

KORMAN, J.

IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.

★ NOV 27 2018 ★

RMT:SK/AFM/MTK
F. #2016R02228

GOLD, M.J.

BROOKLYN OFFICE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

ALEKSANDR ZHUKOV,
BORIS TIMOKHIN,
MIKHAIL ANDREEV,
DENIS AVDEEV,
DMITRY NOVIKOV,
SERGEY OVSYANNIKOV,
ALEKSANDR ISAEV and
YEVGENIY TIMCHENKO,

Defendants.

----- X

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Indictment, unless otherwise indicated:

1. Individuals and businesses (“publishers”) were able to provide free content on the internet—such as websites, search engines, translation services, video playback services and global mapping services—because advertisers paid for the opportunity to show advertisements (sometimes referred to as “ads”) alongside that content.

2. The digital advertising industry was made up of a chain of specialized businesses. Publishers commonly used entities called supply-side platforms (“SSPs”) to conduct auctions that sold the advertising space on their sites. These auctions commenced

INDICTMENT
CR 18 - 633

Cr. No. (T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(1), 982(a)(2)(B), 982(b)(1), 1028A(a)(1), 1028A(b), 1028A(c)(4), 1030(a)(2), 1030(a)(4), 1030(a)(5), 1030(b), 1030(c)(2)(A), 1030(c)(2)(B), 1030(c)(3)(A), 1030(c)(4), 1030(i)(1), 1030(i)(2), 1343, 1349, 1956(h), 1957(a), 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

as soon as an internet user accessed a website and concluded within milliseconds, before the webpage displayed to the user. Businesses seeking to promote their goods and services online (“brands”) commonly used entities called demand-side platforms (“DSPs”) to bid in these auctions and thereby had their advertisements placed on webpages that real human internet users were browsing. Brands commonly paid for advertising on a lump-sum basis, and publishers commonly received payment based on how many times users clicked on or viewed advertisements (sometimes referred to as “impressions”). The entities in between the brands and the publishers—the DSPs, SSPs and ad networks that connected SSPs with publishers—charged fees along the way.

3. The defendants in this case used sophisticated computer programming and infrastructure spread around the world to exploit the digital advertising industry through fraud. They represented to others that they ran legitimate ad networks that delivered advertisements to real human internet users accessing real internet webpages. In fact, the defendants faked both the users and the webpages: in each of the charged schemes, they programmed computers they controlled to load advertisements on fabricated webpages, via an automated program, in order to fraudulently obtain digital advertising revenue.

4. In one iteration—a datacenter-based scheme referred to in the ad industry as “Methbot”—the defendants used computers they controlled that they had rented from commercial datacenters in Dallas, Texas, and elsewhere.

5. In another iteration—a botnet-based scheme referred to in the ad industry as “3ve.2 Template A”—the defendants used computers to which they had gained unauthorized access (i.e. that had been “hacked”), including computers belonging to

individuals and businesses in the United States and elsewhere, including in the Eastern District of New York.

I. The Defendants

6. The defendant ALEKSANDR ZHUKOV was a citizen of the Russian Federation. He led the development of the datacenter-based scheme. ZHUKOV served as the chief executive officer of Ad Network #1, the identity of which is known to the Grand Jury. Ad Network #1 was a private corporation owned by ZHUKOV with offices in the Russian Federation and the Republic of Bulgaria. It purported to assist customers with delivering advertisements to real human internet users via its ad network.

7. The defendant BORIS TIMOKHIN was a citizen of the Russian Federation and worked for Ad Network #1. TIMOKHIN handled programming aspects of the datacenter-based scheme.

8. The defendant MIKHAIL ANDREEV was a resident of the Russian Federation and the Ukraine and worked for Ad Network #1. ANDREEV handled programming aspects of the datacenter-based scheme.

9. The defendant DENIS AVDEEV was a citizen of the Russian Federation and worked for Ad Network #1. AVDEEV handled technical and business aspects of the datacenter-based scheme.

10. The defendant DMITRY NOVIKOV was a resident of the Russian Federation and worked for Ad Network #1. NOVIKOV handled administrative and coordination aspects of the datacenter-based scheme.

11. The defendant SERGEY OVSYANNIKOV was a citizen of the Republic of Kazakhstan. He led the development of the botnet-based scheme and provided

technical assistance to the operators of the datacenter-based scheme. OVSYANNIKOV served as a principal and owner of Ad Network #2, the identity of which is known to the Grand Jury. Ad Network #2 was a private corporation owned by OVSYANNIKOV and ALEKSANDR ISAEV with a registration address in Edinburgh, Scotland. It purported to assist customers with delivering advertisements to real human internet users via its ad networks.

12. The defendant ALEKSANDR ISAEV was a citizen of the Russian Federation and served as a principal, owner and chief executive officer of Ad Network #2. ISAEV handled business and contracting aspects of the botnet-based scheme.

13. The defendant YEVGENIY TIMCHENKO was a resident of the Republic of Kazakhstan and worked at Ad Network #2. TIMCHENKO handled logistical and administrative aspects of the botnet-based scheme.

II. The Schemes to Defraud

A. The Datacenter-Based Scheme

14. In or about September 2014, ZHUKOV, TIMOKHIN, ANDREEV, AVDEEV and NOVIKOV (collectively, the “Methbot defendants”) launched a digital advertising fraud scheme under the guise of operating Ad Network #1. Ad Network #1 had business arrangements with other advertising networks that enabled it to receive payment in return for placing advertising placeholders (“ad tags”) with publishers on behalf of those advertising networks. Rather than place these ad tags on real publishers’ webpages, however, ZHUKOV and others rented more than 1,900 computer servers located at commercial datacenters in Dallas, Texas, and elsewhere, and used those datacenter computer servers to simulate humans viewing ads on fabricated webpages. By these means, the

Methbot defendants caused thousands of datacenter computer servers to load fabricated webpages, offer up the advertising space on the fabricated webpages for bidding, and load advertisements on the fabricated webpages through an automated computer program. This activity (the “fraudulent ad traffic”) was not viewed by any real human internet users.

15. ZHUKOV and others programmed the datacenter computer servers to load fabricated webpages—that is, mostly blank webpages containing a blank space for an ad—that purported to be located at the domains of well-known publishers. ZHUKOV researched lucrative domains to fabricate and ran online searches for the “top 10000 domains” and “top 100k domains.” ZHUKOV then sent TIMOKHIN “new domains to try,” deliberately targeting “the top USA desktop domains” for businesses in the United States. In this way, the Methbot defendants fabricated (or “spoofed”) more than 250,000 webpages distributed across more than 5,000 domains associated with online publishers, including the domains of thousands of businesses in the United States and multiple businesses in the Eastern District of New York.

16. TIMOKHIN, ANDREEV and others also programmed the datacenter computer servers to simulate the internet activity of real human internet users when loading the fabricated webpages, in order to deceive SSPs and others in the digital advertising industry and to evade fraud detection software widely used in the industry. They developed programming code that caused the datacenter computer servers to operate an automated browser, click on online advertisements a randomly determined number of times, simulate a mouse moving around and scrolling down a webpage, control and monitor video playback, and falsely appear to be signed into popular social media services. The programming code

contained explicit references to “Meth” and “Fake,” including “MethBrowser,” “MethFlashObjects,” “FakeClient” and “FakedPixel.”

17. In furtherance of their fraudulent scheme, the Methbot defendants communicated with one another about the development of this programming code using an online project management platform. For example:

(a) On or about October 25, 2014, ANDREEV circulated programming code and stated that it was designed to ensure that signals coming from the datacenter computer servers had the correct “‘browser’ parameters.”

(b) On or about October 28, 2014, NOVIKOV instructed TIMOKHIN to carry out “research about how to make ‘mouse moves and scroll more realistic/meaningful’” on the datacenter computer servers. ZHUKOV similarly instructed TIMOKHIN to address the “lack of mouse move,” an undertaking that continued over the following year. TIMOKHIN researched methods for simulating mouse movements by, for example, running an online search for “actionscript simulate mouse click.”

(c) On or about October 28, 2014, NOVIKOV discussed “[e]mulating ‘video watch’” on the datacenter computer servers and cautioned that “[t]he videos need to be clicked on and watched for 60-90 seconds.” This was because advertisers often would not pay for a video impression unless they knew that the user had watched the video for a substantial amount of time.

(d) On or about November 21, 2014, ANDREEV circulated programming code and stated that it was designed to set the datacenter computer servers’ “IP

address time zone” to “EST”—Eastern Standard Time—“by default.” Earlier that day, ANDREEV had run an online search for “new york timezone.”

(e) On or about December 1, 2014, ANDREEV circulated programming code designed to cause the datacenter computer servers to automatically start and stop an online video player, and stated, “Basically this is how it is possible to generate the events.”

(f) In a to-do list dated June 25, 2015, ZHUKOV instructed TIMOKHIN to cause the datacenter computer servers to appear to be signed into Facebook: “add authorization for Facebook [] users. There is Google, twitter too; [but] no FB (There should be approximately 40% of them.)”

(g) On or about August 4, 2015, ZHUKOV stated that he intended to research the fraud detection software deployed by certain U.S. cybersecurity firms and “check [] out [their] filter for the possibility of fucking them over.”

18. On or about October 16, 2016, after discovering that the signals coming from the datacenter computer servers did not register as fraudulent with a certain U.S. cybersecurity firm, ZHUKOV boasted to TIMOKHIN that their scheme was “magnificent.” On or about December 10, 2016, ZHUKOV sent an email to a potential business partner in which he offered “100% USA traffic” that could pass through “filters” from various U.S. cybersecurity firms and amounted to “20-50 millions [sic] impressions daily.”

19. To further deceive SSPs and others in the digital advertising industry into believing that the datacenter computer servers were genuine human users, ZHUKOV and others leased more than 650,000 Internet Protocol (“IP”) addresses from various IP

address leasing companies and assigned multiple IP addresses to each of the datacenter computer servers. ZHUKOV, AVDEEV and others then created false entries for the datacenter computer servers in a global register of IP addresses. These false entries made it appear that the datacenter computer servers controlled by the Methbot defendants were residential computers belonging to individual human internet users who were subscribed to various residential internet service providers. For example:

(a) Several of the false IP address registry entries misappropriated or mimicked the corporate identities of at least six major U.S. internet service providers, including at least one provider with offices in the Eastern District of New York. ZHUKOV maintained a list of these and other false corporate names in his cloud storage account. None of the IP addresses registered in the respective U.S. internet service providers' real or mimicked names was actually in their possession, custody or control. In this way, the Methbot defendants sought to make it appear to SSPs and others that the computers in question belonged to customers of these internet service providers, rather than being located in datacenters.

(b) For the same reason, the Methbot defendants also incorporated false usage and location information into the IP address registries. For example, on or about May 13, 2016, AVDEEV directed an IP leasing company to change the "Usage type" for approximately 261,000 leased IP addresses from "commercial" or "datacenter" to "ISP" (internet service provider), ascribe a more diverse set of cities and states to the leased IP addresses, and reduce the number of leased IP addresses associated with certain small cities to more realistic levels commensurate with their populations. In this way, the Methbot

defendants sought to make it appear to SSPs and others that the computers in question belonged to real human internet users located in homes and businesses around the country.

20. The Methbot defendants thus created the illusion that real human internet users were visiting real internet webpages. ZHUKOV and others solicited bids on the opportunity to show advertisements to those purported users. In response, DSPs bid on those opportunities. The winning DSPs made payments to SSPs (using money provided by brands) in return for the purported impressions, and the SSPs transferred those payments to advertising networks to be passed along the chain of intermediaries described above.

21. OVSYANNIKOV collaborated with the Methbot defendants to knowingly obtain fraudulent ad traffic for his own companies. OVSYANNIKOV did business with the Methbot defendants, purchased fraudulent ad traffic from the Methbot defendants and provided the Methbot defendants with technical advice and assistance to ensure that the fraudulent ad traffic passed as real. For example, on or about October 22, 2014, OVSYANNIKOV instructed NOVIKOV that the datacenter computer servers' automated browsers needed to include "accept-language" in their headers—indicating the purported user's preferred language—to evade fraud detection software. Similarly, in or about November 2014, OVSYANNIKOV discussed the concept of "mouse move" with the Methbot defendants.

22. Over the course of the scheme, the Methbot defendants falsified billions of ad impressions. Hundreds of brands and ad agencies around the world, including many in the United States and at least one with offices in the Eastern District of New York,

collectively paid more than \$7 million in advertising fees for fraudulent ad traffic. The Methbot defendants, in turn, reaped millions of dollars in revenue.

23. The Methbot defendants recorded the revenue from the datacenter-based scheme—which amounted to 10s of thousands of dollars daily—using an online control panel that tracked the millions of bids solicited by the datacenter computer servers each day and the millions of resulting ad impressions falsified each day. For example, during a single day in October 2016, the Methbot defendants recorded more than \$56,000 in revenue from placing more than 442 million fraudulent bid requests and falsifying more than 16 million ad impressions.

24. The Methbot defendants re-invested some of the proceeds from the datacenter-based scheme to perpetuate the fraud, and they concealed other proceeds by transferring them to other companies. For example, ZHUKOV directed payments from ad networks to a corporate bank account located in the Czech Republic, which he then used to pay for servers and IP addresses used in the scheme. ZHUKOV also redirected \$5.4 million from the account to a corporate bank account located in New Zealand.

25. On or about December 20, 2016, researchers at a private cybersecurity firm based in New York City publicly revealed the operation of the datacenter-based scheme in a white paper titled “The Methbot Operation.”

26. The Methbot defendants reacted to the publication of the white paper by attempting to delete evidence. They deleted all of their communications from the online project management platform that they used to develop the scheme, and they deleted more than 26,000 emails from an email account identified in the white paper, which was the

registration email account for more than 1,400 IP addresses used in the scheme.

TIMOKHIN also deleted more than 96,000 emails from his own email account, which contained explicit discussions of the scheme and referenced more than 15,500 IP addresses used in the scheme.

27. In the days after the publication of the white paper, ANDREEV researched whether he had been publicly associated with the scheme; for example, ANDREEV ran online searches for “russian hackers methbot” and “mikhail andreev methbot.” In communications with associates, ANDREEV privately acknowledged his association with the scheme, speculated that he was “being investigated by the FBI,” admitted to writing code for the scheme “[a]t the initial stage” and explained that “[t]he companies that get fooled consider it fraud.”

B. The Botnet-Based Scheme

28. In or about December 2015, OVSYANNIKOV, ISAEV and TIMCHENKO (collectively, the “Eve 2A defendants”) launched another digital advertising fraud scheme under the guise of operating Ad Network #2.

29. Ad Network #2 had business arrangements with other advertising networks that enabled it to receive payment in return for placing ad tags with publishers on behalf of those advertising networks. Rather than place these ad tags on real publishers’ webpages, however, Ad Network #2 obtained access to a network of computers that had been hacked with malware (a “botnet”) and used those infected computers—without their true owners’ knowledge or permission—to load ads on fabricated webpages.

30. At a single point in time, OVSYANNIKOV and others accessed more than 1.7 million infected computers, including approximately 1 million in the United States and more than 1,500 at residences and businesses in the Eastern District of New York. The overall number of infected computers over the course of the scheme was much larger.

31. OVSYANNIKOV and others caused the infected computers to load fabricated webpages—in this instance, mostly blank webpages containing an internal placeholder for an ad and embedded with computer code instructing the browser to load a video player—that purported to be articles and other content on the domains of well-known publishers. OVSYANNIKOV and TIMCHENKO researched domains to fabricate, deliberately targeting domains for businesses in the United States, and placed promising domains on a running list titled “New companies for spoofing.” OVSYANNIKOV also maintained lists of domains in his cloud storage account and on servers that he controlled. The domains included more than 86,000 domains associated with online publishers, including the domains of thousands of businesses in the United States and multiple businesses in the Eastern District of New York.

32. To carry out the scheme, OVSYANNIKOV, TIMCHENKO and others developed an elaborate infrastructure of command-and-control servers and other servers designed to provide instructions, resources and means of obfuscation to the infected computers. These servers were located in the United States and around the world, including in Missouri, California, New Jersey and the Netherlands. TIMCHENKO deliberately chose certain U.S. service providers because they had the “coolest processors” and a “larger” cache (for temporary data storage) than competing providers. OVSYANNIKOV maintained a

collaborative spreadsheet in his cloud storage account titled “[Ad Network] Structure. Hosting and Domains” that set out this infrastructure and listed many of the servers involved in the scheme (including several designated as repositories of “spoof” webpages). TIMCHENKO had access and editing privileges to the spreadsheet; ISAEV had read-only access to the spreadsheet.

33. The Eve 2A defendants’ servers performed various functions:

(a) The infected computers communicated with the “Redirect Servers,” which provided them with instructions to connect to the “Fraudulent Content Servers.”

(b) The Fraudulent Content Servers (including those described by OVSYANNIKOV in his spreadsheet as repositories of “spoof” webpages) supplied infected computers with fabricated webpages purporting to be located at the spoofed domains. The infected computers loaded the fabricated webpages on hidden browsers that were invisible to the computers’ true owners. The infected computers then downloaded digital video players for use in “watching” video advertisements in the relevant ad spaces on the fabricated webpages.

(c) The infected computers again communicated with the Redirect Servers, which supplied them with ad tags and caused them to contact SSPs and offer up the advertising space on the fabricated webpages for bidding. During this process, the infected computers sent the SSPs information including, among other things, their IP addresses, the webpage addresses for the fabricated webpages, the dimensions of the places in which the advertisements would play, and the technical specifications of the video players.

(d) The Redirect Servers meanwhile communicated with “Backend Servers” thousands of times per hour. The Backend Servers contained lists of online publishers’ domains, as well as computer code designed to respond to incoming communications with domains to be spoofed and ad tags containing instructions to contact an SSP. The Backend Servers also contained computer code designed to vet the IP addresses of infected computers to check and record whether the computers already had been flagged by cybersecurity companies as associated with digital advertising fraud.

(e) Over the course of the scheme, the Eve 2A defendants’ servers connected with over 15 million IP addresses worldwide.

34. OVSYANNIKOV explained the resulting system to his co-conspirators in a communication on April 20, 2016. “[Y]ou give me a company,” he began, and then provided a web address that included a major U.S. retailer’s domain; he continued, “the bot takes that link [and] sets itself accordingly” so that the “spoofed domain” would be “[retailer].com” and the “host ip” would be “www2,” OVSYANNIKOV’s nickname for one of the Fraudulent Content Servers.

35. By these means, the Eve 2A defendants caused millions of infected computers around the world to surreptitiously download fabricated webpages, offer up the advertising space on the fabricated webpages for bidding, and load advertisements on the fabricated webpages. All the while, the infected computers’ true owners saw none of this activity. Thus, the advertisements were not viewed by any real human internet users.

36. To evade fraud detection software, the Eve 2A defendants vetted the information emitted from their bots. They developed programming code designed to check and record whether the IP address and other identifying characteristics of a particular bot had

already been flagged by cybersecurity companies as associated with digital advertising fraud. Over the course of approximately four months, they employed the code to vet more than 9.7 million IP addresses worldwide, including more than 4 million in the United States and more than 8,300 in the Eastern District of New York. OVSYANNIKOV cautioned others not to direct traffic from bots that had already been flagged by cybersecurity companies to SSPs that were relying on those cybersecurity companies.

37. The Eve 2A defendants thus created the illusion that real human internet users were visiting real internet webpages. OVSYANNIKOV and others solicited bids on the opportunity to show advertisements to those purported users. In response, DSPs bid on those opportunities. The winning DSPs made payments to SSPs (using money provided by brands) in return for the purported impressions, and the SSPs transferred those payments to advertising networks to be passed along the chain of intermediaries described above.

38. The Eve 2A defendants recorded the revenue from the botnet-based scheme using various spreadsheets that tracked the millions of bids solicited by the infected computers each day and the millions of resulting ad impressions falsified each day.

39. Over the course of the scheme, the Eve 2A defendants falsified billions of ad impressions. Hundreds of brands and ad agencies around the world, including many in the United States and at least one with offices in the Eastern District of New York, collectively paid 10s of millions of dollars in advertising fees for these falsified ad impressions. The Eve 2A defendants, in turn, reaped 10s of millions of dollars in revenue. For example, from January 2016 through May 2017, the Eve 2A defendants received more than \$29 million in revenue from the scheme.

40. The Eve 2A defendants re-invested some of the proceeds from the botnet-based scheme to perpetuate the fraud. For example, OVSYANNIKOV and ISAEV directed payments from ad networks to corporate bank accounts in the Czech Republic and Switzerland, at least one of which they then used to pay for servers used in the scheme.

41. The Eve 2A defendants sought to conceal other proceeds by layering the funds amongst various shell companies, each of which contained no public website or outward-facing business. For example:

(a) On or about December 1, 2016, OVSYANNIKOV obtained a list of “high filling” publishers’ domains from an employee of an ad network, who requested that OVSYANNIKOV “increase [his] traffic.” The next day, TIMCHENKO added 10 of the domains to the running list of “New companies for spoofing.” In or about March 2017, the ad network paid more than \$340,000 into Ad Network #2’s bank account in the Czech Republic, with the notation “December revenue,” as payment for advertising traffic. Funds were subsequently wired from Ad Network #2’s account to shell entities, including an entity controlled by OVSYANNIKOV and another entity that in turn wired the funds directly to ISAEV. None of these entities had any public website or outward-facing business.

(b) In or around and between July 2016 and May 2017, Ad Network #2’s account also wired approximately \$1.2 million into accounts in Switzerland, held in the name of an entity controlled by OVSYANNIKOV. This entity, too, lacked any public website or outward-facing business.

42. On or about October 22, 2018, foreign law enforcement authorities arrested OVSYANNIKOV in Kuala Lumpur, Malaysia. OVSYANNIKOV sought to notify

his co-conspirators of his arrest, and ISAEV and TIMCHENKO subsequently deleted the contents of their email accounts and online cloud storage accounts used in the scheme.

III. The Victims

43. The datacenter-based scheme and the botnet-based scheme victimized numerous players in the digital advertising industry.

44. The schemes victimized brands who sought opportunities to advertise their goods and services to real human internet users but lost those opportunities and instead paid for advertisements automatically loaded by computers.

45. The schemes victimized online publishers by creating false and fraudulent webpages purporting to be located at real publishers' domains, stealing the publishers' identities and misappropriating those identities for a fraudulent purpose, undermining the reputation and credibility of those publishers in the ad market and reducing the revenues that the actual publishers would otherwise earn.

46. The schemes victimized ad platforms—the SSPs and DSPs—by misusing these clearinghouses of ad traffic for fraud.

47. The datacenter-based scheme victimized internet service providers by stealing their corporate identities for the purpose of registering IP addresses with false information.

48. The botnet-based scheme victimized individuals and businesses whose computers were used, without their knowledge or authorization, to perpetrate the fraud.

COUNT ONE

(Wire Fraud Conspiracy—Datacenter-Based Scheme)

49. The allegations contained in paragraphs one through 27 and 43 through 47 are realleged and incorporated as though fully set forth in this paragraph.

50. In or about and between September 2014 and December 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants ALEKSANDR ZHUKOV, BORIS TIMOKHIN, MIKHAIL ANDREEV, DENIS AVDEEV, DMITRY NOVIKOV and SERGEY OVSYANNIKOV, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud brands, ad platforms and others in the digital advertising industry, and to obtain money and property from brands, ad platforms and others in the digital advertising industry by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, emails and other online communications and monetary transfers, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT TWO

(Wire Fraud—Datacenter-Based Scheme)

51. The allegations contained in paragraphs one through 27 and 43 through 47 are realleged and incorporated as though fully set forth in this paragraph.

52. In or about and between September 2014 and December 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants ALEKSANDR ZHUKOV, BORIS TIMOKHIN, MIKHAIL ANDREEV, DENIS AVDEEV, DMITRY NOVIKOV and SERGEY OVSYANNIKOV, together with others, did knowingly and intentionally devise a scheme and artifice to defraud brands, ad platforms and others in the digital advertising industry, and to obtain money and property from brands, ad platforms and others in the digital advertising industry by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, emails and other online communications and monetary transfers.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT THREE

(Money Laundering Conspiracy—Datacenter-Based Scheme)

53. The allegations contained in paragraphs one through 27 and 43 through 47 are realleged and incorporated as though fully set forth in this paragraph.

54. In or about and between September 2014 and December 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants ALEKSANDR ZHUKOV, BORIS TIMOKHIN, MIKHAIL ANDREEV, DENIS AVDEEV and DMITRY NOVIKOV, together with others, did knowingly and intentionally conspire to:

(a) transport, transmit and transfer monetary instruments and funds from a place in the United States to and through a place outside the United States and to a place in the United States from and through a place outside the United States, (i) with the intent to promote the carrying on of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, contrary to Title 18, United States Code, Section 1956(a)(2)(A); and (ii) knowing that the monetary instruments and funds involved in the transportation, transmission and transfer represented the proceeds of some form of unlawful activity, and knowing that such transportation, transmission and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i); and

(b) engage in one or more monetary transactions within the United States involving property of a value greater than \$10,000 that was derived from one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, knowing that the funds were the proceeds of some unlawful activities and were in fact proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, contrary to Title 18, United States Code, Section 1957(a).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

COUNT FOUR

(Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity—Datacenter-Based Scheme)

55. The allegations contained in paragraphs one through 27 and 43 through 47 are realleged and incorporated as though fully set forth in this paragraph.

56. In or about and between September 2014 and December 2016, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants ALEKSANDR ZHUKOV, BORIS TIMOKHIN, MIKHAIL ANDREEV, DENIS AVDEEV and DMITRY NOVIKOV, together with others, did knowingly and intentionally engage in one or more monetary transactions within the United States involving property of a value greater than \$10,000 that was derived from one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, knowing that the funds were the proceeds of some unlawful activities and were in fact proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, and wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349.

(Title 18, United States Code, Sections 1957(a), 2 and 3551 et seq.)

COUNT FIVE

(Wire Fraud Conspiracy—Botnet-Based Scheme)

57. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

58. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the

defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud brands, ad platforms and others in the digital advertising industry, and to obtain money and property from brands, ad platforms and others in the digital advertising industry by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, emails and other online communications and monetary transfers, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT SIX

(Wire Fraud—Botnet-Based Scheme)

59. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

60. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did knowingly and intentionally devise a scheme and artifice to defraud brands, ad platforms and others in the digital advertising industry, and to obtain money and property from brands, ad platforms and others in the digital advertising industry by means of materially false and fraudulent pretenses, representations and promises,

and for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications to computers and servers in the United States and elsewhere, emails and other online communications and monetary transfers.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT SEVEN

(Aggravated Identity Theft—Botnet-Based Scheme)

61. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

62. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, during and in relation to the crimes charged in Counts Five and Six, did knowingly and intentionally transfer, possess and use, without lawful authority, one or more means of identification of other persons, to wit: IP addresses and other information, knowing that these means of identification belonged to said persons.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), 2 and 3551 et seq.)

COUNT EIGHT

(Conspiracy to Commit Computer Intrusions—Botnet-Based Scheme)

63. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

64. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did knowingly and willfully conspire to:

(a) intentionally access one or more computers without authorization and exceed authorized access, and thereby to obtain information from one or more protected computers for the purpose of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the laws of the United States and any State, and the value of the information obtained exceeded \$5,000, contrary to Title 18, United States Code, Sections 1030(a)(2), 1030(b), 1030(c)(2)(A) and 1030(c)(2)(B);

(b) with intent to defraud access one or more protected computers without authorization, and exceed authorized access, and by means of such conduct to further the intended fraud and obtain something of value, to wit: the use of a computer, information and United States and foreign currency, contrary to Title 18, United States Code, Sections 1030(a)(4), 1030(b) and 1030(c)(3)(A); and

(c) (i) knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization affecting 10 or more protected computers during a one-year period; and (ii) intentionally access one or more protected computers without authorization, and as a result of

such conduct, recklessly cause damage affecting 10 or more protected computers during a one-year period, contrary to Title 18, United States Code, Sections 1030(a)(5), 1030(b) and 1030(c)(4).

65. In furtherance of the conspiracy and to effect its objects, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, committed and caused to be committed, among others, the following:

OVERT ACTS

(a) On or about April 20, 2016, OVSYANNIKOV sent an online message to his co-conspirators explaining how computers in the botnet would be instructed to spoof a domain.

(b) On or about August 8, 2016, ISAEV sent an invoice to an ad network for advertising services.

(c) On or about February 27, 2017, TIMCHENKO logged in to the administrative panel of one of the Fraudulent Content Servers.

(d) On or about May 17, 2018, OVSYANNIKOV, ISAEV and TIMCHENKO, together with others, caused an infected computer belonging to a business in Blue Point, New York, to surreptitiously download a fabricated webpage, offer up the advertising space on the fabricated webpage for bidding and load an advertisement on the fabricated webpage for a nonprofit hospital located in West Islip, New York, all without the knowledge or permission of the infected computer's true owner.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT NINE

(Computer Intrusion and Obtaining Information—Botnet-Based Scheme)

66. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

67. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did knowingly and intentionally access, and attempt to access, one or more computers without authorization and exceed authorized access, and thereby did obtain information from one or more protected computers for the purpose of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the laws of the United States and any State, and the value of the information obtained exceeded \$5,000.

(Title 18, United States Code, Sections 1030(a)(2), 1030(b), 1030(c)(2)(A), 1030(c)(2)(B), 2 and 3551 et seq.)

COUNT TEN

(Computer Intrusion in Furtherance of Fraud—Botnet-Based Scheme)

68. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

69. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did knowingly and with intent to defraud access, and

attempt to access, one or more protected computers without authorization, and exceed authorized access, and by means of such conduct did further the intended fraud and obtain something of value, to wit: the use of a computer, information and United States and foreign currency.

(Title 18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), 2 and 3551 et seq.)

COUNT ELEVEN

(Computer Intrusion and Causing Damage—Botnet-Based Scheme)

70. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

71. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did: (i) knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, intentionally cause damage without authorization affecting 10 or more protected computers during a one-year period; and (ii) intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause damage affecting 10 or more protected computers during a one-year period.

(Title 18, United States Code, Sections 1030(a)(5), 1030(b), 1030(c)(4), 2 and 3551 et seq.)

COUNT TWELVE

(Money Laundering Conspiracy—Botnet-Based Scheme)

72. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

73. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did knowingly and intentionally conspire to:

(a) transport, transmit and transfer monetary instruments and funds from a place in the United States to and through a place outside the United States and to a place in the United States from and through a place outside the United States, (i) with the intent to promote the carrying on of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, and computer intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4) and (a)(5), contrary to Title 18, United States Code, Section 1956(a)(2)(A); and (ii) knowing that the monetary instruments and funds involved in the transportation, transmission and transfer represented the proceeds of some form of unlawful activity, and knowing that such transportation, transmission and transfer was designed in whole and in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, and computer

intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4) and (a)(5), contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i); and

(b) engage in one or more monetary transactions within the United States involving property of a value greater than \$10,000 that was derived from one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, and computer intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4) and (a)(5), knowing that the funds were the proceeds of some unlawful activities and were in fact proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, and computer intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4) and (a)(5), contrary to Title 18, United States Code, Section 1957(a).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

COUNT THIRTEEN

(Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity—Botnet-Based Scheme)

74. The allegations contained in paragraphs one through 13 and 28 through 46 and 48 are realleged and incorporated as though fully set forth in this paragraph.

75. In or about and between December 2015 and October 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants SERGEY OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY TIMCHENKO, together with others, did knowingly and intentionally engage in one or more monetary transactions within the United States involving property of a value greater than

\$10,000 that was derived from one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, and computer intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4) and (a)(5), knowing that the funds were the proceeds of some unlawful activities and were in fact proceeds of one or more specified unlawful activities, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, wire fraud conspiracy, in violation of Title 18, United States Code, Section 1349, and computer intrusion, in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4) and (a)(5).

(Title 18, United States Code, Sections 1957(a), 2 and 3551 et seq.)

**CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS ONE, TWO, FIVE AND SIX**

76. The United States hereby gives notice to the defendants charged in Counts One, Two, Five and Six that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting or derived from proceeds obtained directly or indirectly as a result of such offenses.

77. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (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 which cannot be

divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

**CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS THREE, FOUR, TWELVE AND THIRTEEN**

78. The United States hereby gives notice to the defendants charged in Counts Three, Four, Twelve and Thirteen that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offenses to forfeit any property, real or personal, involved in such offenses, or any property traceable to such property.

79. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (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 which cannot be divided

without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21, United States Code, Section 853(p))

**CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS EIGHT THROUGH ELEVEN**

80. The United States hereby gives notice to the defendants charged in Counts Eight through Eleven that, upon their conviction of such offenses, the government will seek forfeiture in accordance with Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1), which require any person convicted of such offenses to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses, and such person's interest in any personal property that was used or intended to be used to commit or to facilitate such offenses, including but not limited to the following domain names:

- (a) adzos.com;
- (b) clickandia.com
- (c) webvideocore.com;
- (d) clickservers.net;
- (e) clickmediallc.net;
- (f) mobapptrack.com; and
- (g) rtbclick.net.

81. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (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 which cannot be

divided without difficulty;

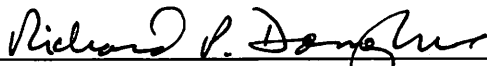
it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Sections 982(b)(1) and 1030(i)(2), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(2)(B), 982(b)(1), 1030(i)(1) and 1030(i)(2); Title 21, United States Code, Section 853(p))

A TRUE BILL



FOREPERSON



RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

F.#: 2016R02228
FORM DBD-34
JUN. 85

No.

UNITED STATES DISTRICT COURT

EASTERN District of NEW YORK

CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

ALEKSANDR ZHUKOV, BORIS TIMOKHIN, MIKHAIL
ANDREEV, DENIS AVDEEV, DMITRY NOVIKOV, SERGEY
OVSYANNIKOV, ALEKSANDR ISAEV and YEVGENIY
TIMCHENKO,

Defendants.

INDICTMENT

(T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(1), 982(a)(2)(B), 982(b)(1), 1028A(a)(1), 1028A(b), 1028A(c)(4), 1030(a)(2), 1030(a)(4), 1030(a)(5), 1030(b), 1030(c)(2)(A), 1030(c)(2)(B), 1030(c)(3)(A), 1030(c)(4), 1030(i)(1), 1030(i)(2), 1343, 1349, 1956(h), 1957(a), 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

A true bill. James Thayer Foreperson

Filed in open court this _____ day,
of _____ A.D. 20 _____
Clerk

Bail, \$ _____

Saritha Komatireddy, Alexander Mindlin, Michael Keilty,
Assistant U.S. Attorneys (718) 254-7000