documents obtained by Defendants and their co-conspirators used the stolen identities of real U.S. persons, including U.S. persons T.W. and J.W.

94. After opening the accounts at Bank 1 and PayPal, Defendants and their co-conspirators used them to receive and send money for a variety of purposes, including to pay for certain ORGANIZATION expenses. Some PayPal accounts were used to purchase advertisements on Facebook promoting ORGANIZATION-controlled social media accounts. The accounts were also used to pay other ORGANIZATION-related expenses such as buttons, flags, and banners for rallies.

95. Defendants and their co-conspirators also used the accounts to receive money from real U.S. persons in exchange for posting promotions and advertisements on the ORGANIZATION-controlled social media pages. Defendants and their co-conspirators typically charged certain U.S. merchants and U.S. social media sites between 25 and 50 U.S. dollars per post for promotional content on their popular false U.S. persona accounts, including Being Patriotic, Defend the 2nd, and Blacktivist.

All in violation of Title 18, United States Code, Section 1349.

COUNTS THREE THROUGH EIGHT

(Aggravated Identity Theft)

96. Paragraphs 1 through 7, 9 through 27, and 29 through 85, and 89 through 95 of this Indictment are re-alleged and incorporated by reference as if fully set forth herein.

97. On or about the dates specified below, in the District of Columbia and elsewhere,

Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, wire fraud and bank fraud, knowing that the means of identification belonged to another real person:

Count	Approximate Date	Initials of Identity Theft Victim	Means of Identification
3	June 16, 2016	T.B.	Social Security Number Date of Birth
4	July 21, 2016	A.R.	Social Security Number Date of Birth
5	July 27, 2016	T.C.	Social Security Number Date of Birth
6	August 2, 2016	T.W.	Social Security Number Date of Birth
7	January 18, 2017	V.S.	Social Security Number
8	May 19, 2017	J.W.	Home Address Date of Birth

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATION

98. Pursuant to Federal Rule of Criminal Procedure 32.2, notice is hereby given to Defendants that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2), and Title 28, United States Code, Section 2461(c), in the event of Defendants' convictions under Count Two of this Indictment. Upon conviction of the offense charged in Count Two, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, and GLEB IGOREVICH VASILCHENKO

shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense of conviction. Upon conviction of the offenses charged in Counts Three through Eight, Defendants INTERNET RESEARCH AGENCY LLC, DZHEYKHUN NASIMI OGLY ASLANOV, GLEB IGOREVICH VASILCHENKO, IRINA VIKTOROVNA KAVERZINA, and VLADIMIR VENKOV shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to the offense(s) of conviction. Notice is further given that, upon conviction, the United States intends to seek a judgment against each Defendant for a sum of money representing the property described in this paragraph, as applicable to each Defendant (to be offset by the forfeiture of any specific property).

Substitute Assets

99. If any of the property described above as being subject to forfeiture, as a result of any act or omission of any defendant --

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be subdivided without difficulty;

it is the intent of the United States of America, pursuant to Title 18, United States Code, Section 982(b) and Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853, to seek forfeiture of any other property of said Defendant.

(18 U.S.C. §§ 981(a)(1)(C) and 982; 28 U.S.C. § 2461(c))

Robert S. Mueller, III
Special Counsel
U.S. Department of Justice

A TRUE BILL:

_____
Foreperson

Date: February ___, 2018

Attachment B

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. 1:18-MJ-464
	)	
ELENA ALEKSEEVNA KHUSYAYNOVA,	)	18 U.S.C. § 371
	)	(Conspiracy)
Defendant.	)	
	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, David Holt, being duly sworn under oath, do hereby depose and state:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since August 2008. I am presently assigned to the Washington Field Office where I am responsible for investigations of foreign influence operations and other national security matters with a cyber nexus. I have also conducted national security investigations of foreign intelligence services and the targeting of critical U.S. infrastructure. As a Special Agent, I have received specialized training and instruction in the field of national security investigations and am authorized to investigate violation of laws of the United States and to execute warrants issued under the authority of the United States.

2. I am submitting this affidavit in support of a criminal complaint and arrest warrant charging the defendant, ELENA ALEKSEEVNA KHUSYAYNOVA, with Conspiracy to defraud the United States, in violation of Title 18, United States Code, Section 371.

3. The statements contained in this Affidavit are based on my experience and background as a criminal investigator, on information provided to me by other members of the

FBI and other law enforcement officers, court records and documents, business records, interviews, publicly available information, and my review of physical and documentary evidence. I have personally participated in the investigation of the offense set forth below and, as a result of my participation and review of evidence gathered in the case, I am familiar with the facts and circumstances of this investigation. Since this Affidavit is being submitted for the limited purpose of supporting a criminal complaint, I have not included every fact resulting from the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe the above-named defendant has violated Title 18, United States Code, Section 371, as set forth herein.

RELEVANT STATUTES AND BACKGROUND

4. Title 18, United States Code, Section 371, makes it a federal crime if "two or more persons conspire . . . to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act to effect the object of the conspiracy."

5. The United States of America, through its departments and agencies, regulates the activities of foreign individuals and entities in and affecting the United States in order to prevent, disclose, and counteract improper foreign influence on U.S. elections and on the U.S. political system. U.S. law bans foreign nationals from making certain expenditures or providing things of value for the purpose of influencing federal elections. U.S. law also bars agents of any foreign entity from engaging in political activities within the United States without first registering with the Attorney General. Various federal agencies, including the U.S. Department of Justice and the Federal Election Commission, are charged with enforcing these laws.

6. The U.S. Department of Justice administers the Foreign Agent Registration Act ("FARA"), Title 22, United States Code, Section 611 *et seq*. FARA establishes a registration, reporting, and disclosure regime for agents of foreign principals (which includes foreign non-government individuals and entities) so that the U.S. government and the people of the United States are informed of the source of information and the identity of persons attempting to influence U.S. public opinion, policy, and law. FARA requires, among other things, that persons subject to its requirements submit periodic registration statements containing truthful information about their activities and the income earned from them. Disclosure of the required information allows the federal government and the American people to evaluate the statements and activities of such persons in light of their function as foreign agents.

7. The Federal Election Commission is a federal agency that administers the Federal Election Campaign Act ("FECA"). Among other things, FECA prohibits foreign nationals from making "a contribution or donation of money or other thing of value, or to make an express or implied promise to make a contribution or donation, in connection with a Federal, State, or local election." 52 U.S.C. § 30121(a)(1)(A). FECA also requires that individuals or entities who make certain independent expenditures in federal elections report those expenditures to the Federal Election Commission. The reporting requirements permit the Federal Election Commission to fulfill its statutory duties of providing the American public with accurate data about the financial activities of individuals and entities supporting federal candidates, and enforcing FECA's limits and prohibitions, including the ban on foreign expenditures.

STATEMENT OF PROBABLE CAUSE

I. Project Lakhta and Efforts to Interfere with U.S. Political System

8. Since at least 2014, known and unknown individuals, operating as part of a broader Russian effort known as "Project Lakhta," have engaged in political and electoral interference operations targeting populations within the Russian Federation and in various other countries, including, but not limited to, the United States, members of the European Union, and Ukraine. Since at least May 2014, Project Lakhta's stated goal in the United States was to spread distrust towards candidates for political office and the political system in general.

9. Beginning in or around mid-2014 and continuing to the present, Project Lakhta obscured its conduct by operating through a number of Russian entities, including Internet Research Agency LLC ("IRA"), Internet Research LLC, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC (a/k/a "NevNov"), Economy Today LLC, National News LLC, Federal News Agency LLC (a/k/a "FAN"), and International News Agency LLC (a/k/a "MAN"). These entities employed hundreds of individuals in support of Project Lakhta's operations with an annual global budget of millions of U.S. dollars. Only some of Project Lakhta's activities were directed at the United States.

10. Concord Management and Consulting LLC and Concord Catering (collectively "Concord") are related Russian entities with various Russian government contracts. Concord was the primary source of funding for Project Lakhta operations. Concord controlled funding, recommended personnel, and oversaw Project Lakhta activities through reporting and interaction with the management of the various Project Lakhta entities.

11. Yevgeniy Viktorovich Prigozhin is a Russian oligarch who is closely identified with Russian President Vladimir Putin. Prigozhin began his career in the food and restaurant

business and is sometimes referred to as "Putin's Chef." Prigozhin controls Concord, which has been paid by the Russian government to feed school children and the military. Concord and Prigozhin spent significant funds to further the Project Lakhta operations.

12. On February 16, 2018, a grand jury in the District of Columbia returned an indictment charging thirteen Russian nationals and three Russian companies, including Prigozhin, the IRA, and Concord, with committing federal crimes while seeking to interfere with U.S. elections and political processes, including the 2016 presidential election. Indictment, *United States v. Internet Research Agency, et al.*, 1:18-CR-32 (DLF) (D.D.C. Feb. 16, 2018). Based on my training and experience, the factual allegations in that indictment provide further probable cause to believe that the above-named defendant has violated Title 18, United States Code, Section 371. That indictment is attached hereto and incorporated by reference.

II. ELENA ALEKSEEVNA KHUSYAYNOVA

13. Defendant ELENA ALEKSEEVNA KHUSYAYNOVA is a resident of St. Petersburg, Russia. Since at least 2014, the defendant has been employed by various entities within Project Lakhta, including the IRA, GlavSet, and the Federal News Agency. Since approximately April 2014, she has acted as the Chief Accountant in Project Lakhta's finance department. As detailed further herein, KHUSYAYNOVA oversaw all aspects of Project Lakhta financing. She managed the budgeting and payment of expenses associated with social media operations, web content, advertising campaigns, infrastructure, salaries, travel, office rent, furniture, and supplies, and the registration of legal entities used to further Project Lakhta activities.

14. There is probable cause to believe that, from at least 2014 to the present, KHUSYAYNOVA conspired with persons known and unknown to defraud the United States by

impairing, obstructing, and defeating the lawful functions of the U.S. Department of Justice and Federal Election Commission in administering federal requirements for disclosure of foreign involvement in certain domestic activities, in violation of Title 18, United States Code, Section 371. Among the persons with whom KHUSYAYNOVA conspired are known and unknown employees and associates of Concord and Project Lakhta entities. The Conspiracy had as its objects impairing, obstructing, and defeating the lawful governmental functions of the United States by dishonest means in order to enable Project Lakhta actors to interfere with U.S. political and electoral processes, including the 2018 U.S. elections.

III. Manner and Means of the Conspiracy

15. The Conspiracy has a strategic goal, which continues to this day, to sow division and discord in the U.S. political system, including by creating social and political polarization, undermining faith in democratic institutions, and influencing U.S. elections, including the upcoming 2018 midterm election. The Conspiracy has sought to conduct what it called internally "information warfare against the United States of America"[1] through fictitious U.S. personas on social media platforms and other Internet-based media.

16. Members of the Conspiracy, posing as U.S. persons, operated fictitious social media personas, pages, and groups designed to attract U.S. audiences and to address divisive U.S. political and social issues or advocate for the election or electoral defeat of particular candidates. These personas, groups, and pages falsely claimed to be controlled by U.S. activists when, in fact, they were controlled by members of the Conspiracy. Over time, these accounts

[1] Throughout this affidavit, statements by members of the Conspiracy are translated or quoted exactly as they appear in the source text, including any spelling, grammatical, or factual errors.

became the Conspiracy's primary means to reach significant numbers of Americans for purposes of interfering with the U.S. political system.

17. Members of the Conspiracy made various expenditures to carry out those activities, including buying social media analytics products and services, as well as advertisements on social media, in some instances through third-party intermediaries. Members of the Conspiracy also staged and promoted political rallies inside the United States, and while posing as U.S. grassroots entities and U.S. persons, and without revealing their Russian identities and Project Lakhta affiliation, promoted or disparaged candidates and campaigns and organized rallies and counter-protests around particular socially divisive issues.

A. KHUSYAYNOVA's Role in Project Lakhta

18. To effectively manage such a large-scale operation, the Conspiracy was headed by a management group and organized into departments, including a design and graphics department, an analysts department, a search-engine optimization ("SEO") department, an information-technology ("IT") department, and a finance department.

19. Between April 2014 and the present, KHUSYAYNOVA, as the Chief Accountant in Project Lakhta's finance department, managed the financing of substantially all aspects of Project operations, which included media and influence activities directed at the United States, the European Union, and Ukraine, as well as the Russian Federation. In that role, she oversaw the budgets of various Project Lakhta entities, including the IRA, MediaSintez LLC, GlavSet LLC, MixInfo LLC, Azimut LLC, NovInfo LLC, Nevskiy News LLC, Economy Today LLC, National News LLC, Federal News Agency LLC, and International News Agency LLC. KHUSYAYNOVA participated in the preparation and submission of hundreds of financial vouchers, budgets, and payment requests for the various Project Lakhta entities, often putting all

company names on the same paperwork and identifying them as part of Project Lakhta. KHUSYAYNOVA maintained Project Lakhta monthly budgets and submitted associated requests for funds to the central finance offices of Concord, which were responsible for disbursing money to Project Lakhta entities.

20. To conceal the nature of Project Lakhta activities, since at least January 2016 the Conspiracy labeled the funds paid by Concord to Project Lakhta as payments related to software support and development. Moreover, since at least January 2016, Concord distributed funds to Project Lakhta through approximately fourteen bank accounts held in the names of Concord affiliates, including Glavnaya Liniya LLC, Merkuriy LLC, Obshchepit LLC, Potentsial LLC, RSP LLC, ASP LLC, MTTs LLC, Kompleksservis LLC, SPb Kulinariya LLC, Almira LLC, Pishchevik LLC, Galant LLC, Rayteks LLC, and Standart LLC. The Conspiracy described payments from these Concord entities to Project Lakhta as being in furtherance of a series of vague contracts that obscured or falsely stated the true intended use of the funds. At various times, such payments were described as being for "providing services to collect and process materials," "providing services in developing an exporting module for results," and "providing services for developing a statistical processing module" (preliminary translation of Russian text).

21. At the same time, KHUSYAYNOVA kept detailed financial documents that tracked itemized Project Lakhta expenses, including efforts to promote the illegal objects of the Conspiracy in the United States. For example, the financial documents included itemized budgets that included IT expenses, social media marketing expenses, and expenses for activities in the United States and the European Union, including expenditures for activists and advertisements on social media platforms. KHUSYAYNOVA also issued and kept track of requests to Concord for funds to cover those expenses. Between at least January 2016 and July

2018, these documents were updated and provided to Concord on approximately a monthly basis. The following illustrative examples demonstrate KHUSYAYNOVA's meticulous record-keeping and management of Project Lakhta funds:

a. In or around January 2017, KHUSYAYNOVA compiled and submitted to Concord a planned itemized budget for February 2017 for Project Lakhta totaling approximately 60 million Russian rubles (approximately $1 million U.S. dollars).[2] This budget also contained a backward-looking accounting of actual expenses for calendar year 2016, which totaled approximately 720 million Russian rubles (approximately $12 million U.S. dollars). In addition to administrative expenses, such as office rent, utility payments, and garbage disposal, the budget identified IT expenses, such as "registration of domain names" and the purchase of "proxy servers;" and social media marketing expenses, such as expenses for "purchasing posts for social networks," "[a]dvertisement on Facebook," "[a]dvertisement on VKontakte," "[a]dvertisement on Instagram," "[p]romoting news postings on social networks," and social media optimization software (such as Twidium and Novapress) (preliminary translation of Russian text). The budgets also contained a section on "USA, EU" activities, which included itemized expenditures for "Instagram," "Facebook advertisement," and "Activists" (preliminary translation of Russian text). Moreover, the budgets identified expenditures for "bloggers" and "developing accounts" on Twitter, and for the development and promotion of online videos (preliminary translation of Russian text).

[2] For the purpose of this affidavit, the approximate U.S. dollar values are based on an approximate currency conversion rate of 60 Russian rubles to 1 U.S. dollar.

b. To cover the February 2017 expenses, KHUSYAYNOVA requested funds from Concord in two parts. KHUSYAYNOVA requested approximately 25 million Russian rubles on or about February 16, 2017, and approximately 35 million Russian rubles on March 6, 2017.

c. In or around January 2018, KHUSYAYNOVA compiled and submitted to Concord a planned itemized budget for February 2018 totaling approximately 100 million Russian rubles (approximately $1.7 million U.S. dollars). This budget also contained a backward-looking accounting of actual expenses for calendar year 2017, which totaled approximately 733 million Russian rubles (approximately $12.2 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.

d. To cover substantial portions of the February 2018 expenses, KHUSYAYNOVA requested funds from Concord in at least six parts. KHUSYAYNOVA requested approximately 20 million Russian rubles on or about February 7, 2018, approximately 10 million Russian rubles on or about February 7, 2018, approximately 15 million Russian rubles on or about February 16, 2018, approximately 3 million Russian rubles on or about February 21, 2018, approximately 5 million Russian rubles on or about February 28, 2018, and approximately 31 million Russian rubles on or about March 6, 2018.

e. In or around March 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for April 2018 for Project Lakhta that exceeded 107 million

Russian rubles (over $1.75 million U.S. dollars). The budget contained, among other things, all of the itemized expenditures identified in subparagraph a, above.

f. To cover substantial portions of the April 2018 expenses, KHUSYAYNOVA requested funds from Concord in at least two parts. KHUSYAYNOVA requested approximately 32 million Russian rubles on or about April 6, 2018, and approximately 21 million Russian rubles on or about May 8, 2018.

g. In or around April 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for May 2018 for Project Lakhta that exceeded 111 million Russian rubles (over $1.86 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.

h. To cover substantial portions of the May 2018 expenses, she requested funds from Concord in at least three parts. She requested approximately 5 million Russian rubles on or about May 8, 2018, approximately 31 million Russian rubles on or about May 10, 2018, and approximately 35 million Russian rubles on or about June 9, 2018.

i. On or about June 1, 2018, KHUSYAYNOVA compiled and submitted to Concord a monthly budget for June 2018 for Project Lakhta that exceeded 114 million Russian rubles (over $1.9 million U.S. dollars). The budget contained, among other things, all of the categories of itemized expenditures identified in subparagraph a, above.

j. To cover substantial portions of the June 2018 expenses, KHUSYAYNOVA requested funds from Concord in three parts. KHUSYAYNOVA requested

approximately 29 million Russian rubles on or about June 1, 2018, approximately 29 million Russian rubles on or about June 4, 2018, and approximately 36 million Russian rubles on July 10, 2018.

22. Between in or around January 2016 and in or around June 2018, Project Lakhta's proposed operating budget totaled more than 2 billion Russian rubles (over $35 million U.S. dollars). Just between in or around January 2018 and in or around June 2018, Project Lakhta's proposed operating budget totaled more than 650 million Russian rubles (over $10 million U.S. dollars).

23. KHUSYAYNOVA also monitored the Project Lakhta budget to ensure that expected payments from Concord were received. For example, on or about November 15, 2017, KHUSYAYNOVA contacted Concord to inform them that she had not received a payment from Almira LLC for certain Project Lakhta companies, and that she was urgently waiting for the payment. Similarly, on or about April 11, 2018, KHUSYAYNOVA confirmed to Concord that she had received payment for a portion of the March 2018 budget for Project Lakhta but was waiting for the remaining payment. On or about April 12, 2018, a Concord employee informed KHUSYAYNOVA that the remaining payment would be forthcoming.

24. Starting at least in or around 2015, the Conspiracy began to purchase advertisements on online social media sites to promote events and social media groups it controlled. These expenditures were included in the budgets that KHUSYAYNOVA submitted to Concord. For example, between approximately January 2018 and June 2018, KHUSYAYNOVA compiled and submitted to Concord expenditures of over 3.7 million Russian rubles (over $60,000 U.S. dollars) for advertisements on Facebook and over 385,000 Russian rubles (over $6,000 U.S. dollars) for advertisements on Instagram. Over that same timeframe,

the budget also included expenditures of over 1,100,000 Russian rubles (over $18,000 U.S. dollars) for "bloggers" and "[d]eveloping accounts" on Twitter (preliminary translation of Russian text). Additionally, the budget included expenditures for "[r]enting software for social networks," including payments for services to manage Twitter posts and generate additional followers (preliminary translation of Russian text).

B. Targeted Messaging to Sow Social and Political Discord

25. Between in or around December 2016 and in or around May 2018, as part of the Conspiracy's effort to sow discord in the U.S. political system, members of the Conspiracy used social media and other internet platforms to inflame passions on a wide variety of topics, including immigration, gun control and the Second Amendment, the Confederate flag, race relations, LGBT issues, the Women's March, and the NFL national anthem debate. Members of the Conspiracy took advantage of specific events in the United States to anchor their themes, including the shootings of church members in Charleston, South Carolina, and concert attendees in Las Vegas, Nevada; the Charlottesville "Unite the Right" rally and associated violence; police shootings of African-American men; as well as the personnel and policy decisions of the current U.S. administration.

26. Members of the Conspiracy were directed to create "political intensity through supporting radical groups, users dissatisfied with [the] social and economic situation and oppositional social movements." The Conspiracy also sought, in the words of one member of the Conspiracy, to "effectively aggravate the conflict between minorities and the rest of the population."

27. The Conspirators' activities did not exclusively adopt one ideological viewpoint; they wrote on topics from varied and sometimes opposing perspectives. Members of the

Conspiracy also developed strategies and guidance to target audiences with conservative and liberal viewpoints, as well as particular social groups. For example, a member of the Conspiracy advised in or around October 2017 that "if you write posts in a liberal group, . . . you must not use Breitbart titles. On the contrary, if you write posts in a conservative group, do not use Washington Post or BuzzFeed's titles." Using the example of individuals of color who are also members of the lesbian, gay, bisexual, and transgender ("LGBT") community, the member of the Conspiracy offered the following guidance on how to target the group:

> Colored LGBT are less sophisticated than white; therefore, complicated phrases and messages do not work. Be careful dealing with racial content. Just like ordinary Blacks, Latinos, and Native Americans, colored LGBT people are very sensitive towards *#whiteprivilege* and they react to posts and pictures that favor white people. . . . Unlike with conservatives, infographics works well among LGBT and their liberal allies, and it does work very well. However, the content must be simple to understand consisting of short text in large font and a colorful picture. (Preliminary translation of Russian text.)

Members of the Conspiracy also sought to target the timing of their posts to attract the widest possible viewership. The same member of the Conspiracy referenced above offered the following guidance on how to overcome the time difference between Russia and the United States:

> Posting can be problematic due to time difference, but if you make your re-posts in the morning St. Petersburg time, it works well with liberals – LGBT groups are often active at night. Also, the conservative can view your re-post when they wake up in the morning if you post it before you leave in the evening St. Petersburg time. (Preliminary translation of Russian text.)

28. Members of the Conspiracy also developed detailed analysis of timely news articles and guidance for how to describe the articles in social media posts in order to promote the objectives of the Conspiracy. For example, in or around early August 2017, one or more members of the Conspiracy working under the guise of the Facebook group "Secured Borders"

analyzed a large quantity of U.S. news articles, summarized the substance of the articles, and outlined ways for the conspiracy to promote them. Specifically, one or more members of the Conspiracy described each article and categorized its theme, provided a strategic response with a particular focus on how to target U.S. audiences, and then noted approval to use the strategic response. The strategic response was referred to as "Tasking Specifics," which appeared to include an assignment to certain members of the Conspiracy to disseminate the message on social media platforms.

a. Citing an online news article titled "McCain Says Thinking a Wall Will Stop Illegal Immigration is 'Crazy,'" from on or about August 5, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> Brand McCain as an old geezer who has lost it and who long ago belonged in a home for the elderly. Emphasize that John McCain's pathological hatred towards Donald Trump and towards all his initiatives crosses all reasonable borders and limits. State that dishonorable scoundrels, such as McCain, immediately aim to destroy all the conservative voters' hopes as soon as Trump tries to fulfill his election promises and tries to protect the American interests. (Preliminary translation of Russian text.)

b. Citing an online news article titled "Paul Ryan Opposes Trump's Immigration Cuts, Wants Struggling American Workers to Stay Poor," from on or about August 5, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> Brand Paul Ryan a complete and absolute nobody incapable of any decisiveness. Emphasize that while serving as Speaker, this two-faced loudmouth has not accomplished anything good for America or for American citizens. State that the only way to get rid of Ryan from Congress, provided he wins in the 2018 primaries, is to vote in favor of Randy Brice, an American veteran and an iron worker and a Democrat. (Preliminary translation of Russian text.)

c. Citing an online news article titled "11 California Counties Might have More Registered Voters Than Eligible," from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> In the California voter registration rolls, there are more registrants than there are residents. This is the time for American conservatives to sound the alarm before the elections turn the Constitution into a mockery and a celebration of lawlessness. Emphasize that previous falsifications during the U.S. elections used to be perceived as a myth; today they became a reality with a threatening force and are perceived accordingly. Emphasize that all illegal voters must be kept away from the ballot boxes at distances "beyond artillery firing range." There is an urgent need to introduce voter IDs for all the states, above all in the blue (liberal and undecided) states. Remind that the majority of the "blue states" have no VOTER IDs, which suggests that large-scale falsifications are bound to be happening there. State in the end that the Democrats in the coming election will surely attempt to falsify the results. (Preliminary translation of Russian text.)

d. Citing an online news article titled "Savage: Civil War if Trump Taken Down," from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> Forcefully support Michael Savage's point of view with competence and honesty. Savage made it clear that any attempt to remove Trump is a direct path to a civil war in the United States. Name those who oppose the president and those who impede his efforts to implement his pre-election promises. Focus on the fact that the Anti-Trump Republicans: a) drag their feet with regard to financing the construction of the border wall; b) are not lowering taxes; c) slander Trump and harm his reputation (bring up McCain); d) do not want to cancel Obamacare; e) are not in a hurry to adopt laws that oppose the refugees coming from Middle Eastern countries entering this country. Summarize that in case Republicans will not stop acting as traitors, they will bring upon themselves forces of civil retribution during the 2018 elections. (Preliminary translation of Russian text.)

e. Citing an online news article titled "Trump: No Welfare To Migrants For Grants For First 5 Years" from on or about August 6, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> Fully support Donald Trump and express the hope that this time around Congress will be forced to act as the president says it should. Emphasize that if Congress continues to act like the Colonial British government did before the War of Independence, this will call for another revolution. Summarize that Trump once again proved that he stands for protecting the interests of the United States of America. (Preliminary translation of Russian text.)

f. Citing an online news article titled "The 8 Dirtiest Scandals of Robert Mueller No One Is Talking About," from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> Special prosecutor Mueller is a puppet of the establishment. List scandals that took place when Mueller headed the FBI. Direct attention to the listed examples. State the following: It is a fact that the Special Prosecutor who leads the investigation against Trump represents the establishment: a politician with proven connections to the U.S. Democratic Party who says things that should either remove him from his position or disband the entire investigation commission. Summarize with a statement that Mueller is a very dependent and highly politicized figure; therefore, there will be no honest and open results from the investigation. Emphasize that the work of this commission is damaging to the country and is aimed to declare impeachment of Trump. Emphasize that it cannot be allowed, no matter what. (Preliminary translation of Russian text.)

g. Citing an online news article titled "CNN's Pro-Jeb! Republican: Trump White House Like a 'Brothel,'" from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> CNN commentator "RINO" likened the Trump administration to a "brothel." Mass News Media Criticism! Accuse CNN of yet another lie. State that during past elections, namely, this mainstream media, which supported Hillary Clinton's candidacy

> for U. S. President almost 100%, disseminated fake news, insulting statements, and lies about Donald Trump and his supporters. This continues now. This is precisely why such news sources as the New York Times, Washington Post, CNN, CBS, Time, and Huffington Post must not be taken seriously, for they are the main propaganda channels that are screwing with the heads of American citizens. Remind readers that each of the above-mentioned media resources supported Hillary Clinton and received funds from her election fund. They produced fake social study research results at polls predicting a Clinton win with a 10-15% lead over Trump and tried hard to insult and discredit Trump. Summarize with a statement that CNN long ago lost its reputation as a trusted source and that its reputation is still declining. (Preliminary translation of Russian text.)

h. Citing an online news article titled "Pro-Amnesty Sen. Marco Rubio: Trump's Immigration Bill Will Not Pass the Senate," from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> VERY IMPORTANT! We expose Marco Rubio as a fake conservative who is a traitor to Republican values and who in his soul despises the American Constitution and civil liberties. Remind that Rubio is the protégé of the preposterous Jeb Bush, who is a disgrace to the conservative movement. State that victims of violence committed by illegals and the relatives of the victims hate Marco Rubio completely and wholeheartedly. In other words, Rubio is a liberal who penetrated the Republican Party for the purpose undermining it from the inside. Summarize in a statement that voting for Rubio during the Senate elections is practically the same as voting for Hillary Clinton. (Preliminary translation of Russian text.)

i. Citing an online news article titled "Sanctuary City Objects to Arrest of Accused Illegal Alien Child Molester," from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> Characterize the position of Californian sanctuary cities along with the position of the entire California administration as absolutely and completely treacherous and disgusting. Stress that protecting an illegal rapist who raped an American child is the peak of

> wickedness and hypocrisy. Summarize in a statement that "sanctuary city" politicians should surrender their American citizenship, for they behave as true enemies of the United States of America. (Preliminary translation of Russian text.)

j. Citing an online news article titled "Maryland City Mulling Over Idea to Let Illegal Immigrants Vote" from on or about August 7, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> Stress that the leadership in sanctuary cities has lost all connection with reality and is trying to provide criminals who illegally crossed the U.S. borders with voting rights that are available only to the citizens of the United States. Summarize in a statement that the leaders of sanctuary cities are people without conscience and without any respect for the American Constitution. (Preliminary translation of Russian text.)

k. Citing an online news article titled "Dobbs Slams McConnell, Says It's Time to 'Ditch Mitch,'" from on or about August 8, 2017, a member of the Conspiracy directed that the article be messaged in the following way:

> It's time for Mitch McConnell (leader of the Senate Republicans) to retire. Show solid support for the news anchor. Emphasize that McConnell exhausted himself as a politician. State that Mitch McConnell, like many other Republican senators, behaves as a renegade and a vile liberal. McConnell has done nothing to fulfill Trump's and other Republicans' election promises. Remind that McConnell is a friend of Joe Biden, who has no political principles. Emphasize that boycotting the conservative agenda is the most inadequate and treacherous behavior possible in the given situation. Summarize in a statement that people did not vote for the Republicans in 2014 and in 2016 so that today they would do the same things that Democrats usually busy themselves with. (Preliminary translation of Russian text.)

C. Use of Specific U.S. Fake Personas

29. Since at least in or around 2015, the Conspiracy used social media platforms to create thousands of social media and email accounts that appeared to be operated by U.S. persons and used them to create and amplify divisive social and political content targeting a U.S.

audience. These accounts were also used to advocate for the election or electoral defeat of particular candidates in the 2016 and 2018 U.S. elections, to post derogatory information about a number of candidates, and, on occasion, to promote political donations against particular candidates.

30. In or around May 2015, the Conspiracy created a Facebook account registered under the false U.S. persona "Helen Christopherson." On her Facebook page, "Helen Christopherson" purported to be a resident of New York City and identified her hometown as Charleston, South Carolina. Between in or around March 2016 and in or around July 2017, while concealing its true identity, location, and purpose, the Conspiracy used the false U.S. persona "Helen Christopherson" to contact individuals and groups in the United States to promote protests, rallies, and marches, including by funding advertising, flyers, and rally supplies. Specific examples of this account's activities, as well as the activities of other accounts described in this subsection, are contained in the Overt Acts section below.

31. In or around June 2015, the Conspiracy created a Facebook account registered under the false U.S. persona "Bertha Malone." On her Facebook page, "Bertha Malone" purported to be a resident of New York City, identified her hometown as New York City, and stated that she had attended a university in New York City. In or around January 2016, the Conspiracy used the "Bertha Malone" Facebook account to create a Facebook page for a group called "Stop A.I.," which is an abbreviation for "Stop All Invaders." Between in or around December 2016 and in or around August 2017, while concealing its true identity, location, and purpose, the Conspiracy used the "Bertha Malone" Facebook account to create over 400 posts on Facebook containing inflammatory political and social content focused primarily on immigration and Islam. Between on or about July 17, 2017, and on or about July 23, 2017, alone, the content

on the "Stop A.I." Facebook page reached approximately 1,385,795 individuals and approximately 130,851 individuals purposefully engaged with the Facebook page. In total, by on or about July 23, 2017, the Facebook page received approximately 194,221 total page likes.

32. The Conspiracy also used the "Bertha Malone" Facebook account, while concealing its true identity, location, and purpose, to solicit at least one person presumed to be located in the United States to assist with Project Lakhta's social media activities in or around July 2017, such as by posting and managing content on the "Stop A.I." Facebook page. Moreover, the Conspiracy used the "Stop A.I." Facebook page to accept money from individuals to post ads and other content on the Facebook group's page.

33. In or around June 2016, the Conspiracy created a Twitter account that went by various names, including "@UsaUsafortrump," "@USAForDTrump," "@TrumpWithUSA," "@TrumpMov," "@POTUSADJT," "@imdeplorable201," "@swampdrainer659," "@maga2017trump," and "@TXCowboysRawk." Most recently, the Twitter account went by the name "@CovfefeNationUS." Between in or around November 2017 and in or around December 2017, while concealing its true identity, location, and purpose, the Conspiracy used the Twitter account "@CovfefeNationUS" to post or repost over 23,000 messages.

34. In or around September 2016, the Conspiracy created a Facebook account registered under the false U.S. persona "Rachell Edison" and an associated Facebook page for a group called "Defend the 2nd." Between in or around December 2016 and in or around May 2017, while concealing its true identity, location, and purpose, the Conspiracy used the "Rachell Edison" Facebook account to create over 700 posts on Facebook containing inflammatory political and social content primarily focused on gun control and the Second Amendment.

35. In or around March 2017, the Conspiracy created the Twitter account "@wokeluisa" registered under the false U.S. persona "Luisa Haynes." Between in or around March 2017 and in or around March 2018, while concealing its true identity, location, and purpose, the Conspiracy used the Twitter account "@wokeluisa" to post over 2,000 Tweets on topics such as the 2018 midterm election, the disenfranchisement of African-American voters, the NFL national anthem debate, the current U.S. administration, and the U.S. President's family. By in or around March 2018, the Twitter account amassed over 55,000 followers.

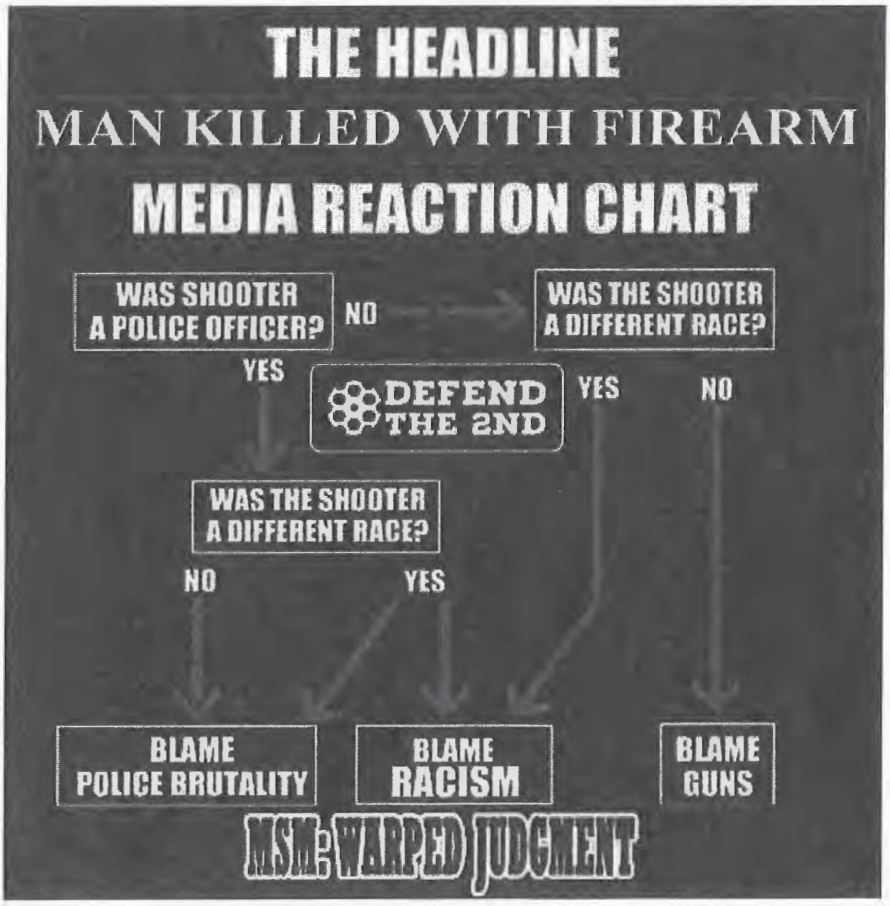
36. In or around September 2017, the Conspiracy created several Twitter accounts that it used to create and amplify content that would resonate with either liberal or conservative audiences. For example, on or about September 4, 2017, one or more members of the Conspiracy created the Twitter accounts "@JohnCopper16," "@Amconvoice," and "@TheTrainGuy13." Members of the Conspiracy used these accounts to post messages on controversial social and political topics using a perspective that they believed would resonate with a conservative audience in the United States. Similarly, one or more members of the Conspiracy created the Twitter account "@KaniJJackson" on or about September 5, 2017, and the Twitter account "@JemiSHaaaZzz" on or about September 6, 2017, and used these accounts to post on many of the same controversial social and political topics from a perspective that they believed would resonate with a liberal audience in the United States. Between in or around September 2017 and in or around May 2018, while concealing its true identity, location, and purpose, the Conspiracy used these Twitter accounts to post thousands of Tweets, on topics including, but not limited to, the 2018 midterm election, gun rights, the net neutrality debate, negotiations with North Korea, and the personnel and policy decisions of the current U.S. administration. In some cases, these accounts attracted significant numbers of followers. For

example, by in or around May 2018, the Twitter account "@KaniJJackson" had amassed over 33,000 followers.

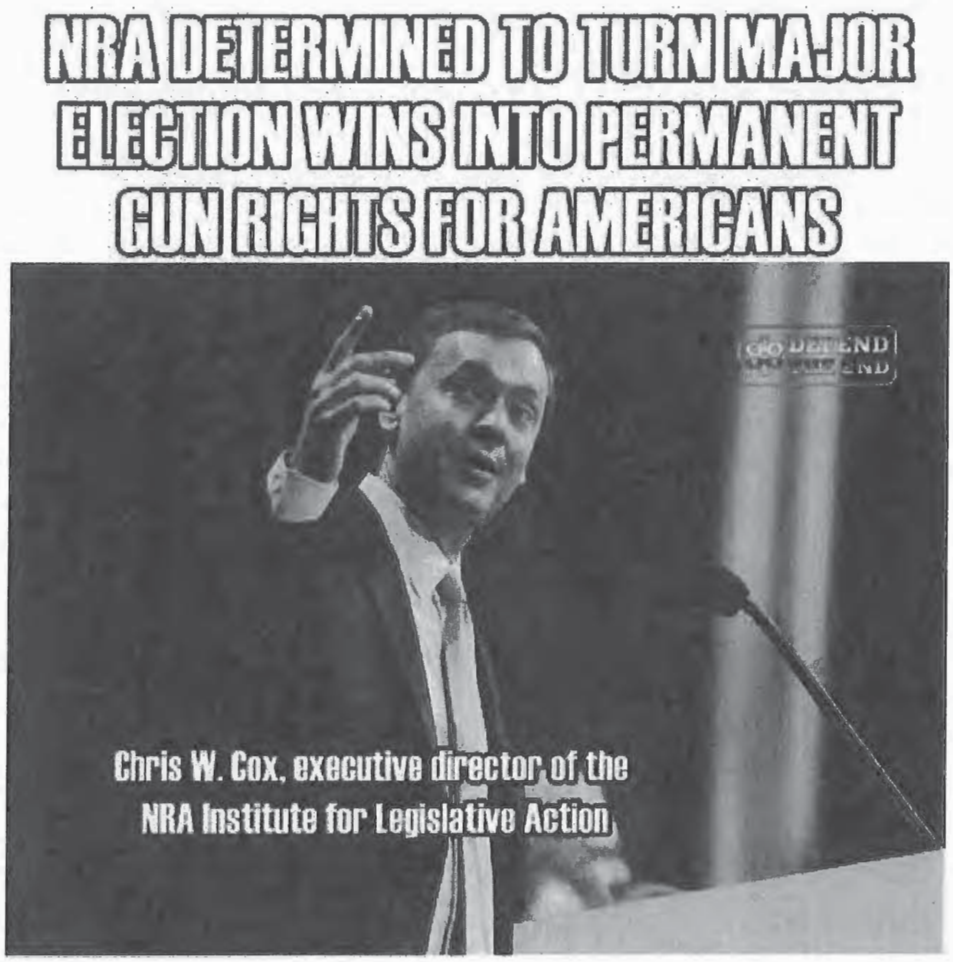
IV. Overt Acts

37. Between in or around December 2016 and in or around May 2018, in the Eastern District of Virginia and elsewhere, while concealing its true identity, location, and purpose, the Conspiracy committed the following overt acts involving U.S. social media platforms in furtherance of the Conspiracy and to effect its illegal objects:

38. On or about December 5, 2016, a member of the Conspiracy used the "Rachell Edison" Facebook account to post the following image on Facebook, accompanied by the comment "Whatever happens, blacks are innocent. Whatever happens, it's all guns and cops. Whatever happens, it's all racists and homophobes. MainStream Media...":



39. On or about April 28, 2017, a member of the Conspiracy used the "Rachell Edison" Facebook account to post the following image on Facebook:



The image was accompanied by the following comment advocating political activities:

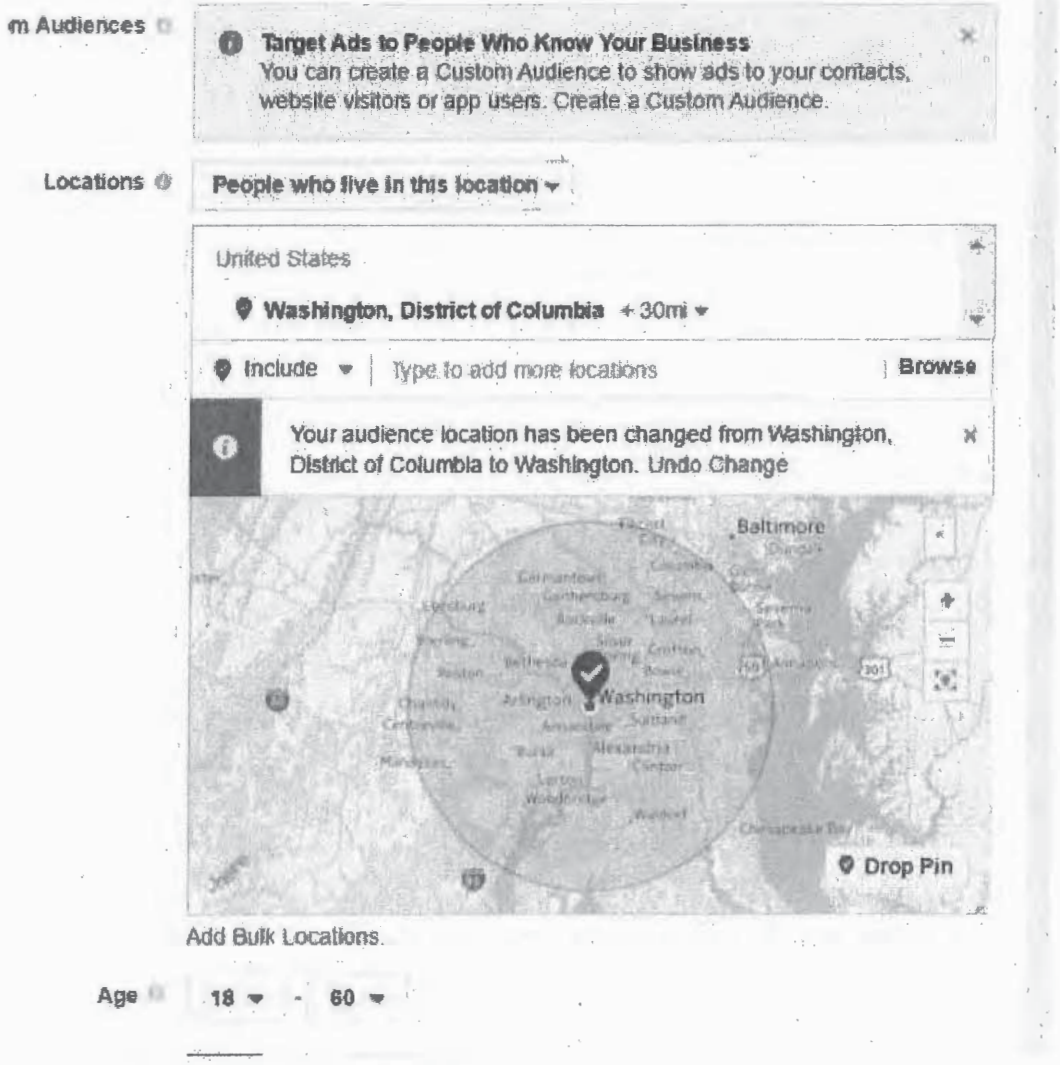
> Gun rights backers need to make sure that election victories translate into action on Capitol Hill and expanded support in the states, the National Rifle Association's legislative chief said Thursday, a day ahead of President Trump's speech at the NRA's annual convention. And he is absolutely right. Now it is the time for us to demand our rights. With current, administration it is possible to defend our right to bear arms. I think next 4 years will be great for all Americans, and for gun lovers especially! But we must stand for our rights! And in the end, I believe, we will win!

40. On or about July 1, 2017, a member of the Conspiracy used the "Helen Christopherson" Facebook account to contact the Facebook accounts for three real U.S. organizations (hereinafter U.S. Organizations 1, 2, and 3) to inquire about collaborating with

these groups on an anti-President Trump "flash mob" at the White House, which was already being organized by the groups for July 4, 2017. The organizers had described the event as "inviting resistance activists, show tune lovers, and karaoke fans to come join us on Independence Day, sing a song of freedom, and demand Trump's impeachment."

41. On or about July 2, 2017, a member of the Conspiracy used the "Helen Christopherson" Facebook account to contact U.S. Organization 1 and a U.S. person affiliated with the organization, U.S. Person 1, and inform them that "I got some cash on my Facebook ad account so we can promote it for 2 days," adding "I got like $80 on my ad account so we can reach like 10000 people in DC or so. That would be Massive!"

42. On or about July 2, 2017, a member of the Conspiracy used the "Helen Christopherson" Facebook account to send U.S. Organization 1 a proposal to purchase advertising targeting individuals within 30 miles of Washington, DC, including significant portions of the Eastern District of Virginia, as depicted below:



The proposed advertisements had an estimated reach of 29,000 to 58,000 individuals. Subsequently, U.S. Organization 1 agreed to make the "Helen Christopherson" Facebook account a co-organizer of the event on Facebook.

43. On or about July 4, 2017, a member of the Conspiracy used the "Bertha Malone" Facebook account to engage in the following conversation with U.S. Person 2 about U.S. Person 2 assisting with posting content and managing the "Stop A.I." Facebook page, which members of the Conspiracy controlled:

Malone: Hey girl! How u doin? still got free time on ya hands? So...remember u wanted to help me with that page i'm workng on? It's a little bit unorthodox, but nwm that. Content is not of my choosing. So what tell ya? Help a sister out?
U.S. Person 2: Hi! Let me think bout 4 a sec. what's the name of the page again?
Malone: https://www.facebook.com/StopAllInvaders/
...
Malone: Nothin muh, [U.S. Person 2]. Just general scannin, answer subcribers now and then and mb post something (i'll be sending content to u directly)
Malone: nwm the posts lol
Malone: just business
Malone: makes ratinging for clients, that's what i know.
Malone: ratings*
Malone: u know how rednecks are
Malone: so here's the deal. I give u admin rights, u check the page when i'm not around and basically do some stuff i tell u to :D
...
U.S. Person 2: You know I can't let my sis down
U.S. Person 2: so I'm in
...
U.S. Person 2: but please tell me I'm not going to jail for this
...
Malone: jeez why would u
Malone: just page lol
Malone: i'll vouch fou 4 mb u get some money out that even
...
U.S. Person 2: i trust you

44. On or about July 28, 2017, a member of the Conspiracy used the "Bertha Malone" Facebook account to post the following image on Facebook:

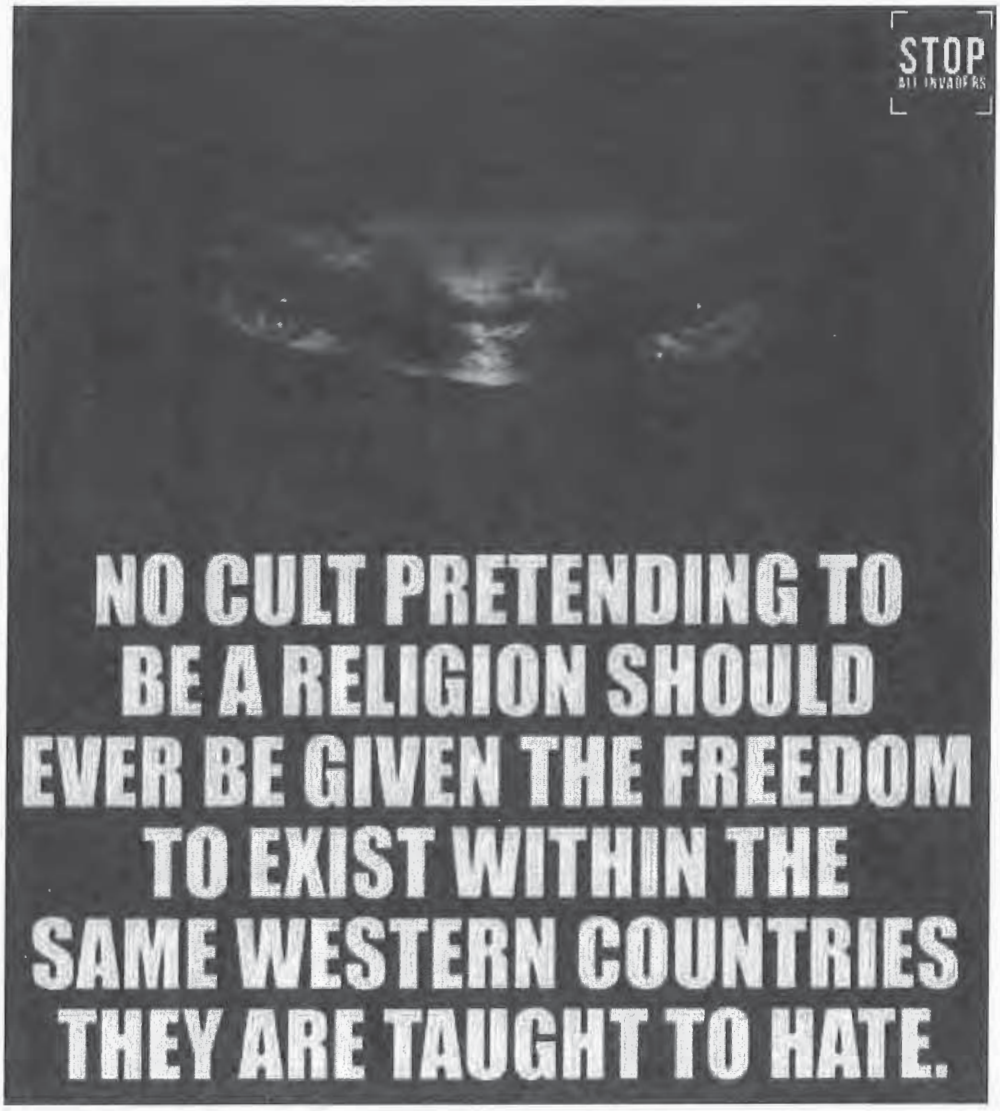
The image was accompanied by the following comment:

> Instead this stupid witch hunt on Trump, media should investigate this traitor and his plane to Islamize our country. If you are true enemy of America, take a good look at Barack Hussein Obama and Muslim government officials appointed by him.

45. On or about July 31, 2017, a member of the Conspiracy used the "Bertha Malone" Facebook account to post the following image on Facebook, with the comment "Stop separating families! Deport them all, including their anchor babies! And spend saved money on Americans who really need it, for example our homeless Vets":

46. On or about July 31, 2017, a member of the Conspiracy used the "Bertha Malone" Facebook account to post the following image on Facebook, with the comment "Feel the difference!":

47. On or about August 1, 2017, a member of the Conspiracy used the "Bertha Malone" Facebook account to post the following image on Facebook, with the comment "Damn right! And we all know which cult we need to kick out of America…":



The post generated approximately 104 comments between on or around August 1, 2017, and on or around August 2, 2017.

48. On or about December 10, 2017, a member of the Conspiracy used the Twitter account "@CovfefeNationUS" to repost a Tweet encouraging readers to donate to a political action committee aiming to unseat Democratic Senators and Representatives in the 2018 midterm election:

> Tell us who you want to defeat! Donate $1.00 to defeat @daveloebsack Donate $2.00 to defeat @SenatorBaldwin Donate $3.00 to defeat @clairecmc Donate $4.00 to defeat @NancyPelosi Donate $5.00 to defeat @RepMaxineWaters Donate $6.00 to defeat @SenWarren

The Tweet included a link to the donation website of a political action committee.

49. On or about December 12, 2017, a member of the Conspiracy used the Twitter account "@KaniJJackson" to post a Tweet about the 2017 special election in Alabama:

> Dear Alabama, You have a choice today. Doug Jones put the KKK in prison for murdering 4 young black girls. Roy Moore wants to sleep with your teenage daughters. This isn't hard. #AlabamaSenate

50. On or about December 12, 2017, a member of the Conspiracy used the Twitter account "@JohnCopper16" to post a Tweet about the 2017 special election in Alabama:

> People living in Alabama have different values than people living in NYC. They will vote for someone who represents them, for someone who they can trust. Not you. Dear Alabama, vote for Roy Moore.

51. On or about December 16, 2017, a member of the Conspiracy used the Twitter account "@KaniJJackson" to post a Tweet about the Special Counsel's Office's investigation:

> If Trump fires Robert Mueller, we have to take to the streets in protest. Our democracy is at stake.

52. On or about December 17, 2017, a member of the Conspiracy used the Twitter account "@Amconvoice" to repost a Tweet about the Special Counsel's Office's investigation:

> Liberals : If Trump fire/removes Mueller, we will take to the streets/protest. (DNC must have sent that talking point out today. Everyone using same line) Why would Trump need to remove/fire Mueller. Mueller is doing fine job destroying himself. Keep the implosion coming Mueller.

53. On or about January 19, 2018, a member of the Conspiracy used the Twitter account "@KaniJJackson" to post a Tweet about the government shutdown of 2018:

> Who ended DACA? Who put off funding CHIP for 4 months? Who rejected a deal to restore DACA? It's not #SchumerShutdown. It's #GOPShutdown.

54. On or about January 20, 2018, a member of the Conspiracy used the Twitter account "@JohnCopper16" to repost a Tweet about the government shutdown of 2018:

> Anyone who believes that President Trump is responsible for the #shutdown2018 is either an outright liar or horribly ignorant. #SchumerShutdown for illegals. #DemocratShutdown #DemocratLosers #DemocratsDefundMilitary #AlternativeFacts

55. On or about January 26, 2018, a member of the Conspiracy used the Twitter account "@JemiSHaaaZzz" to repost a Tweet about a Senate vote on reproductive health issues, referencing the telephone number of the U.S. Capitol switchboard:

>  Republicans have scheduled a vote Monday on legislation that would ban some women's health care choices 
>
> We can't turn back the clock on women's reproductive health. Call your Senators now and tell them to vote NO: (202) 224-3121.

56. On or about February 8, 2018, a member of the Conspiracy used the Twitter account "@Amconvoice" to post a Tweet about the 2018 U.S. midterm election:

> The only way the Democrats can win 101 GOP seats is to cheat like they always do with illegals & dead voters.

57. On or about February 15, 2018, a member of the Conspiracy used the Twitter account "@KaniJJackson" to post a Tweet about the Parkland, Florida, school shooting and the 2018 U.S. midterm election:

> Reminder: the same GOP that is offering thoughts and prayers today are the same ones that voted to allow loosening gun laws for the mentally ill last February. If you're outraged today, VOTE THEM OUT IN 2018. #guncontrol #Parkland

58. On or about February 16, 2018, a member of the Conspiracy used the Twitter account "@JemiSHaaaZzz" to repost a Tweet about the Special Counsel's Office's indictment of Russian companies and nationals who sought to interfere with U.S. elections and political processes:

> Dear @realDonaldTrump: The DOJ indicted 13 Russian nationals at the Internet Research Agency for violating federal criminal law to help your campaign and hurt other campaigns. Still think this Russia thing is a hoax and a witch hunt? Because a lot of witches just got indicted.

59. On or about February 16, 2018, a member of the Conspiracy used the Twitter account "@JohnCopper16" to post two Tweets about the Special Counsel's Office's indictment:

> Russians indicted today: 13 Illegal immigrants crossing Mexican border indicted today: 0 Anyway, I hope that all those Internet Research Agency f*ckers will be sent to gitmo.
>
> We didn't vote for Trump because of a couple of hashtags shilled by the Russians. We voted for Trump because he convinced us to vote for Trump. And we are ready to vote for Trump again in 2020!

60. On or about February 19, 2018, a member of the Conspiracy used the Twitter account "@KaniJJackson" to post a Tweet about the 2018 midterm election:

> Midterms are in 261 days, use this time to: - Promote your candidate on social media - Volunteer for a campaign - Donate to a campaign - Register to vote - Help others to register to vote - Spread the word We have only 261 days to guarantee survival of democracy. Get to work!

61. On or about February 27, 2018, a member of the Conspiracy used the Twitter account "@JohnCopper16" to post the following Tweet about the 2018 midterm election:

> Dem 2018 platform: - We want women raped by the jihadists - We want children killed - We want higher gas prices - We want more illegal aliens - We want more Mexican drugs And they are wondering why @realDonaldTrump became the President...

62. On or about March 9, 2018, a member of the Conspiracy used the Twitter account "@JohnCopper16" to post the following two Tweets about the summit between President Trump and North Korean President Kim Jong Un:

> WOW! Donald Trump is going to meet Kim Jong Un to discuss denuclearization of North Korea, If Trump gets North Korea to denuclearize its game over for the Democrats! That would be monumental!
>
> RETWEET if you think that Donald Trump deserves a Nobel Peace Prize for resolving the North Korean crisis!

63. On or about March 9, 2018, a member of the Conspiracy used the Twitter account "@KaniJJackson" to post the following two Tweets about the summit between President Trump and North Korean President Kim Jong Un:

> Trump says he will meet with Kim Jong Un in May. But he might not even be president by then. Mueller is coming!
>
> The same people who criticized Barack Obama for signing the Iran Nuclear deal are already praising Trump for his promise to meet with Kim Jong Un and talk about denuclearization.

64. On or about March 14, 2018, a member of the Conspiracy used the Twitter account "@wokeluisa" to post several Tweets regarding the Pennsylvania special election on March 13, 2018, for a House of Representatives seat:

> Enthusiastically watching #PA18 turn blue
>
> Lamb up by only 703 votes... EVERY. VOTE. COUNTS. #PA18

We need to flip about 20 seats to regain control of the House! 19 after tonight! #PA18

Tonight's results are a message regardless of the outcome: D voters are motivated! Blue Wave coming! #PA18

65. On or about March 14, 2018, a member of the Conspiracy used the Twitter account "@TheTrainGuy13" to repost a Tweet about voter fraud:

66. On or about March 18, 2018, a member of the Conspiracy used the Twitter account "@wokeluisa" to post the following Tweet about election fraud:

> Fun fact: the last time a new Republican president was elected without electoral fraud was in 1988

67. On or about March 18, 2018, a member of the Conspiracy used the Twitter account "@wokeluisa" to repost the following Tweet:

> Just a reminder that: - Majority black Flint, Michigan still has drinking water that will give you brain damage if consumed. - Republicans are still trying to keep black people from voting. - A terrorist has been targeting black families for assasination in Austin, Texas.

68. On or about March 19, 2018, a member of the Conspiracy used the Twitter account "@wokeluisa" to post the following Tweets about an explosion in Austin, Texas:

> Trump will tweet NOTHING about yet another explosion in Austin b/c all of the victims have been black and hispanic. Mark my words

> Another explosion in southwest Austin, Texas! Why these bombings ain't a bigger story? Oh yes... all of the victims have been Black and Hispanic #AustinBombings

69. On or about March 19, 2018, a member of the Conspiracy used the Twitter account "@wokeluisa" to post the following Tweet about the 2018 midterm election:

> Make sure to pre-register to vote if you are 16 y.o. or older. Don't just sit back, do something about everything that's going on because November 6, 2018 is the date that 33 senate seats, 435 seats in the House of Representatives and 36 governorships will be up for re-election.

70. On or about March 22, 2018, a member of the Conspiracy used the Twitter account "@johncopper16" to post the following Tweet about the 2018 midterm election:

> Just a friendly reminder to get involved in the 2018 Midterms. They are motivated They hate you They hate your morals They hate your 1A and 2A rights They hate the Police They hate the Military They hate YOUR President

71. On or about May 17, 2018, a member of the Conspiracy used the Twitter account "@KaniJJackson" to repost two Tweets about a U.S. Senate vote on Net Neutrality:

> Ted Cruz voted to repeal #NetNeutrality. Let's save it and repeal him instead.
>
> Here's the list of GOP senators who broke party lines and voted to save #NetNeutrality: Susan Collins John N Kennedy Lisa Murkowski Thank you!

CONCLUSION

72. Based on the foregoing, and on my training, experience, and participation in this and other investigations, I submit there is probable cause to believe that, from at least 2014 to the present, ELENA ALEKSEEVNA KHUSYAYNOVA has violated Title 18, United States Code, Section 371.

David Holt
Special Agent
Federal Bureau of Investigation

Reviewed by:

Jay V. Prabhu
Chief, Cybercrime Unit
Assistant U.S. Attorney

Alex Iftimie
Special Assistant U.S. Attorney

Sworn to before me this 28 th day
of September, 2018

/s/
Ivan D. Davis
United States Magistrate Judge