UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

U.S. SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **v.** **VLADISLAV KLIUSHIN (a/k/a VLADISLAV KLYUSHIN), NIKOLAI RUMIANTCEV (a/k/a NIKOLAY RUMYANTCEV), MIKHAIL IRZAK, IGOR SLADKOV, and IVAN YERMAKOV (a/k/a IVAN ERMAKOV),** **Defendants.**	**Civil Action No. 21-CV-12088** **COMPLAINT** **Jury Trial Demanded**

Plaintiff Securities and Exchange Commission ("SEC") alleges as follows against Vladislav Kliushin, a/k/a Vladislav Klyushin ("Kliushin"), Nikolai Rumiantcev, a/k/a Nikolay Rumyantcev ("Rumiantcev"), Mikhail Irzak ("Irzak"), Igor Sladkov ("Sladkov," and together with Kliushin, Rumiantcev, and Irzak, the "Trader Defendants"), and Ivan Yermakov, a/k/a Ivan Ermakov ("Yermakov"), and together with the Trader Defendants, "Defendants").

SUMMARY

1. This action involves Defendants' fraudulent scheme to deceptively obtain material nonpublic pre-release earnings announcements of companies with shares of stock publicly traded on U.S. securities exchanges by hacking into the computer systems of two

service-provider firms, and to use the hacked information to profit by trading in advance of the public release of the earnings information.

2. The service-provider firms that were hacked by Defendants, hereinafter referred to as the "Servicers," assist publicly traded companies with the preparation and filing of periodic and other reports with the SEC, including reports containing the public companies' earnings information. The Servicers help the public companies file the reports with the SEC through the SEC's online Electronic Data Gathering, Analysis and Retrieval ("EDGAR") system.

3. Beginning no later than February 2018 and continuing until at least August 2020 (the "Relevant Period"), Yermakov, a Russian hacker who is the subject of two pending federal criminal indictments, made material misstatements and used deceptive devices and contrivances to obtain material nonpublic information about securities issuers stored on the Servicers' computer systems. This included the use of compromised credentials of the Servicers' employees (*e.g.*, usernames and passwords that did not belong to Yermakov), malware, and other computer hacking techniques.

4. Yermakov hacked into the Servicers' systems for the purpose of accessing and downloading corporate earnings announcements and then providing that information to other individuals to profitably trade securities based upon the hacked earnings announcements. The earnings announcements contained material information about the public companies' earnings that had not yet been made public.

5. Yermakov, directly or indirectly, provided and communicated the hacked, deceptively-obtained pre-release earnings announcements and/or access to those announcements through the Servicers' systems, to the Trader Defendants.

6. Using these hacked, deceptively-obtained pre-release earnings announcements, the Trader Defendants made timely trades in the securities of the Servicers' public company clients, collectively reaping unlawful profits of at least $82.5 million during the Relevant Period.

7. As detailed more fully below, the Trader Defendants' use of the hacked, deceptively-obtained, pre-release earnings announcements is reflected by, among other things, the fact that the trading occurred shortly after the hacking, images of pre-release earnings announcements in the possession of certain Trader Defendants, and the Trader Defendants' overwhelming focus on trading in the securities of the Servicers' publicly-traded company clients, making it statistically almost impossible that their trading occurred by chance.

8. The trades by the Trader Defendants were disproportionately focused around the earnings announcements of publicly-traded companies that used the Servicers to make their EDGAR filings, as compared to earnings announcements where the required EDGAR filings were not made through the Servicers. Indeed, statistical analysis shows that there is a ***less than one-in-one-trillion chance*** that the Trader Defendants' choice to trade so frequently on earnings events tied to the EDGAR filings of the Servicers' public company clients would occur at random.

9. The Trader Defendants (as set forth in the details for each Trader Defendant throughout this complaint) provided substantial assistance to the fraudulent scheme, among other ways, by monetizing the hacked information through unlawful, illicit, and profitable securities trading based on the hacked pre-release earnings announcements, and by participating in transactions and business dealings that enabled them to share their trading profits with Yermakov. In this way, both Yermakov and the Trader Defendants were essential participants in

the fraudulent scheme, and all the Defendants acted with intent to deceive, manipulate, or defraud.

10. By engaging in the misconduct described herein with the requisite scienter, Defendants violated, and, unless enjoined, will continue to violate and are likely in the future to violate the federal securities laws.

NATURE OF PROCEEDING AND RELIEF SOUGHT

11. The SEC brings this action pursuant to Section 20 of the Securities Act of 1933 [*15 U.S.C. §§ 77t(b)*] (the "Securities Act") and Sections 21(d) and 21A of the Securities Exchange Act of 1934 [*15 U.S.C. §§ 78u(d) and 78u-1*] (the "Exchange Act") to enjoin the transactions, acts, practices, and courses of business in this Complaint, and to seek orders of disgorgement, civil money penalties, and further relief as the Court may deem appropriate.

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action pursuant to Sections 20(b) and 22(a) of the Securities Act [*15 U.S.C. §§ 77t(b) and 77v(a)*] and Sections 21(d), 2l(e), 21A and 27 of the Exchange Act [*l5 U.S.C. §§ 78u(d), 78u(e) 78u-l and 78aa*].

13. Each Defendant, directly or indirectly, made use of the means or instrumentalities of interstate commerce, or of the mails, or the facilities of a national securities exchange in connection with the transactions, acts, practices, and courses of business alleged herein. Yermakov provided hacked, deceptively-obtained, material nonpublic information to the Trader Defendants, who used the information to make securities trades that were cleared through U.S.-based brokerage firms and placed on multiple U.S. securities exchanges, and to purchase or sell certain derivatives that resulted in securities trades on multiple U.S. securities exchanges, in a manner that used the instrumentalities of interstate commerce.

14. Venue is proper in this Court pursuant to Section 22(a) of the Securities Act [*15 U.S.C. § 77v(a)*] and Section 27 of the Exchange Act [*15 U.S.C. § 78aa*]. Certain of the acts, practices, transactions, and courses of business constituting the violations alleged in this Complaint occurred within the District of Massachusetts, and were effected, directly or indirectly, by making use of the means or instruments or instrumentalities of transportation or communication in interstate commerce, or of the mails, or the facilities of a national securities exchange. Specifically, numerous instances of unauthorized access to one of the Servicers' systems containing material nonpublic information originated from IP addresses leased to a virtual private network provider that had servers located at a data center in Boston, Massachusetts. Also, at least one of the public companies whose material nonpublic information was unlawfully obtained by Yermakov and then provided to the Trader Defendants, who unlawfully traded on the hacked information, is headquartered in Massachusetts. Furthermore, venue is proper because the Defendants, as foreign nationals residing outside the United States, may have suit brought against them in any district.

DEFENDANTS

15. **Vladislav Kliushin**, age 41, is a Russian citizen who resides in Moscow, Russia. Kliushin is the founder of a Russian media/information technology company (the "IT Company") and serves as a director of IT Company. Kliushin traded securities, alone and in collaboration with Rumiantcev, using material nonpublic information hacked from the Servicers. Kliushin traded through eight brokerage accounts held in his name and a brokerage account held in the name of IT Company. Kliushin also traded through six other brokerage accounts that he and Rumiantcev controlled, as reflected by, among other evidence, (a) screen shots of information for these accounts in Kliushin's possession; (b) electronic communications in which

Kliushin reported on trading in certain of the six accounts and provided passwords to two account holders so they could view the accounts; and (c) an IP address associated with IT Company that accessed these six other accounts as well as the accounts in Kliushin's name. Twelve of the brokerage accounts that Kliushin held in his name or that he controlled were held at either a Cyprus-based brokerage firm or a United Kingdom-based brokerage firm, both of which cleared their trades through U.S. brokerage firms. The other three accounts that Kliushin held in his name or that he controlled were held at a Danish brokerage firm and used by Kliushin primarily to trade "contracts for difference" (a type of security), which resulted in hedging transactions in U.S. markets.

16. **Nikolai Rumiantcev**, age 33, is a Russian citizen who resides in Moscow, Russia. Rumiantcev is a director of IT Company along with Kliushin. Rumiantcev traded securities, alone and in collaboration with Kliushin, using material nonpublic information hacked by Yermakov from the Servicers. Rumiantcev traded through a brokerage account held in his own name and had power of attorney and/or trading authority over eight brokerage accounts held in Kliushin's name and a brokerage account held in the name of IT Company. The accounts held in Rumiantcev's name and the name of IT Company were held at a Cyprus-based brokerage firm, which cleared its trades through a U.S. brokerage firm. Rumiantcev and Kliushin also controlled trading in six other brokerage accounts, as described above in paragraph 15. Between at least July 2018 and August 2020, Kliushin and Rumiantcev used the above-described accounts to trade based on material nonpublic information hacked by Yermakov from the Servicers in advance of more than 300 earnings announcements.

17. **Mikhail Irzak**, age 43, is a Russian citizen who resides in Saint Petersburg, Russia. Irzak holds himself out as a marketing manager for a Russian telecommunications

company. Beginning no later than April 2018 and continuing until at least August 2020, Irzak traded securities based on material nonpublic information hacked by Yermakov from the Servicers in advance of more than 400 earnings announcements. Irzak used three brokerage accounts held in his name to engage in the trading. Irzak held one of these accounts at a Cyprus-based brokerage firm and another account at a Portugal-based brokerage firm, both of which cleared their trades through a U.S. brokerage firm. Irzak held his third account at the same Danish brokerage firm used by Kliushin; like Kliushin, Irzak used his Danish account primarily to trade contracts for difference, which resulted in hedging transactions in U.S. markets.

18. **Igor Sladkov**, age 42, is a Russian citizen who resides in Saint Petersburg, Russia. In correspondence with his broker, Sladkov represented that he worked in the information technology and media services business from approximately 2012 through 2017. Beginning no later than February 2018 and continuing through at least August 2020, Sladkov used an account in his name to regularly trade securities based on material nonpublic information hacked by Yermakov from the Servicers in advance of more than 200 earnings announcements. Sladkov held this account at a Cyprus-based brokerage firm, which cleared its trades through a U.S. brokerage firm. As early as 2018, Sladkov knew that Yermakov was sought by the Federal Bureau of Investigation for his role in hacking conspiracies for which he was indicted that year.

19. **Ivan Yermakov**, age 35, is a Russian citizen who resides in Moscow, Russia. Yermakov served as a Russian military intelligence officer in the Russian Federation's Main Intelligence Directorate of the General Staff ("GRU"). Yermakov is a director of IT Company founded by Kliushin and for which Kliushin and Rumiantcev serve as directors. Yermakov is also a long-time friend of Sladkov. In July and October 2018, the Department of Justice charged Yermakov in federal indictment numbers CR 18-215 in the U.S. District Court for the District of

Columbia and CR 18-263 in the U.S. District Court for the Western District of Pennsylvania for his alleged roles in a hacking conspiracy involving gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election and hacking operations targeting anti-doping agencies, sporting federations, and anti-doping officials. Yermakov also had access to at least one of the accounts held in Kliushin's name that traded on information hacked from the Servicers.

THE HACKED SERVICERS

20. **Servicer A** is a Delaware corporation headquartered in Chicago, Illinois that, among other things, assists companies with the preparation and filing with the SEC of periodic and other reports, including reports containing earnings information.

21. **Servicer B** is a division of a foreign company, which has offices in various U.S. locations. Servicer B assists companies with preparation and filing with the SEC of periodic and other reports, including reports containing earnings information.

TERMS USED IN THIS COMPLAINT

Short-Selling

22. "Short-selling" is the sale of a security not owned by the seller and is a technique used to take advantage of an anticipated decline in the price of the security. An investor borrows stock for delivery at the time of the short sale. If the seller can buy that stock later at a lower price, then a profit results; if, however, the price of the stock rises, then a loss results.

Contracts for Difference

23. A contract for difference, or "CFD," is a stock derivative, which is an agreement between two parties to exchange the difference in value of an underlying stock between the time that the contract is opened and the time that it is closed. If the share price of the underlying

security increases, then the seller pays this difference to the buyer. If, however, the share price of the underlying security declines, then the buyer must pay the seller the difference. Generally, an investor who anticipates an increase in the price of a security will buy a CFD; an investor who anticipates a decrease in the price of the referenced security will sell a CFD. A CFD typically mirrors the movement and pricing of its underlying stock on a dollar-for-dollar basis, such that any fluctuation in the market price of the underlying security is reflected in the unrealized gain or loss of the CFD position.

24. The trading at issue in this action includes the Trader Defendants' purchases and sales of CFDs referencing the stock of the Servicers' public company clients based on the hacked earnings announcements. The CFD provider that facilitated the Trader Defendants' trades at issue in this action generally hedged the Trader Defendants' CFD trades by entering into transactions with U.S.-based broker-dealers, which resulted in those broker-dealers executing trades in the securities underlying the CFDs in the U.S. equity markets.

IP Address

25. An "internet protocol address," or "IP address," is a unique number required for online activity conducted by a computer or other device connected to the internet. Computers use the unique identifier to send data to specific computers on a network.

26. Often, IP addresses can be used to identify the geographic location of the server through which a computer accessed the internet. Thus, in simple terms, an IP address is like a return address on a letter.

27. An individual can conceal the IP address from which he or she is accessing the internet through a number of different techniques and tools, such as a "virtual private network"

or "VPN." Such means enable individuals to assume and use IP addresses different than their own, including IP addresses associated with different geographical regions.

Domain

28. A "domain" is an identifier that refers to a group of internet resources under common administration, authority, or control. For example, "sec.gov" is a domain for which the United States government has authority and that is administered by the SEC.

Virtual Machine

29. A virtual machine is a resource created by software, instead of a physical computer, in order to run an operating system like Microsoft Windows. A relatively powerful physical computer, such as a server in a datacenter, is loaded with a host operating system and runs one or more virtual machines with their own operating systems, each isolated from the activities of the other.

Malware

30. "Malware" is software that is intended to damage or disable computers or computer networks or installed security and access controls, usually installed using deception and without the computer or network user's knowledge.

FACTS

Overview of the Hack-to-Trade Scheme

The Hacking and Trading

31. The Servicers provide proprietary, cloud-based software platforms to facilitate public companies' filing of periodic and other reports with the SEC. The Servicers' public company clients' filings include, among other things, Forms 8-K and related exhibits, which consist of press releases containing the public companies' earnings announcements. The

Servicers' public company clients can use the Servicers' software platforms to create, edit, and submit their filings to the SEC via the SEC's EDGAR filing system.

32. Information contained in pre-release earnings announcements was nonpublic because it had not yet been disseminated to the public through publication or filing designed to achieve a broad dissemination to the investing public generally and without favoring any special person or group. In addition, information contained in pre-release earnings announcements was material. The issuers' earnings information would have been important to the reasonable investor, and viewed by the reasonable investor as having significantly altered the total mix of information made available. Earnings information is material because it relates, among other things, to an issuer's financial condition, solvency, and profitability. For example, public disclosure of earnings information frequently leads to a change in the price of a company's stock. It is common for financial analysts to estimate and/or model a given company's quarterly or annual earnings. The market reaches a consensus expectation based in part on these different estimates. When a company releases its earnings announcements, the price at which shares of that company's stock trade often increases (if earnings exceed market expectations) or decreases (if earnings fall short of market expectations).

33. Typically, the Servicers' public company clients begin the filing process for an earnings announcement by loading a draft earnings announcement onto the Servicer's platform. Once loaded, the public company client can edit the draft earnings announcement on the Servicer's platform, before finalizing the earnings announcement and releasing the final version to the public via a newswire, and filing the announcement with the SEC as an attachment to a Form 8-K called "Exhibit 99.1." There is generally a window of several hours or days between the time that the public company client uploads the pre-release earnings announcement onto the

Servicer's platform and the time at which the client publicly disseminates the final earnings announcement through a newswire and the filing of the Form 8-K with the SEC. The Defendants exploited this window by deceptively acquiring draft earnings announcements and placing trades based on material nonpublic information contained in draft earnings announcements before that information was made public.

34. Beginning no later than February 2018 and continuing until at least August 2020, Defendants engaged in an unlawful scheme in which:

a. Yermakov made material misstatements, used deceptive means, and engaged in deceptive acts to gain unauthorized access into the Servicers' systems. These included use of compromised credentials of the Servicers' employees, malware, and other computer hacking techniques;

b. Once Yermakov gained unauthorized access into the Servicers' systems, Yermakov targeted and unlawfully accessed and downloaded pre-release earnings announcements of the Servicers' public company clients;

c. Yermakov, directly or indirectly, provided and communicated the deceptively-obtained, pre-release earnings announcements and/or access to the announcements through the Servicers' systems for trading purposes to the Trader Defendants;

d. Before the public dissemination of the earnings announcements, the Trader Defendants placed trades in the securities of the Servicers' public company clients on the basis of what they were aware was deceptively-acquired, material nonpublic information provided by Yermakov. If the pre-release earnings announcement indicated that the public company client's stock

price was likely to increase, then the Trader Defendants bought stock in the company or CFDs referencing the company. If the pre-release earnings announcement indicated that the public company client's stock price was likely to decline, then the Trader Defendants sold short shares of the company's stock or sold CFDs referencing the company; and

e. Once the earnings announcements were made public and the public company clients' stock prices moved (as the market learned the previously undisclosed material nonpublic information), the Trader Defendants closed out their trading positions, reaping substantial profits.

35. The Trader Defendants used the information hacked and deceptively-obtained from the Servicers' systems by Yermakov to realize at least $82.5 million in illicit profits between February 2018 and August 2020.

Yermakov's Relationships and Profit-Sharing with the Trader Defendants

36. Yermakov had ongoing professional and personal relationships with each of the Trader Defendants, including through Yermakov's role as a co-director of IT Company (along with Kliushin and Rumiantcev). Yermakov's ongoing relationships and business dealings with Kliushin and Rumiantcev provided opportunities to funnel profits from their illicit trading to Yermakov as compensation for providing them access to the hacked earnings information. Together with Kliushin and Rumiantcev, Yermakov also had access to at least one of the accounts held in Kliushin's name that traded based on hacked, deceptively-obtained, pre-release earnings announcements that Yermakov provided and communicated, directly or indirectly, to Kliushin and Rumiantcev.

37. Yermakov also had ongoing professional and personal relationships with Irzak and Sladkov, including through a long-time friendship with Sladkov. Yermakov engaged in various business activities with Irzak and Sladkov, through which they were able to funnel profits from their illicit trading to Yermakov as compensation for providing them access to the hacked earnings information.

38. Yermakov, directly or indirectly, shared in the profits of the Trading Defendants' unlawful and illicit trading. This is demonstrated through Yermakov's access to a brokerage account in which some of the illicit trading occurred (as alleged above in paragraph 36), his communications, and other evidence. For example, Yermakov communicated with Kliushin about the trading profits realized from their illicit trading on hacked, deceptively-obtained, pre-release earnings announcements provided by Yermakov. Specifically, on May 25, 2019, Yermakov and Kliushin exchanged text messages, in Russian, about Kliushin's trading success. Kliushin told Yermakov that he counted ***198 percent profitability*** in one account and ***69 percent profitability*** in another. Kliushin then commented, "They don't even ask why so anymore." Yermakov responded with thumbs up 👍 and tears of joy 😂 emojis. An emoji is a small image or symbol used in text fields in electronic communications, such as text messages, to convey information or the emotional attitude of the writer.

39. Moreover, in a June 2020 text message exchange, Yermakov remarked to Kliushin, in Russian, that they needed to go to work to make money to buy an apartment. Kliushin responded that there was no need to do that, because they just had to "turn on the computer" to make money, an apparent reference to Defendants' illicit hacking and trading activities. Meanwhile, emails from the second half of 2019 and early 2020 indicate that Yermakov and Irzak were jointly communicating with a management company relating to an

apartment, and that Irzak agreed to purchase real estate from a relative of Yermakov for the equivalent of approximately $1 million.

40. As directors of IT Company, Yermakov, Kliushin, and Rumiantcev all potentially stood to share in trading profits made by IT Company through the trading account held in IT Company's name, or directed to IT Company from other trading accounts in the names of or controlled by Rumiantcev and Kliushin. A September 2020 communication between Rumiantcev and Kliushin states that IT Company was to receive 60 percent of the profits from one of the trading accounts controlled by Rumiantcev and Kliushin. An image in Kliushin's possession included a list, in Russian, of balances in multiple accounts that were in Kliushin's name or controlled by Kliushin, and one of these accounts was held in the name of IT Company.

41. During the course of the hacking and trading scheme, Yermakov also communicated with Irzak and Sladkov, who illicitly traded based on hacked, deceptively-obtained, pre-release earnings announcements that Yermakov, directly or indirectly, provided, and/or to which Yermakov provided access through the Servicers' systems. Evidence that Irzak and Sladkov obtained from Yermakov, directly or indirectly, pre-release earnings announcements that Yermakov hacked and deceptively obtained from the Servicers, and then illicitly traded based on this information, includes the following:

a. In February 2018, Sladkov possessed a digital photograph of the pre-release earnings announcement of a U.S. publicly traded company, which was also a Servicer A client. This photograph was created one day after Yermakov deceptively hacked the announcement from Servicer A's system and less than three hours before Sladkov traded in the securities of the company.

Sladkov took a position in the securities of this issuer ***after*** the photograph was created, but ***before*** public release of the earnings announcement.

b. In October 2018, Sladkov possessed a digital photograph of the pre-release earnings announcement of a U.S. publicly traded company, which was also a Servicer A client. The Trader Defendants took positions in the securities of this issuer ***after*** the photograph was created, but ***before*** public release of the earnings announcement.

c. Other photographs in Sladkov's possession show Irzak and Sladkov together with a laptop that they used to view hacked earnings announcements like those referenced in paragraphs 41(a) and 41(b) above.

d. In May 2019, one day after Yermakov deceptively hacked the pre-release earnings announcement of a U.S. publicly traded company from Servicer A's system, Yermakov exchanged market information about the company with Sladkov. ***After*** the hack, but ***before*** public release of the final earnings announcement, the Trader Defendants took positions in the securities of this issuer.

e. Sladkov possessed lists of dozens of ticker symbols associated with the Servicers' public company clients alongside dates of the public company clients' earnings announcements.

42. Yermakov and the Trader Defendants expected to profit from unlawful trading based on pre-release earnings announcements hacked and deceptively obtained by Yermakov. Based on their relationships and communications with Yermakov (as set forth in paragraphs 36 to 41 directly above) as well as the close temporal proximity of their unlawful trading and

Yermakov's hacking of the Servicers' systems (as set forth in paragraphs 71 to 121 below), the Trader Defendants, directly or indirectly, shared with Yermakov the illicit profits that they made from trading based on the pre-release earnings announcements hacked and deceptively obtained by Yermakov.

Yermakov's Deceptive Hacks of the Servicers' Systems

43. Yermakov intentionally made material misstatements and employed a variety of deceptive and fraudulent devices, contrivances, artifices, practices, means, and acts to gain unauthorized access into the Servicers' systems and download pre-release earnings announcements, including use of compromised credentials of the Servicers' employees and malware. Yermakov also used anonymized IP addresses designed to conceal his identity. Yermakov's repeated hacks continued against Servicer A for approximately two years and against Servicer B for approximately one year, before the Servicers detected Yermakov's intrusions into their systems and took steps to mitigate them.

Yermakov's Deceptive Hacks of Servicer A

44. By at least February 2018, without authorization from Servicer A, Yermakov obtained the credentials of a Servicer A employee, which the employee used in the course of his or her employment to access Servicer A's system. Without authorization from Servicer A, Yermakov subsequently obtained the credentials of at least two additional Servicer A employees, which the employees used in the course of their employment to access Servicer A's system.

45. Beginning no later than February 2018 and continuing until at least August 2020, Yermakov made material misstatements, affirmatively misrepresented himself and his identity, and deceptively used the credentials of these Servicer A employees to gain unauthorized access into the Servicer's system and to unlawfully access and download numerous pre-release earnings

announcements of Servicer A's public company clients. By using the deceptively-obtained credentials, Yermakov falsely presented himself as an authorized user of Servicer A's system.

46. When he hacked into Servicer A's system, Yermakov further concealed his identity by using an intermediary internet service, which concealed his IP address, and, hence, his physical location. The intermediary service routed Yermakov's queries of Servicer A's system through one of over 100 rotating IP addresses associated with different geographic locations around the world, including the Commonwealth of Massachusetts. The more than 100 IP addresses were unaffiliated with any individual, and, thus, were "anonymized." Yermakov used rotating, anonymized IP addresses to hide his misconduct.

47. On May 2, 3, and 9, 2018, an IP address associated with Yermakov accessed Servicer A's system, posing as a Servicer A employee. The IP address associated with Yermakov accessed and downloaded files of at least eight of Servicer A's public company clients during this time period, including a pre-release earnings announcement for Issuer A, a U.S.-listed public company.

48. The download of Issuer A's pre-release earnings announcement by the IP address associated with Yermakov correlated with trading by Irzak in the securities of Issuer A, as follows:

Date	Time	Event
5/3/2018	1:35 p.m. ET	IP address associated with Yermakov accessed Issuer A's pre-release earnings announcement in Servicer A's system.
5/3/2018	2:48 p.m. ET	Irzak purchased CFDs referencing Issuer A.
5/3/2018	4:02 p.m. ET	After the close of regular market trading, Issuer A publicly announced its first quarter 2018 earnings.
5/4/2018	9:31 a.m. ET	Shortly after the opening of regular market trading, Irzak closed his CFD position referencing Issuer A, realizing a profit.
5/4/2018	4:00 p.m. ET	The price of Issuer A's common stock closed 8% higher than it did on May 3, 2018.

49. In or around July 2020, Servicer A discovered evidence of malware on three of its employees' laptops. The malware contained names of two different domains registered through

a U.S.-based domain name registrar, using different fictitious names and addresses, and foreign email addresses. The purchaser of the two domains used cryptocurrency, in an effort to further mask his identity. Additionally, the same domain name registrar was used to register domains that were found to be encoded in the malware on Servicer B's systems, as described below. The fictitious persona that registered one of the domains associated with the hack of Servicer A used the same fake address location and phone number as fictitious personas that registered domains associated with the hack of Servicer B.

Yermakov's Deceptive Hacks of Servicer B

50. No later than January 2019, Yermakov also made material misrepresentations, affirmatively misrepresented himself and his identity, and used deceptive means to gain unauthorized access into Servicer B's systems, including by using the compromised credentials of Servicer B employees and a disguised virtual machine (which used a naming convention that was intended to escape detection by Servicer B), and to unlawfully access and download numerous pre-release earnings announcements of Servicer B's public company clients.

51. Between January 2019 and January 2020, Servicer B's computer servers logged ***over 900 instances*** in which a virtual machine outside of Servicer B's network remotely accessed the system accounts of five Servicer B employees, whose duties included supporting Servicer B's public company clients. The virtual machine that accessed the accounts of five Servicer B employees was fraudulently disguised by mimicking Servicer B's system naming convention to appear legitimate to Servicer B employees.

52. On or about January 21, 2020, Servicer B discovered unusual activity in the account of a Servicer B employee. This led Servicer B to identify Yermakov's intrusions and related misconduct in Servicer B's systems, dating back at least one year.

53. Following its January 2020 discovery, Servicer B identified additional abnormalities on its systems. Specifically, Servicer B identified malware on a server cluster associated with its systems and on the workstations of several of its employees.

54. Domain names encoded in the malware identified on Servicer B's system were registered with the same U.S.-based domain name registrar as the domains that were encoded in the malware on the computers of Servicer A's employees. As with Servicer A, the domain names were registered using fictitious names and addresses and foreign email addresses, and paid for using cryptocurrency such as bitcoin.

55. Defendants perpetrated this scheme, in part, using the resources of IT Company for which Kliushin, Rumiantcev, and Yermakov serve as directors. An IP address associated with IT Company is connected to a November 2018 cryptocurrency transaction with a U.S.-based domain name registrar. Digital asset tracing links the bitcoin address associated with this November 2018 transaction to other bitcoin transactions in August and November 2018 by fictitious personas. These fictitious personas were used to set up or purchase hacking infrastructure such as servers and domains associated with the hack of Servicer B's systems. In August 2018, one of these fictitious personas also appears to have been used to conduct reconnaissance of a company that provides EDGAR filing services similar to those provided by the Servicers. In addition, this same IP address associated with IT Company logged into brokerage accounts that were in the names of or controlled by Rumiantcev and Kliushin, and that participated in some of the illicit trading based on the hacked information, more than 200 times during the Relevant Period. Thus, this same IP address associated with IT Company was connected to both hacking conduct and a portion of the illicit trading described herein.

56. After its January 2020 discovery of Yermakov's hacking of its systems, Servicer B took additional steps to secure its systems. These additional steps appear to have succeeded in securing Servicer B's systems against further intrusion by the end of January 2020.

Unlawful Trading Based on the Hacked Earnings Announcements

57. During the Relevant Period, Defendants—individually, collaboratively, and in parallel—used material, nonpublic, information from numerous deceptively-obtained hacked pre-release earnings announcements to trade in the stock and CFDs referencing the Servicers' public company clients, thereby reaping large, unlawful profits. An investor in these issuers suffered an informational disadvantage vis-à-vis the Trader Defendants who had material nonpublic information stemming from Yermakov's fraudulent hacking; that disadvantage could not be overcome with research or skill and thus undermined the integrity of, and investor confidence in, the securities markets.

58. The hack-to-trade scheme followed a consistent pattern:

a. Yermakov deceptively accessed and downloaded pre-release earnings announcements of public company clients from the Servicers' systems;

b. Yermakov, directly or indirectly, provided the Trader Defendants with the hacked, deceptively-obtained, pre-release earnings announcements and/or access to the announcements through the Servicers' systems;

c. Hours or days after a pre-release earnings announcement was accessed and downloaded, but before the final version of that announcement was made public through a newswire release and/or filing with the SEC, the Trader Defendants placed trades in the stock or CFDs referencing the public company client whose pre-release earnings announcement had been deceptively obtained;

d. The trading decisions of the Trader Defendants significantly benefitted from the material nonpublic information contained in the pre-release earnings announcements, because the Trader Defendants were able to use this information to predict the anticipated direction and magnitude of change in the public company clients' stock prices;

e. Shortly after the Servicers' public company clients issued their earnings announcements and the market incorporated the information contained in the earnings announcements into the price of the security, the Trader Defendants closed their positions, typically profiting handsomely.

59. Paragraphs 71 through 121 below provide specific examples of trading before earnings announcements on the basis of hacked information by the Trader Defendants between at least February 2018 and August 2020.

60. Yermakov's use of the Trader Defendants to monetize the hacked information was part of a deceptive course of conduct.

61. Yermakov knew, consciously avoided knowing, was reckless in not knowing, or should have known that he was participating, assisting, and acting in furtherance of a scheme to defraud.

62. The Trader Defendants participated in and provided substantial assistance to Yermakov's violations and scheme, by monetizing the hacked material, deceptively-obtained, nonpublic information through unlawful, illicit, and profitable securities trading based on this information.

63. The Trader Defendants concealed their access to the hacked information and their trading activities through the use of multiple brokerage accounts.

64. The trading activity of the Trader Defendants mirrored their access to material nonpublic information maintained on the Servicers' systems. Before Servicer B secured its system, in January 2020, the Trader Defendants focused their trading in the securities of ***both*** Servicers' public company clients, while trading far less frequently in the securities of other companies around earnings announcements. After Servicer B secured its system, however, the Trader Defendants largely stopped trading in the securities of Servicer B public company clients, and instead focused their trading in the securities of Servicer A's public company clients.

Statistical Analysis of the Trader Defendants' Unlawful Trading

65. The Trader Defendants routinely traded on material nonpublic information contained in pre-release earnings announcements of Servicer A's and Servicer B's public company clients, which were hacked and made available to the Trader Defendants by Yermakov, realizing unlawful profits of at least $82.5 million during the Relevant Period.

66. It is virtually impossible that the Trader Defendants' decision to trade in advance of earnings announcements of the Servicers' public company clients occurred at random. There are many thousands of other earnings announcements by public companies who did not use the services of either Servicer A or Servicer B. However, the vast majority of trading by the Trader Defendants around earnings announcements was in advance of the earning announcements by the Servicers' public company clients, to the exclusion of other public companies' earnings announcements.

67. Statistical analysis of the Trader Defendants' trading shows that there is a less than a one-in-one-trillion chance that the Trader Defendants would have traded so frequently around the earnings announcements of the Servicers' public company clients at random. This means that it is nearly impossible that the Trader Defendants' trading is unrelated to the role of

the Servicers in the earnings announcements of the public companies whose securities the Trader Defendants traded.

68. This also means that it is nearly impossible that the Trader Defendants' trading is unrelated to Yermakov's hacks of the Servicers' systems. As alleged above, Yermakov conducted hacks of both Servicer A and Servicer B during the Relevant Period, which can be directly tied to illegitimate trading based on the hacked information. In particular, in May 2018, less than 20 hours after an IP address associated with Yermakov deceptively accessed Servicer A's system and downloaded files of multiple public company clients of Servicer A, the following events occurred: Irzak purchased the securities of one of the company clients whose files were hacked; the company client publicly announced its first quarter 2018 earnings; and Irzak sold the securities that he had just bought for a profit. Malware subsequently discovered on the systems of both Servicers A and B contained names of domains registered through the same U.S.-based domain name registrar, all using fictitious names and addresses, and foreign email addresses. The fake address location and phone number of a domain associated with the hack of Servicer A was the same fake address location and phone number of domains associated with the hack of Servicer B.

69. Between February 2018 and August 2020, the Trader Defendants collectively placed trades before more than 500 earnings announcements of Servicer A and Servicer B public company clients for which the Servicers made EDGAR filings, obtaining total illicit profits of at least $82.5 million.

70. The overwhelming emphasis by the Trader Defendants on trading ahead of the earnings announcements of the Servicers' public company clients, as compared to their far less frequent trading around all other earnings announcements during the time period of the hacks,

evidences that they were trading with the benefit of deceptively-obtained material nonpublic information.

Examples of Unlawful Trading by the Trader Defendants Based on Hacked Earnings Announcements Provided by Yermakov

71. The following examples—in addition to the examples described above in paragraphs 41 and 48)—are illustrative of the more than 500 instances of trading before earnings announcements on the basis of hacked information by the Trader Defendants between at least February 2018 and August 2020. These examples further demonstrate the Trader Defendants' unlawful use of the material nonpublic information deceptively obtained by Yermakov from the Servicers' systems to place winning trades and make illicit profits of millions of dollars.

The October 2019 Earnings Release of Issuer B

72. Issuer B is a publicly traded company incorporated in Delaware and headquartered in California. It has a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the Nasdaq Capital Market ("Nasdaq") during the Relevant Period. Issuer B is a public company client of Servicer A.

73. On October 23, 2019, at approximately 6:17 a.m. ET, using an anonymized IP address, Yermakov made material misstatements, affirmatively misrepresented himself and his identity, and deceptively used the credentials belonging to a Servicer A employee to gain access to Servicer A's system. Yermakov accessed and downloaded Issuer B's pre-release earnings announcement.

74. Starting less than an hour after Yermakov hacked into Servicer A's system, between approximately 6:53 a.m. and 3:57 p.m. ET on October 23, 2019, Sladkov purchased 55,000 shares of Issuer B's stock.

75. Shortly after Sladkov began buying shares of Issuer B's stock, Irzak also began purchasing Issuer B's securities. On October 23, 2019, between approximately 9:44 a.m. ET and 3:46 p.m. ET, Irzak bought 7,200 shares of Issuer B's stock and 4,000 CFDs referencing Issuer B.

76. Within hours of Yermakov's hack of Servicer A's system, between approximately 10:23 a.m. ET and 1:26 p.m. ET on October 23, 2019, Rumiantcev and Kliushin also bought 37,031 shares of Issuer B's stock and 4,300 CFDs referencing Issuer B.

77. At approximately 4:54 p.m. ET on October 23, 2019, after the close of U.S. trading markets, Issuer B publicly released its earnings announcement, in which it reported earnings information from its third quarter of 2019, which beat analysts' estimates.

78. Following Issuer B's public earnings announcement, shares of Issuer B's stock rose more than 20 percent in after-hours trading. At the end of the next trading session, on October 24, 2019, Issuer B's stock price closed at $299.68, an increase of approximately 18 percent from the prior day's closing price.

79. Moments after Issuer B publicly released its earnings announcement on October 23, 2019, Irzak liquidated the Issuer B stock that he had finished buying less than an hour earlier. From approximately 4:54 p.m. to 5:00 p.m. ET, in after-hours trading, Irzak sold 7,000 shares of Issuer B stock. The next morning, on October 24, 2019, from approximately 7:00 a.m. to 9:41 a.m. ET, Irzak closed out his CFD position by selling 4,000 CFDs referencing Issuer B. Irzak sold the remaining 200 shares of Issuer B stock he held at approximately 1:14 p.m. ET on October 24, 2019.

80. From approximately 4:57 p.m. to 5:18 p.m. ET on October 23, 2019, in after-hours trading, Kliushin and Rumiantcev sold 26,331 shares of Issuer B's stock. Between

approximately 9:30 a.m. and 12:14 p.m. ET on October 24, 2019, Kliushin and Rumiantcev sold the remaining 10,700 shares of Issuer B's stock they held and 4,300 CFDs referencing Issuer B.

81. Between approximately 4:57 p.m. and 4:59 p.m. ET on October 23, 2019, in after-hours trading, Sladkov sold 21,580 shares of Issuer B stock that he had purchased that same day. On October 24, 2019, between approximately 6:42 a.m. and 7:26 a.m. ET, Sladkov sold the remaining 33,420 Issuer B shares he held.

82. Irzak made approximately $377,000 in unlawful profits through his timely purchases and sales of Issuer B's securities based on the material nonpublic information contained in the deceptively-obtained Issuer B pre-release earnings announcement.

83. Sladkov made approximately $2.2 million in unlawful profits through his timely purchases and sales of Issuer B's securities based on the material nonpublic information contained in the deceptively-obtained Issuer B pre-release earnings announcement.

84. Rumiantcev and Kliushin made approximately $1.6 million in unlawful profits through their timely purchases and sales of Issuer B's securities based on the material nonpublic information contained in the deceptively-obtained Issuer B pre-release earnings announcement.

The November 2019 Earnings Release of Issuer C

85. Issuer C is a publicly traded company incorporated in Delaware and headquartered in California. It has a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the Nasdaq during the Relevant Period, and continues to trade on the Nasdaq today. Issuer C is a public company client of Servicer A.

86. On at least four different occasions between November 1 and November 6, 2019, Yermakov made material misrepresentations, affirmatively misrepresented himself and his identity, and deceptively used the credentials belonging to a Servicer A employee and an

anonymized IP address to gain unauthorized access into Servicer A's system and access and download Issuer C's pre-release earnings announcement.

87. On November 5, 2019, between approximately 10:10 a.m. and 12:27 p.m. ET, Kliushin and Rumiantcev sold short 1,310 shares of Issuer C's stock.

88. On November 6, 2019, between approximately 10:30 a.m. and 3:59 p.m. ET, Kliushin and Rumiantcev sold short 33,810 shares of Issuer C's stock and sold 220,558 CFDs referencing Issuer C.

89. Also on November 6, 2019, between approximately 10:42 a.m. and 3:41 p.m. ET, Irzak sold short 5,000 shares of Issuer C's stock.

90. The short sales of Issuer C's stock and the sales of CFDs are consistent with a bet that the per-share price of Issuer C would decline in the near term.

91. Within minutes of the last short sales of Issuer C's securities, at approximately 4:00 p.m. ET on November 6, 2019, after the close of U.S. trading markets, Issuer C publicly released its earnings announcement with earnings information from its third quarter of 2019. Following Issuer C's earnings announcement, the price of Issuer C's stock fell in after-hours trading and opened approximately 16 percent lower at the start of the next day's trading session. At the close of the next trading session, on November 7, 2019, Issuer C's stock price remained 16 percent lower than its prior day's closing price.

92. Minutes after Issuer C released its earnings announcement on November 6, 2019, from approximately 4:02 p.m. to 4:08 p.m. ET, Irzak closed out his short position in Issuer C's stock, buying 5,000 shares.

93. Also on November 6, 2019 between 4:10 p.m. and 5:10 p.m. ET, Kliushin and Rumiantcev purchased 3,310 shares of Issuer C's stock to close out a portion of their short position.

94. On November 7, 2019, between approximately 8:45 a.m. and 11:02 a.m. ET, Kliushin and Rumiantcev bought 31,810 shares of Issuer C's stock to close out the remainder of their short position and 220,558 CFDs referencing Issuer C to close out their CFD position.

95. Irzak made approximately $87,000 in unlawful profits through his timely sales and purchases of Issuer C securities based on the material nonpublic information contained in Issuer C's pre-release earnings announcement

96. Kliushin and Rumiantcev made approximately $6 million in unlawful profits through their timely sales and purchases of Issuer C securities based on the material nonpublic information contained in Issuer C's pre-release earnings announcement.

The December 2019 Earnings Announcement of Issuer D

97. Issuer D is a publicly traded company incorporated in Delaware and headquartered in Illinois. It has a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the Nasdaq during the Relevant Period. Issuer D is a public company client of Servicer B.

98. On December 2, 2019, between approximately 5:20 a.m. and 5:22 a.m. ET, Yermakov made misrepresentations and deceptively used credentials belonging to a Servicer B employee to gain unauthorized access into Servicer B's systems. Yermakov accessed and downloaded Issuer D's pre-release earnings announcement.

99. On December 3, 2019, between approximately 3:47 a.m. and 3:50 a.m. ET, Yermakov again made material misstatements, affirmatively misrepresented himself and his

identity, and used deceptive means to gain unauthorized access into Servicer B's system, and access Issuer D's pre-release earnings announcement.

100. At approximately 10:47 a.m. ET on December 3, 2019, Kliushin and Rumiantcev purchased 1,000 shares of Issuer D's stock.

101. Between approximately 10:17 a.m. and 2:22 p.m. ET on December 4, 2019, Kliushin and Rumiantcev purchased 4,000 shares of Issuer D's stock.

102. On December 5, 2019, between approximately 8:13 a.m. and 3:58 p.m. ET, Irzak purchased 2,600 shares of Issuer D's stock.

103. On December 5, 2019, between approximately 9:38 a.m. and 2:54 p.m. ET, Kliushin and Rumiantcev purchased 26,100 shares of Issuer D's stock.

104. At approximately 4:03 p.m. ET on December 5, 2019, after the close of U.S. trading markets, Issuer D publicly released its earnings announcement with earnings results from its third quarter of 2019. Among other generally positive earnings news, Issuer D announced that gross profit as a percentage of net sales increased 40 basis points to 37.1 percent compared to 36.7 percent in the third quarter of the prior year. Issuer D's stock price rose in reaction to the company's public announcement and closed at $262.20 per share at the end of the next trading day, December 6, 2019—approximately 11 percent higher than the close on December 5, 2019.

105. Between approximately 4:07 p.m. ET on December 5, 2019, and 10:28 a.m. ET on December 6, 2019, Irzak sold 2,600 shares of Issuer D's stock that he had just bought on December 5, 2019.

106. Between 9:36 a.m. and 10:17 a.m. ET on December 6, 2019, Kliushin and Rumiantcev sold 27,500 shares of Issuer D's stock. They closed out the remainder of their

position by selling 3,600 shares of Issuer D's stock between 9:39 a.m. and 9:40 a.m. ET on December 9, 2019.

107. Kliushin and Rumiantcev realized profits of approximately $785,000 through their timely purchases and sales of Issuer D securities based on the material nonpublic information contained in Issuer D's pre-release earnings announcement.

108. Irzak made approximately $59,000 through his timely purchases and sales of Issuer D securities based on the material nonpublic information contained in Issuer D's pre-release earnings announcement.

The January 2020 Earnings Release of Issuer E

109. Issuer E is a publicly traded company incorporated and headquartered in New York State. It has a class of shares registered under Section 12(b) of the Exchange Act and its common stock traded on the New York Stock Exchange ("NYSE") during the Relevant Period. Issuer E is a public company client of Servicer B.

110. On January 21, 2020, between approximately 8:58 a.m. and 9:34 a.m. ET, Yermakov made material misrepresentations, affirmatively misrepresented himself and his identity, and deceptively used the credentials belonging to a Servicer B employee to gain unauthorized access into Servicer B's systems. Yermakov accessed and downloaded the pre-release earnings announcements of eight different public company clients of Servicer B, including Issuer E.

111. Between approximately 10:40 a.m. and 10:42 a.m. ET on January 21, 2020, a little more than an hour after the hack of Issuer E's pre-release earnings announcement on Servicer B's system, Irzak bought 5,000 shares of Issuer E's stock. Irzak bought an additional 700 shares of Issuer E's stock at approximately 1:32 p.m. ET on January 21, 2020.

112. Between approximately 12:21 p.m. and 3:58 p.m. ET on January 21, 2020, Kliushin and Rumiantcev bought 87,200 shares of Issuer E's stock.

113. Between approximately 2:07 p.m. and 2:49 p.m. ET on January 21, 2020, Sladkov bought 45,000 shares of Issuer E's stock.

114. At approximately 4:04 p.m. ET on January 21, 2020, after the close of U.S. trading markets, Issuer E publicly released its earnings announcement with earnings results from the fourth quarter and full year 2019. Issuer E's earnings results beat analysts' estimates and forecasted earnings growth in 2020.

115. On January 22, 2020, Issuer E's stock price closed at $143.89, an increase of approximately three percent from its closing price on January 21, 2020.

116. On January 22, 2020, between approximately 9:31 a.m. and 12:50 p.m. ET, Kliushin and Rumiantcev sold 87,200 shares of Issuer E's stock, closing out their position.

117. On January 22, 2020, between approximately 9:35 a.m. and 9:42 a.m. ET, Irzak sold the 5,700 shares of Issuer E's stock that he had bought the day before.

118. On January 22, 2020, between approximately 9:36 a.m. and 9:55 a.m. ET, Sladkov sold the 45,000 shares of Issuer E's stock that he had bought the day before.

119. Irzak made approximately $39,000 in unlawful profits through his timely purchases and sales of Issuer E securities based on the material nonpublic information contained in Issuer E's pre-release earnings announcement.

120. Kliushin and Rumiantcev made approximately $493,000 in unlawful profits through their timely purchases and sales of Issuer E securities based on the material nonpublic information contained in Issuer E's pre-release earnings announcement.

121. Sladkov made approximately $270,000 in unlawful profits through his timely purchases and sales of Issuer E securities based on the material nonpublic information contained in Issuer E's pre-release earnings announcement.

Certain Trader Defendants Lied To Cover Up Their Illegal Trading

122. Kliushin and Rumiantcev also furthered Defendants' fraudulent scheme by deceiving one of their brokerage firms. In or around April 2020, brokerage firm personnel questioned Kliushin and Rumiantcev about their trading strategy, including their focus on trading around earnings announcements. Kliushin and Rumiantcev falsely told brokerage firm personnel that they relied on "open source" information and did not use inside information.

The Trader Defendants Knowingly or Recklessly Participated In and Substantially Assisted Yermakov's Hacking Scheme

123. The Trader Defendants were aware of and knowingly or recklessly furthered and substantially assisted Yermakov's deceptive hacking scheme by colluding with Yermakov and each other to use the material nonpublic information contained in the deceptively-obtained pre-release earnings announcements of the Servicers' public company clients as a basis for securities trades. The Trader Defendants knew, consciously avoided knowing, were reckless in not knowing, or should have known of the violation of the securities laws that Yermakov committed, and in particular, that the material nonpublic information that they received, directly or indirectly, from Yermakov was obtained through a scheme to defraud. Indeed, the Trader Defendants knew, consciously avoided knowing, were reckless in not knowing, or should have known that they were each participating, assisting, and acting in furtherance of a scheme to defraud.

CONCLUSION

124. As detailed above, Defendants participated in a common scheme to defraud and otherwise committed primary violations of the federal securities laws cited below, which required the participation of Yermakov and one or more of the Trader Defendants to succeed.

125. In addition or in the alternative, also as detailed above, Yermakov violated the securities laws cited below, and the Trader Defendants aided and abetted those violations by knowingly or recklessly providing substantial assistance to Yermakov in violation of those securities laws, and are therefore in violation to the same extent as Yermakov.

FIRST CLAIM FOR RELIEF
Violations of Securities Act Section 17(a)
(Against All Defendants)

126. Paragraphs 1 through 125 are re-alleged and incorporated herein by reference, as if they were fully set forth herein.

127. By engaging in the conduct described above, Defendants knowingly, recklessly, or negligently, in the offer or sale of securities, by use of the means or instruments of transportation or communication in interstate commerce or by use of the mails, directly or indirectly:

a. employed devices, schemes, or artifices to defraud;

b. obtained money or property by means of untrue statements of material facts, or omissions to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or

c. engaged in transactions, practices, or courses of business which operated or would operate as a fraud or deceit upon the purchaser.

128. By engaging in the foregoing conduct, Defendants violated, and unless enjoined will continue to violate and are likely in the future to violate, Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*].

SECOND CLAIM FOR RELIEF
Violation of Section 10(b) of the Exchange Act and Rule 10b-5 Thereunder
(Against All Defendants)

129. Paragraphs 1 through 125 are re-alleged and incorporated herein by reference, as if they were fully set forth herein.

130. By engaging in the conduct described above, Defendants knowingly or recklessly, in connection with the purchase or sale of securities, directly or indirectly, by use of the means or instrumentalities of interstate commerce, or the mails, or the facilities of a national securities exchange:

a. employed devices, schemes, or artifices to defraud;

b. made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or

c. engaged in acts, practices, or courses of business that operated or would operate as a fraud or deceit upon any person in connection with the purchase or sale of any security.

131. By engaging in the foregoing conduct, Defendants violated, and unless enjoined will continue to violate and are likely in the future to violate, Exchange Act Section 10(b) [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [*17 C.F.R. § 240.10b-5*].

THIRD CLAIM FOR RELIEF
Violation of Section 20(b) of the Exchange Act
(Against Trader Defendants)

132. Paragraphs 1 through 125 are re-alleged and incorporated herein by reference, as if they were fully set forth herein.

133. By engaging in the foregoing conduct, the Trader Defendants violated Section 17(a) of the Securities Act [*15 U.S.C. § 77q(a)*] and Section 10(b) of the Exchange Act [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [*17 C.F.R. § 240.10b-5*], through or by means of Yermakov.

134. By engaging in the foregoing conduct, pursuant to Section 20(b) of the Exchange Act [*15 U.S.C. § 78t(b)*], the Trader Defendants violated, and unless enjoined will continue to violate and are likely in the future to violate, Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*] and Section 10(b) of the Exchange Act [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [*17 C.F.R. § 240.10b-5*].

FOURTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Securities Act Section 17(a)
(Against Trader Defendants)

135. Paragraphs 1 through 125 are re-alleged and incorporated herein by reference, as if they were fully set forth herein.

136. Yermakov violated Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*].

137. Through, among other things, their unlawful and illicit trading, and sharing of profits with Yermakov directly or indirectly, the Trader Defendants knowingly or recklessly provided substantial assistance to, and thereby aided and abetted, the Yermakov's violations of the securities laws.

138. By engaging in the foregoing conduct, pursuant to Securities Act Section 15(b) [*15 U.S.C. § 77o(b)*], the Trader Defendants violated, and unless enjoined will continue to violate and are likely in the future to violate, Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*].

FIFTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act Section 10(b) and Rule 10b-5 Thereunder
(Against Trader Defendants)

139. Paragraphs 1 through 125 are re-alleged and incorporated herein by reference, as if they were fully set forth herein.

140. As alleged above, Yermakov violated Exchange Act Section 10(b) [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [*17 C.F.R. § 240.10b-5*].

141. Through their unlawful and illicit trading, and sharing of profits with Yermakov directly or indirectly, the Trader Defendants knowingly or recklessly provided substantial assistance to, and thereby aided and abetted, Yermakov's violations of the securities laws.

142. By engaging in the foregoing conduct, pursuant to Exchange Act Section 20(e) [*15 U.S.C. § 78t(e)*], the Trader Defendants violated, and unless enjoined will continue to violate and are likely in the future to violate, Exchange Act Section 10(b) [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [*17 C.F.R. § 240.10b-5*].

PRAYER FOR RELIEF

WHEREFORE, the Commission respectfully requests that the Court enter Final Judgments:

A. Permanently restraining and enjoining Defendants from, directly or indirectly, engaging in conduct in violation of Section 17(a) of the Securities Act [*15 U.S.C. § 77q(a)*], and Section 10(b) of the Exchange Act [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [*17 C.F.R. § 240.10b-5*]; and permanently restraining and enjoining the Trader Defendants from violating the

above-listed provisions through or by means of Yermakov, in violation of Section 20(b) of the Exchange Act [*15 U.S.C. § 78t(b)*].

B. Ordering each Defendant to disgorge, with prejudgment interest, all illicit trading profits, avoided losses, or other ill-gotten gains received, including, but not limited to, all illicit trading profits or other ill-gotten gains received, directly or indirectly, from another Defendant, as a result of the actions alleged herein.

C. Ordering each Defendant to pay a civil penalty up to three times the profits made pursuant to Section 21A of the Exchange Act [*15 U.S.C. § 78u-1*] or, alternatively, to pay a civil penalty under Section 20(d) of the Securities Act [*15 U.S.C. § 77t(d)*] or Section 21(d) of the Exchange Act [*15 U.S.C. § 78u(d)*];

D. Granting such other and further relief as the Court may deem just, equitable, or necessary.

JURY TRIAL DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, the SEC demands a jury trial on all the issues so triable.

Dated: December 20, 2021

Respectfully submitted,

By: David Mendel

David S. Mendel
(D.C. Bar No. 470796)
Tel: (202) 551-4418
Fax: (301) 623-1192
MendelD@sec.gov

James P. Connor
(D.C. Bar No. 981684)
Tel: (202) 551-8394
Fax: (301) 623-1192
Connorja@sec.gov

SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, D.C. 20549

Of Counsel:
Joseph G. Sansone
Diana K. Tani
Megan M. Bergstrom
David E. Bennett
SECURITIES AND EXCHANGE COMMISSION