

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

v.

Criminal No.

ALEKSEI SERGEYEVICH MORENETS
EVGENII MIKHAYLOVICH SEREBRIAKOV
IVAN SERGEYEVICH YERMAKOV
ARTEM ANDREYEVICH MALYSHEV
DMITRIY SERGEYEVICH BADIN
OLEG MIKHAYLOVICH SOTNIKOV
ALEXEY VALEREVICH MININ

Defendants.

18 U.S.C. §§ 371, 1030(a)(2)(C),
1030(a)(5)(A)
(Conspiracy)
18 U.S.C. § 1349 and § 3559(g)(1)
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1343 (Wire Fraud)
18 U.S.C. § 1028A
(Aggravated Identity Theft)
18 U.S.C. § 1956(h)
(Conspiracy to Launder Money)

[UNDER SEAL]

INDICTMENT

COUNT ONE
(Conspiracy)

The grand jury charges:

1. At all times relevant to the indictment, from at least 2014 up to and including May 2018, the Russian Federation (Russia) operated a military intelligence agency called the Main Intelligence Directorate of the General Staff (GRU). The GRU was headquartered in Moscow, Russia, and was comprised of multiple units, including Units 26165 and 74455. Military Unit 26165, also known as the “GRU 85 Main Special Service Center,” was located at 20 Komsomolskiy Prospekt, Moscow, Russia. Military Unit 74455 was located at 22 Kirova Street, Khimki, Moscow, Russia.

2. During the charged timeframe, members of the GRU conducted persistent and sophisticated criminal cyber intrusions by hacking into the computers of victims that included U.S. persons, corporate entities, international organizations and their respective employees. These victims were located around the world, including in the Western District of Pennsylvania, and were targeted by the GRU for their strategic interest to the Russian government.

3. Specifically, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ were GRU officers who knowingly and intentionally conspired with each other, and with persons known and unknown to the grand jury, (collectively, the conspirators) to gain unauthorized access (to “hack”) into victim computers and steal private or otherwise sensitive information, in violation of United States laws. In many instances, the stolen information was publicized by the GRU as part of a related “influence and disinformation” campaign designed to undermine the legitimate interests of the victims, further Russian interests, retaliate against Russia’s detractors and sway public opinion in Russia’s favor.

THE VICTIMS

4. Among those victims targeted by the GRU were U.S. and international anti-doping agencies, sporting federations, anti-doping officials, other sports-related organizations and nearly 250 athletes from approximately 30 countries. The victims included, among others, the following:

- the U.S. Anti-Doping Agency (USADA), a U.S. based agency, headquartered in Colorado Springs, Colorado;

- the World Anti-Doping Agency (WADA), an international agency, headquartered in Montreal, Canada;
- the Canadian Centre for Ethics in Sport (CCES), a Canadian-based anti-doping agency, headquartered in Ottawa, Canada;
- the International Association of Athletics Federations (IAAF), an international sports governing body, headquartered in Monaco;
- The Court of Arbitration for Sport (TAS/CAS), headquartered in Lausanne, Switzerland; and,
- the Fédération Internationale de Football Association (FIFA), an international governing body for football, headquartered in Zurich, Switzerland.

5. These victims were targeted by the GRU for their role in the investigation or public condemnation of Russia's state-sponsored athlete doping program and their public support of, or involvement in, a ban on Russian athletes in worldwide athletic competitions (including the 2016 Summer Olympics and Paralympics in Rio de Janeiro, Brazil). The GRU also targeted the victims to steal athletes' medical records which were then publicized as part of an influence and disinformation campaign.

6. In addition to anti-doping agencies, the GRU targeted other victims of potential benefit to Russian interests, including:

- Westinghouse Electric Corporation (WEC), a nuclear energy company headquartered in the Western District of Pennsylvania;
- the Organisation for the Prohibition of Chemical Weapons (OPCW), an organization headquartered in The Hague, Netherlands, investigating the use of

chemical weapons in Syria and the March 2018 poisoning of a former GRU officer and others in the United Kingdom with a chemical nerve agent; and,

- the Spiez Swiss Chemical Laboratory located in Spiez, Switzerland, an accredited laboratory of the OPCW that analyzed the chemical agent connected to the poisonings of a former GRU officer and others in the United Kingdom.

Cyber Intrusions and Related Influence and Disinformation Campaigns

7. The cyber intrusions conducted by the GRU involved sophisticated, persistent and unauthorized access into the victims' computer networks for the purpose of stealing private or otherwise sensitive information.

8. The hacking was often conducted remotely, from Russia. If the remote hack was unsuccessful or if it did not provide the conspirators with sufficient access to victims' networks, "on-site" or "close access" hacking operations were conducted by the conspirators. On-site operations involved trained GRU hackers with sophisticated hacking equipment traveling to victims' locations around the world. These on-site operations often involved targeting the computer networks used by victims organizations or their personnel through Wi-Fi connections, such as hotel Wi-Fi networks, in an effort to gain unauthorized access to the victims' computer networks.

9. Defendants MORENETS and SEREBRIAKOV were two such on-site GRU hackers who traveled to foreign countries with other conspirators, in some instances using Russian government issued diplomatic passports to conduct on-site operations. (See Exhibit A).

10. The intrusions were typically conducted by the conspirators for the purpose of stealing private or otherwise sensitive information.

11. The conspirators thereafter publicly released select items of stolen information under the false auspices of a hacktivist group calling itself the “Fancy Bears’ Hack Team.” The conspirators publicly disseminated the stolen information using online accounts and other infrastructure. These accounts and associated infrastructure were acquired and maintained by GRU Unit 74455.

12. Among the goals of the conspiracy was to publicize stolen information to conduct an influence and disinformation campaign designed to:

- (i) undermine, retaliate against and otherwise delegitimize the efforts of international anti-doping organizations and officials who had publicly exposed Russian government-sponsored doping by Russian athletes;
- (ii) pose as the “Fancy Bears’ Hack Team,” publicize and expose individual sensitive medical information and drug testing results of athletes;
- (iii) damage the reputations of clean athletes from various countries by falsely claiming that such athletes were using banned or performance-enhancing drugs.

THE DEFENDANTS

13. During the timeframe of the conspiracy, ALEKSEI SERGEYEVICH MORENETS (Моренец Алексей Сергеевич) served as a Russian military intelligence officer assigned to Unit 26165. MORENETS was a member of a Unit 26165 team that traveled with technical equipment to locations around the world to conduct on-site hacking operations to target and maintain persistent access to Wi-Fi networks used by victim organizations and personnel. As early as July 2016 and continuing through September 2016, MORENETS targeted U.S. and international anti-doping agencies and sporting federations in Rio de Janeiro, Brazil (July and August 2016, prior to

and during the 2016 Summer Olympics) and Lausanne, Switzerland (September 2016). MORENETS did so by compromising Wi-Fi networks used by anti-doping personnel with access to the networks of USADA, WADA and CCES. Additionally, in April 2018, MORENETS was encountered while conducting an on-site hacking operation targeting the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland.

14. During the timeframe of the conspiracy, EVGENII MIKHAYLOVICH SEREBRIAKOV (Серебряков Евгений Михайлович) served as a Deputy Head of Directorate, Section Chief, assigned to Unit 26165. SEREBRIAKOV was another member of a Unit 26165 team that participated in the on-site hacking operations in Rio de Janeiro, Brazil (August 2016), and Lausanne, Switzerland (September 2016), that targeted USADA, WADA and CCES. In April 2018, SEREBRIAKOV targeted the OPCW in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland.

15. During the timeframe of the conspiracy, IVAN SERGEYEVICH YERMAKOV (Ермаков Иван Сергеевич) served as a Russian military intelligence officer in the GRU assigned to Unit 26165. YERMAKOV conducted technical and online reconnaissance of victim organizations, their employees and their computer networks and thereafter sent spearphishing emails using fictitious personas and proxy servers in an attempt to obscure his identity and GRU affiliation. YERMAKOV also participated in, and provided remote support to, MORENETS' and SEREBRIAKOV's on-site hacking operations, all on behalf of Unit 26165. As early as November 2014 and continuing through at least August 2016, YERMAKOV and his co-conspirators targeted Westinghouse Electric Corporation (WEC) and its employees, in the Western District of

Pennsylvania, WADA and USADA. YERMAKOV is a charged defendant in federal indictment number CR 18-215 in the District of Columbia.

16. During the timeframe of the conspiracy, ARTEM ANDREYEVICH MALYSHEV (Мальшев Артём Андреевич) served as a Senior Lieutenant assigned to Unit 26165. In 2016, MALYSHEV monitored X-Agent malware (a/k/a “Chopstick”) implanted on victim networks and utilized online fictitious personas to conduct technical and online reconnaissance of victim organizations and to send spearphishing emails, all on behalf of Unit 26165. As early as July 2016 and continuing through at least August 2016, MALYSHEV participated in intrusion activities targeting WADA. MALYSHEV is a charged defendant in federal indictment number CR 18-215 in the District of Columbia.

17. During the timeframe of the conspiracy, DMITRIY SERGEYEVICH BADIN (Бадин Дмитрий Сергеевич) was an “Assistant Head of Department” assigned to Unit 26165. In his supervisory role, BADIN oversaw the criminal activities of conspirators as they engaged in computer intrusions and stole credentials, medical records and other data. BADIN also compiled and used malware and other tools to aid in the compromise of victim networks by the conspirators, including the CCES network in September and October 2016. BADIN is a charged defendant in federal indictment number CR 18-215 in the District of Columbia. (Images of defendants YERMAKOV, MALYSHEV and BADIN are attached as Exhibit B).

18. During the timeframe of the conspiracy, OLEG MIKHAYLOVICH SOTNIKOV (Олег Михайлович Сотников) served as a Russian military intelligence officer. SOTNIKOV provided support to his conspirators during their targeting of the OPCW in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland.

19. During the time period of the conspiracy, ALEXEY VALEREVICH MININ (Алексей Валерьевич Минин) served as a Russian military intelligence officer. MININ provided support to MORENETS and SEREBRIAKOV during their targeting of the OPCW in The Hague, Netherlands, and intended to thereafter target the Spiez Swiss Chemical Laboratory in Switzerland. (See Exhibit A, images of SOTNIKOV and MININ).

MANNER AND MEANS OF THE CONSPIRACY

20. The members of the conspiracy, who are both known and unknown to the grand jury, used the following manner and means to accomplish their objectives, which included gaining unauthorized access to computers at entities of interest to the Russian government, including Westinghouse Electric Company (WEC), the U.S. Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), the Canadian Centre for Ethics in Sport (CCES), Court of Arbitration for Sport (TAS/CAS), the International Association of Athletics Federations (IAAF), the Fédération Internationale de Football Association (FIFA), and the Organisation for the Prohibition of Chemical Weapons (OPCW). Conspirators further used that unauthorized access to steal information and, in some instances, publicized the stolen materials to engage in influence and disinformation operations to advance the interests of the Russian government.

21. In order to avoid detection by law enforcement, security researchers and victims, and to mask their GRU affiliation and location in Russia, the conspirators used a variety of fictitious names and personas, as well as online infrastructure, including servers, domains, cryptocurrency, email accounts, social media accounts and other online services provided by companies in the United States and elsewhere. The conspirators used this infrastructure for a wide range of conduct in furtherance of the conspiracy: to communicate, research and probe victims and

their computer networks; to send spearphishing emails; to mimic legitimate domains and websites; to store and distribute additional malware; to manage malware; to transfer stolen data; to publicly release stolen information; to draw public and media attention to such stolen information; and, to negatively influence the perception of such stolen information and the victims. Conspirators used common infrastructure to target multiple victim organizations and individuals. For example, the conspirators utilized approximately 38 common IP addresses to conduct the intrusion activities at both WADA and USADA, and much of the stolen information from all of the anti-doping-related victims was posted and disseminated through the social media accounts or website of the Fancy Bears' Hack Team, fancybear.net and fancybear.org.

22. In those instances where conspirators purchased hacking infrastructure, payments were made using a complex web of transactions involving operational accounts in fictitious names and typically utilized cryptocurrencies, such as Bitcoin, to further mask their identities and conduct.

23. The conspirators typically initiated their hacking activities by researching the victim organizations, including their computer networks and employees. This research provided technical and biographical information that the conspirators could exploit in subsequent intrusion activities.

24. The conspirators also registered domain names for use in their hacking activities. Examples include “westinqhousenuclear.com” (deliberately substituting a “q” for a “g,”), “wada.awa.org” and “wada.arna.org” (WADA’s legitimate domain was “wada.ama.org”). These domains were intended to mimic or “spoof” those of legitimate websites that victims were familiar with, including webmail login pages, VPN login screens or password reset pages.

25. Frequently, the conspirators crafted email messages known as “spearphishing,” designed to trick unwitting recipients into giving the conspirators access to their computers and account credentials (e.g., a username and password). Spearphishing messages were composed to resemble emails from trustworthy senders, such as email providers or colleagues, and requested the recipients to click on hyperlinks in the messages. Such hyperlinks would direct recipients to spoofed websites which prompted the recipients to enter their login and password and enabled the capture of their credentials. In many cases, the hyperlinks were created using an online service (e.g., Bit.ly) that abbreviated lengthy website addresses (referred to as a “URL-shortening service”). In other cases, the hyperlinks were domains that the conspirators registered for a fee with online providers, such as “wada.awa.org,” and “wada.arna.org.”

26. When the conspirators’ remote hacking efforts failed to capture log-in credentials, or if those accounts that were successfully compromised did not have the necessary access privileges for the sought-after information, teams of GRU intelligence officers traveled to locations around the world where targets were physically located. Using specialized equipment, and with the remote support of conspirators in Russia, these on-site teams hacked into Wi-Fi networks used by victim organizations or their personnel, including hotel Wi-Fi networks. After a successful hacking operation, the on-site, or close access, team transferred such access to conspirators in Russia.

27. The conspirators developed and utilized malware and hacking tools, including “Gamefish,” “X-agent” (a/k/a “Chopstick”), “X-tunnel,” “Remcomsvc,” and “Responder.exe,” in order to hack and compromise victim computers and networks, to maintain command and control over such networks, and to steal network credentials and other sensitive and private data.

28. After hacking into victim computers, remotely or aided by the on-site teams, the conspirators performed a variety of functions designed to identify, collect, package and steal targeted data from the victims' computers. In instances where the hacking was part of an influence or disinformation operation, conspirators publicly posted and disseminated such information, including victims' personal email communications and individual health and medical information. In some instances, such information was modified from its original form. Thereafter, the conspirators would actively solicit and promote media coverage so the stolen information would receive international attention. This was done to further a narrative favorable to the Russian government and in order to amplify its impact.

COMPUTER INTRUSIONS and OTHER OVERT ACTS

Westinghouse Electric Company (WEC)

29. At all times during the conspiracy, WEC was a U.S.-based nuclear power developer, with its headquarters outside of Pittsburgh, Pennsylvania, that provided fuel, services and plant design to international customers in the commercial nuclear industry. All of WEC's internet traffic is routed through servers located in the Western District of Pennsylvania. The company's power plant designs are the basis for approximately half of the world's currently operating nuclear power plants. Since 2008, WEC has supplied Ukraine with increasing amounts of nuclear fuel.

30. As early as November 20, 2014, IVAN SERGEYEVICH YERMAKOV performed technical reconnaissance of WEC, WEC-related IP addresses, network ports and associated domains. On December 8, 9, and 22, 2014, YERMAKOV's reconnaissance included research on WEC, its employees, and their background in nuclear energy research and development.

31. On December 10, 2014, YERMAKOV and his co-conspirators registered a fake domain and website, “https://webmail.westinghousenuclear.com” to mimic a legitimate WEC domain. Spearphishing emails were sent to at least five WEC employees, designed to appear as routine emails from the Westinghouse.com Microsoft Exchange Server. Upon clicking an enclosed link, users were directed to the spoofed domain where their login credentials were stolen and saved. Once stolen credentials were determined to be authentic by the conspirators, victims were then re-routed to the original, legitimate WEC network so that they were unaware that the theft of their passwords had occurred.

32. Following the targeting of WEC corporate accounts, on December 24, 2014, January 15, 2015, January 17, 2015 and November 18, 2015, using Bit.ly accounts, YERMAKOV and conspirators sent spearphishing emails to the personal email accounts of four WEC employees who resided near Pittsburgh, Pennsylvania. The users of two of the accounts clicked on the malicious link which would have enabled the theft of the login credentials to their personal email accounts. These employees worked in the nuclear energy field and were involved in advanced nuclear reactor development and new reactor technology.

World Anti-Doping Agency (WADA)

33. WADA was established under the initiative of the International Olympic Committee (IOC) in 1999 as an international independent agency, which is composed of and funded equally by the sports movement and governments of the world. WADA, which is headquartered in Montreal, Canada, administers the World Anti-Doping Code – the document harmonizing anti-doping policies in all sports and all countries - and coordinates anti-doping activities internationally through its central drug testing clearinghouse, the Anti-Doping

Administration and Management System (ADAMS) database. The ADAMS database contains laboratory results of drug tests and location information for nearly 30,000 athletes in addition to records related to the granting or denial of therapeutic use exemptions (TUEs) for otherwise prohibited substances. Athletes whose medical information resides in the ADAMS database reside throughout the world, including in the Western District of Pennsylvania.

34. In 2014, a German documentary titled, “Top Secret Doping: How Russia Makes its Winners,” aired interviews of husband and wife Russian whistleblowers who admitted to participation in the Russian state-sponsored doping program as an anti-doping official and athlete, respectively. Shortly thereafter, WADA launched an Independent Commission (IC) to investigate the validity of the allegations. In a November 2015 report, the WADA IC released its findings, namely, it “confirmed the existence of widespread cheating through the use of doping substances and methods to ensure, or enhance the likelihood of, victory for [Russian] athletes and teams.” The IC made “specific findings” regarding the involvement of the Russian Federal Security Service (FSB) in Russia’s efforts to evade anti-doping procedures and protections.

35. In May 2016, a prominent television newsmagazine and newspaper each published stories regarding allegations from the husband and wife whistleblowers, as well as a new Russian whistleblower who had previously managed Russia’s anti-doping laboratory. The whistleblowers all alleged a Russian state-sponsored doping effort at the 2014 Sochi Winter Olympics. In response, WADA named an “independent person” (IP) to investigate their allegations.

36. On July 18, 2016, the WADA-appointed IP published his first report, the “McLaren Report,” regarding Russia’s systematic state-sponsored subversion of the drug testing processes prior to, during and subsequent to the 2014 Sochi Winter Olympics. WADA’s Executive

Committee issued a statement accompanying this report, which recommended that the IOC and the International Paralympic Committee (IPC) “decline entries for Rio [Olympics and Paralympics] 2016, of all athletes submitted by the Russian Olympic Committee (ROC) and the Russian Paralympic Committee.” Beginning that same day, multiple IP addresses were used to scan WADA’s network for vulnerabilities or potential access points.

37. On July 24, 2016, the IOC Executive Board announced a “preliminary decision” (later affirmed by the broader IOC) that, as a result of the WADA IP’s report, individual sporting federations could exclude Russian athletes from the 2016 Rio Summer Olympics, with each positive decision having to be approved by an arbitrator from the international Court of Arbitration for Sport (TAS/CAS). Ultimately, 111 Russian athletes were barred from participation in the Olympics. The IPC issued a blanket ban of Russian athletes for the 2016 Rio Summer Paralympics.

38. The next day, on July 25, 2016, conspirators launched a Distributed Denial-of-Service (DDoS) attack against, and vulnerability scan, of WADA’s official website: wada-ama.org.

Compromise of WADA’s Computer Networks

39. On August 2, 2016, conspirators used multiple IP address to connect to or scan WADA’s network. Such activity continued on August 4, 5, 8 and 9, 2016.

40. Also on August 2, 2016, defendant YERMAKOV researched WADA and password recovery requirements for WADA’s ADAM’s database.

41. On August 3, 2016, conspirators registered the domain “wada.awa.org” using an email account and a fictitious name. This registered domain spoofed, or falsely mimicked, WADA’s legitimate domain: wada-ama.org.

42. On August 3 and 4, 2016, defendant YERMAKOV researched WADA and ADAMS, as well as exploits and other hacking techniques.

43. On August 4, 2016, conspirators, including defendant MALYSHEV, sent spearphishing emails to eleven WADA employees, appearing to be from the WADA Chief Technology Officer, which prompted the employees to click on the link to authenticate their WADA email accounts. In fact, the link was designed to steal WADA employee login credentials. Approximately four WADA employees clicked on the malicious link which enabled conspirators to steal their login account credentials, which were later used to access their WADA accounts.

44. On August 5, 2016, defendant YERMAKOV conducted research regarding WADA, the WADA-appointed IP, the McLaren Report and CISCO firewalls. This included research of a specific WADA employee, including his or her LinkedIn profile. Minutes later, conspirators created a link embedding that employee’s email address using the URL-shortening service Bit.ly, and a corresponding spearphishing email was sent to the victim’s email account. The employee clicked on the malicious link which was designed to allow defendant YERMAKOV and the conspirators to harvest his or her log-in credentials and gain access to his or her emails. Over the course of the conspirators’ targeting of WADA, this Bit.ly account created links for the personal email accounts of at least four WADA employees.

45. On August 8, 2016, conspirators registered the domain “wada-arna.org” using an email account and a fictitious name. This registered domain spoofed, or falsely mimicked, WADA’s legitimate domain: wada-ama.org.

46. That same day, and again on August 9, 2016, defendant YERMAKOV continued research targeting WADA employees. He also prepared to send spearphishing emails, by composing English-language draft emails and by researching information regarding CISCO security updates, CISCO access and privilege escalation. On August 9, 2016, defendant MALYSHEV also prepared to send spearphishing emails by conducting research and reviewing a draft spearphishing email.

47. On August 9, 2016, defendants YERMAKOV and MALYSHEV sent spearphishing emails written to appear as if they were from a WADA IT Manager to WADA employees prompting them to click on a link to “update their Cisco client.” At least one WADA employee clicked on the link and entered his or her login credentials.

Compromise of WADA’s
Computer Networks Through On-Site Operations

48. Conspirators made two operational trips to Rio de Janeiro, the site of the 2016 Summer Olympics and Paralympics, to conduct hacking operations targeting and maintaining persistent access to Wi-Fi networks used by anti-doping officials. First, from July 10 through July 19, 2016, prior to the Olympics, defendant MORENETS traveled to Rio. Second, from August 13, 2016 to August 19, 2016, during the Olympics, defendants MORENETS and SEREBRIAKOV traveled together to Rio.

49. During defendants MORENETS’ and SEREBRIAKOV’s second trip to Rio, defendant YERMAKOV provided remote support to their close access operation. For example,

on August 13 and 14, 2016, defendant YERMAKOV conducted research concerning an identified hotel chain that hosted Olympics officials, including IOC, TAS/CAS, WADA and USADA officials. Within minutes, defendant YERMAKOV also researched the routers used by some of those hotels for Wi-Fi access and methods of exploiting those routers, including through “brute force” password cracking.

50. On August 19, 2016, approximately 15 hours before defendants MORENETS’ and SEREBRIAKOV’s departure from Rio, an identified IOC anti-doping official used his or her administrator credentials to log into WADA’s ADAMS database from a Brazilian IP address. The conspirators captured that IOC official’s username and password and thereafter used them, and another set of ADAMS credentials belonging to the same official that was created specifically for anti-doping officials at the Rio Olympic games, to gain unauthorized access to the ADAMS database and medical and anti-doping-related information available to those accounts. The broader ADAMS database was not compromised in the attack. The conspirators conducted large-scale exports of data from WADA’s networks on August 29, 2016 and September 6, 2016.

Tribunal Arbitral du Sport/Court of Arbitration for Sport (TAS/CAS)

51. TAS/CAS is an independent institution based in Lausanne, Switzerland, which resolves sports-related legal disputes through arbitration. In this capacity, TAS/CAS was involved in the Russian doping scandal, including a July 21, 2016 decision to uphold the suspension by IAAF of the All-Russia Athletics Federation and the July 24, 2016 decision by the IOC that individual sporting confederations could ban Russian athletes from the Rio Olympics, with the approval of a TAS/CAS arbitrator. On July 26, 2016, TAS/CAS established an *ad hoc* tribunal to

resolve disputes at the Rio Olympics, which was located at a Rio hotel operated by the hotel chain described herein as having been targeted by defendant YERMAKOV.

52. On August 8, 2016, the conspirators used the same email account and fictitious name that was used to register the spoofed “wada-arna.org” domain to register a second domain “tas-cass.org.” The registered domain falsely mimicked TAS/CAS’ legitimate domain: tas-cas.org.

53. One day later, on August 9, 2016, defendants MALYSHEV and YERMAKOV conducted online reconnaissance efforts targeting TAS/CAS email accounts and made other preparations for sending spearphishing emails.

U.S. Anti-Doping Agency (USADA)

54. USADA is the national anti-doping organization in the United States for Olympic and Paralympic Sports. USADA implements a national anti-doping program that includes athlete testing and also oversees therapeutic use exemptions (TUEs) for prohibited substances, consistent with the World Anti-Doping Code and in coordination with WADA and the IOC. Like WADA, USADA maintains thousands of sensitive, confidential records regarding the location of United States athletes, their drug testing history and results and TUEs. USADA is headquartered in Colorado Springs, Colorado.

55. During the timeframe of the conspiracy, USADA leadership was publicly outspoken regarding its concern about state-sanctioned doping among Russian athletes and advocated for a ban of Russian athletes from the 2016 Rio Olympics. This included cooperative efforts with CCES and other national anti-doping agencies in July 2016 to make a concerted push for a ban upon the anticipated release of the WADA McLaren Report. USADA was also a vocal

critic of the IOC's July 24, 2016 decision not to institute a full ban on Russian athletes participating in the 2016 Rio Olympics, releasing a statement that, "the decision regarding Russian participation and the confusing mess left in its wake is a significant blow to the rights of clean athletes."

56. On August 2, 2016, defendant YERMAKOV conducted research of USADA.

57. On August 14, 2016, conspirators began efforts to compromise USADA's network, including through "SQL injection" attacks against USADA's "ufcathlete.usada.org" website from multiple IP addresses (SQL injection attacks are a hacking technique that involved typing commands in the website's fields in order to tamper with, steal or gain unauthorized access to a database). USADA also administers the anti-doping program for the Ultimate Fighting Championship (UFC) and specifically maintains a Russian language option for its UFC athletes. These attacks, which consisted of 24,227 SQL injection attempts from 62 different sources, continued intermittently until August 18, 2016, and used some of the same infrastructure from similar attacks against WADA during the same time frame. The SQL injection attacks, as captured on USADA logs, show that the hackers attempted to use the "change language" function to switch from English to Russian.

58. In late August 2016, a senior USADA anti-doping official traveled to Rio de Janeiro, Brazil for the Olympics and Paralympic games. At that time, the USADA official served on the IPC which had unanimously suspended Russia from official participation in the 2016 Rio Paralympics. A number of anti-doping officials stayed at a Rio hotel operated by the hotel chain described herein as having been targeted by defendant YERMAKOV. Throughout his or her stay, the USADA official used Wi-Fi at his or her hotel and other Wi-Fi access points in Rio to remotely access USADA's computer systems and conduct official business via his or her portable electronic

devices.

59. On August 19 and 25, 2016, conspirators sent spearphishing emails to the personal account of an officer serving on the USADA Board of Directors. The emails contained a malicious link that was created by the same Bit.ly account used to send spearphishing emails to WADA employees in August 2016.

60. On September 6, 2016, while the USADA official was still in Rio, conspirators successfully compromised the credentials for his or her USADA VPN account and Office 365 Exchange mailbox, the latter of which contained all of his or her emails. At that time, the USADA official's account contained over 90,000 messages and an estimated 10 gigabytes of data, which included summaries of athlete test results and prescribed medications.

61. The conspirators subsequently attempted to use the USADA official's credentials to gain unauthorized access to 33 separate USADA systems between September 7 and 14, 2016. These attempts were ultimately unsuccessful.

Canadian Centre for Ethics in Sport (CCES)

62. CCES is the national anti-doping organization for Canada and oversees the implementation and management of Canada's Anti-Doping Program. During the timeframe of the conspiracy, CCES coordinated drug testing and analysis, assured adherence to the World Anti-Doping Code and considered exemptions for athletes with medical conditions. The headquarters for CCES are in Ottawa, Canada.

63. During the conspiracy, CCES leadership spoke out publicly against Russia's state-sponsored doping program and joined with USADA in support of a ban for the Rio Olympics and beyond. On September 19, 2016, CCES issued a media release condemning the hacking of WADA

and the athlete information in the ADAMS database, as well as the public posting of such information.

64. In mid-September 2016, a senior CCES official traveled to Lausanne, Switzerland for a WADA-hosted anti-doping conference. Conference proceedings and lodging were hosted at a specific hotel in Lausanne (Lausanne Hotel 1), which offered Wi-Fi for its guests. During this trip, the CCES official traveled with a laptop computer, stayed at Lausanne Hotel 1 and used the hotel Wi-Fi connection to access the internet and conduct official business.

65. On September 18, 2016, defendants MORENETS and SEREBRIAKOV traveled to Lausanne, Switzerland, with defendant SEREBRIAKOV staying in Lausanne Hotel 1, and defendant MORENETS staying in a second hotel in close proximity (Lausanne Hotel 2), which was also hosting anti-doping officials as guests. Both reservations were for four nights. Defendants MORENETS and SEREBRIAKOV were at the time in possession of equipment used for on-site or close access Wi-Fi compromises.

66. On September 19, 2016, while the CCES official was staying at Lausanne Hotel 1 and connected to the hotel's Wi-Fi network, defendants MORENETS and SEREBRIAKOV, together with co-conspirators, compromised the hotel Wi-Fi network to gain unauthorized access to the CCES official's laptop. Using that access, the conspirators accessed the CCES official's emails and placed, or attempted to place, malware, namely Gamefish, X-agent, X-Tunnel, Remcomsvc, and Responder.exe, onto the laptop.

67. On September 20, 2016, while at Lausanne Hotel 1, the CCES official happened to check the "Sent items" email folder on his laptop. In the folder, he or she found a message to the Chief Medical Officer of another international sporting organization that he or she had neither

composed nor sent. The message contained several blatant typographical errors and inaccurately attempted to mimic the cell phone signature line of the CCES officer: “Sent from my SamsunCopenhagen.” The message also contained what appeared to be an embedded malicious link.

68. Starting on September 20, 2016, the conspirators, using the CCES official’s credentials, moved laterally from the CCES official’s laptop to CCES’ computer network in Canada. The conspirators maintained access to, and installed tools and malware Gamefish, X-agent, and Remcomsvc, on the CCES network until at least October 24, 2016, when CCES took its network offline.

69. Forensic evidence obtained from CCES revealed that the conspirators had used a file named “vsc.exe,” which was a tool used to extract hashed passwords from a victim computer network. Analysis of the metadata of this tool revealed that it had been compiled by defendant DMITRIY SERGEYEVICH BADIN.

International Association of Athletics Federations (IAAF)

70. The IAAF is an international sports federation that governs track-and-field competitions and related standardized technical equipment and official world records. During the timeframe of the conspiracy, the IAAF maintained an anti-doping department and staff, which was transitioned into a newly-formed IAAF “Athletics Integrity Unit” (AIU) in April 2017. Even before the establishment of the AIU, IAAF’s anti-doping staff were responsible for all aspects of the anti-doping program for international-level athletes, including education, testing, intelligence gathering, investigations, results management, prosecutions and appeals. The IAAF is headquartered in the Principality of Monaco.

71. On November 13, 2015, shortly after WADA released its first report, the Council of the IAAF provisionally suspended the membership of the All-Russia Athletics Federation (ARAF) in response to allegations of Russian state-sponsored doping allegations. On July 21, 2016, TAS/CAS upheld ARAF's suspension and Russian track-and-field athletes were barred from the 2016 Rio Olympics. Since that time, IAAF has continued the suspension, in part due to the refusal by ARAF and Russian sporting officials to acknowledge the McLaren Report's findings.

72. From January 19 to 24, 2017, three weeks before the IAAF was to release a recommendation regarding ARAF's reinstatement, the conspirators compromised the computers of at least four IAAF officials, including the head of IAAF's anti-doping department. Specifically, through malware placed on the IAAF network, including X-agent, the conspirators were able to review keylogger results, monitor Skype communications and access file directories. Prior to these specific events, the command and control infrastructure for the IAAF X-agent malware was managed from an IP address frequently used by MALYSHEV.

Fédération Internationale de Football Association (FIFA)

73. FIFA is an international sports federation that governs football (soccer). During the timeframe of the conspiracy, FIFA maintained a Medical and Anti-Doping Unit that directly administered the anti-doping programs for all FIFA competitions through a worldwide network of doping control officers. FIFA is headquartered in Zurich, Switzerland.

74. A second, more detailed report released by WADA on December 9, 2016 (the "Second McLaren Report") included evidence that Russian football players may have been involved in the state-sponsored doping scandal. As a result, FIFA announced an investigation.

75. From at least December 6, 2016 to January 2, 2017, the conspirators compromised a computer belonging to the head of FIFA's Medical and Anti-Doping Unit. Specifically, through malware placed on the computer, including X-agent, the conspirators downloaded more than 100 documents related to the First and Second McLaren Reports, including supporting evidence, FIFA's anti-doping policy and strategy, lab results, medical reports, contracts with doctors and medical testing labs, information about medical testing procedures and TUEs. Prior to these specific events, the command and control infrastructure for the X-agent malware was managed from an IP address frequently used by defendant MALYSHEV.

Influence and Disinformation Operations Using Stolen Information

76. Beginning on or about September 1, 2016, and continuing in separate installments through May 2018, the conspirators, falsely claiming to be the hacktivist group Fancy Bears' Hack Team, used online accounts and other infrastructure procured and managed, at least in part, by conspirators in GRU Unit 74455 to release data stolen from WADA, USADA, CCES, TAS/CAS, IAAF, and FIFA, as well as data that appeared to be stolen from 35 other anti-doping agencies or sporting organizations. Such data was available to and viewed by residents in the Western District of Pennsylvania.

The Public Release of Stolen Information

77. The domains fancybear.org and fancybear.net were registered on September 1, 2016. On September 12, 2016, data stolen from WADA and its ADAMS database by conspirators first appeared on fancybear.net, including medical information for individual athletes, and private, official email communications. Although the initial disseminations focused on U.S. athletes, subsequent releases of stolen data included records of nearly 250 athletes from almost 30 countries.

These athlete records from WADA included testing history and TUEs for an athlete and resident of the Western District of Pennsylvania. Many of the WADA documents released by the conspirators did not accurately reflect their original form. On fancybear.net, individual athletes were named, categorized by nationality and sport, and identified as having such personal diagnoses as “ADD” (attention deficit disorder), “drug addiction,” “diabetes insipidus,” or “circulatory collapse.” As one example, an athlete’s stolen record was posted, listing the athlete’s date of birth, sport, nationality, the daily dose and manner of administration of a prescribed therapeutic substance, approving physician and the results of a recent (urine) drug test.

78. On or about October 6, 2016, emails and data that conspirators stole from USADA were released on fancybear.net. The records included personal medical information, such as testing histories and TUEs, for multiple athletes, including an athlete and resident of the Western District of Pennsylvania.

79. On December 13, 2016, emails and data that conspirators stole from CCES network were released on fancybear.net.

80. On or about June 22, 2017, and July 5, 2017, emails and data that conspirators stole from IAAF’s network were released on fancybear.net, including emails about doping violations of non-Russian athletes.

81. On August 28, 2017, emails and data that that conspirators stole from FIFA’s network were released on fancybear.net, including lists of players who were provided TUEs before the 2010 World Cup, a list of failed drug tests, and emails between FIFA and anti-doping officials.

The Conspirators Sustained Media Campaign

82. The conspirators released this stolen information to further one of the objectives of the conspiracy, namely to undermine and retaliate against international anti-doping officials who had exposed the Russian state-sponsored doping program at the 2014 Sochi Winter Olympics and other competitions.

83. In some instances, the Fancy Bears' Hack Team's posts and other communications parroted or supported themes that were already found in the Russian government's narrative. The following are examples of official Russian statements regarding the investigative findings:

- a. On August 2, 2016, the President of the Olympic Committee of Russia claimed that “[w]e are witnessing the direct interference of politics in sport”;
- b. On August 21, 2017, the Russian Minister of Sport and the President of the Olympic Committee of Russia indicated in a joint letter to the IOC that “the problem of doping is faced not only by Russia”; and
- c. On or about February 11, 2018, the Russian Foreign Minister claimed that the accusations of state-sponsored doping were orchestrated by the United States “because they can’t beat us fairly.”

84. The Fancy Bears' Hack Team, on fancybear.net, made similar misleading statements, such as:

- a. “U.S. and Canada Sports Officials’ Secret Plot Revealed”; and
- b. Canada and the United States “tried to further their political interests pretending to fight for clean sport”;
- c. “We have proof of American athletes taking doping”; and

- d. “WADA has failed to be a viable and trusted anti-doping organization because its leadership and [national anti-doping agencies’] chiefs follow Anglo-Saxon political agenda.”

85. Between September 12, 2016 and at least January 17, 2018, the conspirators engaged in a concerted effort to draw media attention to the leaks through a proactive outreach campaign that went beyond its public social media posts. During that timeframe, the @fancybears and @fancybearHT Twitter accounts sent direct messages to the Twitter accounts of approximately 116 reporters around the world advertising the stolen information.

86. Similarly, between September 19, 2016, and July 20, 2018, the conspirators, using the Fancy Bears’ Hack Team persona, exchanged e-mails with approximately 70 reporters around the world. The only condition set forth by the conspirators in such exchanges was that reporters were required to refer to the Fancy Bears’ Hack Team by name in the story and later provide a link to the story back to the conspirators. In some cases, reporters pressed for and received promises of exclusivity in such reporting, with one such reporter attempting to make arrangements for a right of first refusal for articles on all future leaks and actively suggesting methods with which the conspiracy could search the stolen materials for documents of interest to that reporter (e.g., keywords of interest).

87. After the articles were published, conspirators used the Fancy Bears’ Hack Team social media accounts to draw attention to the articles, in an apparent attempt to amplify the exposure and effect of their message.

Organisation for the Prohibition of Chemical Weapons (OPCW)

88. The OPCW is the body that implements the Chemical Weapons Convention of

1997 and includes 193 member nations, including the United States. On April 7, 2018, the OPCW Executive Council convened at its headquarters in The Hague to discuss the use of toxic chemical weapons in Syria. Also, in April 2018, including on or about April 11 and 12, OPCW transmitted statements regarding its investigation of the March 4, 2018 poisoning of a former GRU officer and another Russian national in the United Kingdom with a chemical nerve agent.

89. On April 10, 2018, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, all using Russian diplomatic passports, traveled to The Hague in the Netherlands in furtherance of another on-site operation. According to a taxi receipt found on his person, prior to his departure from Moscow on April 10, 2018, defendant MORENETS traveled by taxi from Nesvizhsky Pereulok, a street located at the rear entrance of GRU headquarters for Unit 26165, directly to Sheremetyevo Airport. (See Exhibit C).

90. Upon their arrival in the Netherlands, an identified official from the Russian Embassy escorted defendants MORENETS, SEREBRIAKOV, SOTNIKOV and MININ through customs. All four thereafter checked into a hotel situated adjacent to the OPCW headquarters in The Hague.

91. On April 11, 2018, defendants SOTNIKOV and MININ rented a car and thereafter assembled and secreted technical hacking equipment in the car's trunk. The technical equipment was capable of several techniques, including long-distance, surreptitious interception of Wi-Fi signals, as well as harvesting of Wi-Fi user credentials. The next day, all four defendants checked into a second hotel located adjacent to the OPCW headquarters in The Hague.

92. On April 13, 2018, defendants MORENETS, SEREBRIAKOV, SOTNIKOV and

MININ parked the rental car adjacent to the OPCW property, with the trunk facing the OPCW. (See Exhibit D). The hacking equipment was deployed with an antenna (covered by a jacket) aimed at the nearby headquarters of the OPCW and configured so that it could be controlled by either an attached laptop computer or through a remote 4G connection. (See Exhibit E).

93. After the GRU team activated the equipment, the Dutch defence intelligence service (Militaire Inlichtingen en Veiligheidsdienst or MIVD) disrupted the GRU team's operation. As a result, the conspirators abandoned their equipment, including defendant SEREBRIAKOV's backpack. This backpack contained additional technical equipment that the team could also use to surreptitiously intercept Wi-Fi signals and traffic, including a "Wi-Fi Pineapple." (See Exhibit F). At least one item of equipment in defendant SEREBRIAKOV's possession contained technical data indicating that it had been used to connect to hotel Wi-Fi at Lausanne Hotels 1 and 2, where defendants MORENETS and SERBRIAKOV had stayed in Switzerland on September 20-22, 2016, (the dates they conducted the Wi-Fi compromise of the senior CCES official's laptop at the same hotel), as well as multiple other international destinations, including a hotel in Kuala Lumpur, Malaysia, in December 2017. Defendant SEREBRIAKOV's equipment was also found to have contained an image that placed him at the 2016 Summer Olympics in Rio on August 14, 2016. (See Exhibit G).

94. Further data on defendant SEREBRIAKOV's equipment indicated that, on April 9, 2018, he had conducted online searches of the Spiez Swiss Chemical Laboratory, an accredited laboratory of the OPCW for conducting analysis of military chemical agents, including the chemical agent that United Kingdom authorities connected to the poisoning of the former GRU officer in the United Kingdom. Defendants MORENETS, SEREBRIAKOV, SOTNIKOV and

MININ had earlier purchased train tickets from The Hague to Bern, Switzerland, dated April 17, 2018, in order to continue their operational deployment to target the Spiez laboratory.

STATUTORY ALLEGATIONS

95. Beginning at least in or about 2014 and continuing until at least in or about May 2018, the exact dates being unknown to the Grand Jury, in the Western District of Pennsylvania and elsewhere, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, did knowingly and intentionally combine, conspire, confederate, and agree together, with each other and with others known and unknown to the grand jury, to commit offenses against the United States, namely:

- a. to access a computer without authorization and exceed authorized access to a computer, and to obtain thereby information from a protected computer, in furtherance of a criminal and tortious act in violation of the laws of the Commonwealth of Pennsylvania, namely, the common law tort of Invasion of Privacy, and where the value of the information did, and would if completed, exceed \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B);
- b. to cause the transmission of a program, information, code, and command, and as a result of such conduct, to cause damage without authorization to a protected computer, and where the offense did cause and would, if completed, have caused, loss aggregating \$5,000 in value to at least one person during a one-year

period from a related course of conduct affecting a protected computer, and damage affecting at least 10 protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B); and, All in violation of Title 18, United States Code, Section 371.

COUNT TWO
(Wire Fraud Conspiracy)

The grand jury further charges:

96. The allegations contained in Paragraphs 1 through 94 of this indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

THE CONSPIRACY AND ITS OBJECTS

97. From at least approximately 2014, and continuing thereafter to in and around April 2018, in the Western District of Pennsylvania and elsewhere, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, knowingly and willfully did conspire, combine, and agree to commit an offense against the United States, that is, wire fraud, contrary to the provisions of Title 18, United States Code, Section 1343, to wit:

the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, together with conspirators, having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, did transmit and cause to be transmitted by means of wire

communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice.

98. Specifically, an object of the conspiracy was to gain unauthorized access into the computer networks of Westinghouse Electric Company (WEC), the U.S. Anti-Doping Agency (USADA), the World Anti-Doping Agency (WADA), and the Canadian Center for Ethics in Sport (CCES) as well as the personal and business email accounts of their respective employees, in order to steal user login credentials and passwords, email communications, personally identifiable information, sensitive medical information of international athletes, proprietary information, data, property and other information of value, by means of false and fraudulent pretenses, to further the interests of the Russian Federation.

99. In order to gain unauthorized access to victims' email accounts and computer networks, defendants IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, ALEKSEI SERGEYEVICH MORENETS and EVGENII MIKHAYLOVICH SEREBRIAKOV, together with their conspirators, crafted and transmitted, in interstate and foreign commerce, spearphishing emails that targeted the victims. The spearphishing emails were designed to appear legitimate in order to deceive recipient victims into opening the email and clicking on a malicious attachment or link that, when clicked, enabled the conspirators to steal the victims' login credentials to gain access to the victims' networks. The malicious links included "spoofed," or mimicked, domains that resembled legitimate websites associated with the victim entities. For example, the conspirators registered the domain "Westinghousenuclear" on December 10, 2014, "wada.awa.org" on August 3, 2016, and "wada.arna.org," and "tas-cass.org"

on August 8, 2016, and thereafter utilized those spoofed domains in furtherance of the fraud scheme.

All in violation of Title 18, United States Code, Sections 1349 and 3559(g)(1).

COUNTS THREE THROUGH SEVEN

(Wire Fraud)

The grand jury further charges:

100. The allegations contained in Paragraphs 1 through 94 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

101. On or about the dates set forth below, in the Western District of Pennsylvania and elsewhere, the defendant, IVAN SERGEYEVICH YERMAKOV, having devised and intending to devise a scheme and artifice to defraud, and to obtain property by means of false and fraudulent pretenses, representations and promises, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, and pictures for the purpose of executing such scheme and artifice; to wit, the defendant did knowingly transmit spearphishing emails, designed to appear legitimate, that contained malicious Bit.ly links, to the personal email accounts of the victims identified below, all employees of Westinghouse Electric Company (WEC), on or about the dates set forth below, with the intention of obtaining the victims' account login credentials, with each such transmission being a separate count of this indictment:

Count	Approx. Date	Victim	Bit.ly Link	Bit.ly Account
3	December 24, 2014	A	http://bit.ly/16Q0fWb	activqwe
4	December 24, 2014	B	http://bit.ly/1xb8Efq	activqwe
5	December 24, 2014	C	http://bit.ly/13vFZqx	activqwe
6	January 17, 2015	D	http://bit.ly/1CiXN3W	activqwe
7	January 17, 2015	E	http://bit.ly/1Cz3Fqk	activqwe

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS EIGHT AND NINE
(Aggravated Identity Theft)

The grand jury further charges:

102. The allegations contained in Paragraphs 1 through 94 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

103. Beginning in at least November 2014 and continuing until at least September 2016, in the Western District of Pennsylvania and elsewhere, the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV and DMITRIY SERGEYEVICH BADIN, aided and abetted by others known and unknown to the grand jury, 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 Title 18, United States Code, Section 1028A(c), namely, conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349, knowing that the means of identification belonged to another real person who worked on behalf of the targeted victim organizations: Westinghouse Electric Company and the U.S. Anti-Doping Agency (USADA).

Count	Approx. Date	Victim Org.	Means of Identification
8	From November 2014- January 2015	WEC	Username and passwords for multiple employee accounts
9	September 6, 2016	USADA	Login credentials for USADA official

In violation of Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028(c)(4) and 2.

COUNT TEN

(Conspiracy to Commit Money Laundering)

The grand jury further charges:

104. The allegations contained in Paragraphs 1 through 94 of this Indictment are repeated, re-alleged, and incorporated by reference as if fully set forth herein.

105. To facilitate the purchase of infrastructure used in their hacking activity—targeting anti-doping and other sports-related organizations and releasing the stolen documents—defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, together with conspirators known and unknown, conspired to launder money through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin.

106. Although the conspirators caused transactions to be conducted in a variety of currencies, including U.S. dollars, they principally used bitcoin when purchasing servers, registering domains, and otherwise making payments in furtherance of hacking activity. Many of these payments were processed by companies located in the United States that provided payment processing services to hosting companies, domain registrars, and other vendors both international and domestic. The use of bitcoin allowed the conspirators to avoid direct relationships with traditional financial institutions, allowing them to evade greater scrutiny of their identities and sources of funds.

107. All bitcoin transactions are added to a public ledger called the Blockchain, but the Blockchain identifies the parties to each transaction only by alpha-numeric identifiers known as

bitcoin addresses. To further avoid creating a centralized paper trail of all of their purchases, the conspirators purchased infrastructure using hundreds of different email accounts, in some cases using a new account for each purchase. The conspirators used fictitious names and addresses in order to obscure their identities and their links to Russia and the Russian government. For example, the wada.arna.org, tas-cass.org domains and an associated virtual private server were registered and paid for using the fictitious name “Beula Town.”

108. The conspirators used several dedicated email accounts to track basic bitcoin transaction information and to facilitate bitcoin payments to vendors. One of these dedicated accounts received hundreds of bitcoin payment requests from approximately 100 different email accounts. For example, on or about August 8, 2016, the account received the instruction to “[p]lease send exactly 0.012684 bitcoin to” a certain thirty-four character bitcoin address. Shortly thereafter, a transaction matching those exact instructions was added to the Blockchain.

109. On occasion, the conspirators facilitated bitcoin payments using the same computers that they used to conduct their hacking activity, including to create and send test spearphishing emails.

110. The conspirators funded the purchase of computer infrastructure for their hacking activity in part by “mining” bitcoin. Individuals and entities can mine bitcoin by allowing their computing power to be used to verify and record payments on the bitcoin public ledger, a service for which they are rewarded with freshly-minted bitcoin. The pool of bitcoin generated from the GRU’s mining activity was used, for example, to pay a United States-based company to register the domain wada-arna.org through a payment processing company located in the United States.

111. The conspirators used the same funding structure—and in some cases, the very same pool of funds—to purchase key accounts, servers, and domains used in their anti-doping-related hacking activity. For example, the conspirators used the same pool of bitcoins to fund two operational personas which, in turn, registered the domains wada-arna.org (to target WADA), tas-cass.org (to target TAS/CAS) and the domains upmonserv.net and appexrv.com, used for command and control of X-agent malware installed on CCES network.

STATUTORY ALLEGATIONS

112. From at least in or around 2015 through 2016, within the Western District of Pennsylvania and elsewhere, defendants ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, together with others, known and unknown to the grand jury, did knowingly and intentionally conspire to transport, transmit, and transfer monetary instruments and funds to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, namely, a violation of Title 18, United States Code, Section 1030, contrary to Title 18, United States Code, Section 1956(a)(2)(A).

All in violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATIONS

113. The allegations contained in Counts One through Ten of this Indictment are incorporated herein by reference as though fully set forth herein for the purpose of alleging criminal forfeitures pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(A).

114. As a result of the commission of the violations charged in Count One, the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, did use the following to commit or to promote the commission of said violations (hereinafter collectively referred to as the "Subject Domain Names"): fancybear.net and fancybear.org.

115. The United States hereby gives notice to the defendants, ALEKSEI SERGEYEVICH MORENETS, EVGENII MIKHAYLOVICH SEREBRIAKOV, IVAN SERGEYEVICH YERMAKOV, ARTEM ANDREYEVICH MALYSHEV, DMITRIY SERGEYEVICH BADIN, OLEG MIKHAYLOVICH SOTNIKOV and ALEXEY VALEREVICH MININ, charged in Count One that, upon their conviction of such offense, the government will seek forfeiture in accordance with: (a) Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i)(1)(B), which require any person convicted of such offense to forfeit any property constituting or derived from proceeds obtained directly or indirectly as a result of such offense; and (b) Title 18, United States Code, Section 1030(i)(1)(A), which requires any person convicted of such offense to forfeit any personal property that was used or intended to be used to

commit or to facilitate the commission of the offense, including but not limited to the following

SUBJECT DOMAIN NAMES: fancybear.net and fancybear.org.

A True Bill,

FOREPERSON



SCOTT W. BRADY
United States Attorney
PA ID No. 88352