Cheryl L. Crumpton
Stephan J. Schlegelmilch
U.S. SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, DC 20549
Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

U.S. SECURITIES AND EXCHANGE COMMISSION,

Plaintiff,

v.

OLEKSANDR IEREMENKO,
SPIRIT TRADE, LTD.,
SUNGJIN CHO,
DAVID KWON,
IGOR SABODAKHA,
VICTORIA VOROCHEK,
IVAN OLEFIR,
CAPYIELD SYSTEMS, LTD., and
ANDREY SARAFANOV,

Defendants,

and

KYUNGJA CHO,
LYUDMILA KALINKINA,
ANDREY MELEYNIKOV, and
IVAN SOLOVEV

Relief Defendants.

Civil Action No. 19-cv-505

Jury Trial Demanded

COMPLAINT

Plaintiff United States Securities and Exchange Commission (the "SEC"), 100 F Street, N.E., Washington, DC 20549, alleges as follows against the following Defendants and Relief Defendants, whose names and last known addresses are set forth below:

a. Oleksandr Ieremenko – Kiev, Ukraine;

b. Spirit Trade, Ltd., Wellborne Comm CTR 8, Hong Kong, RM 709, Hong Kong Special Administrative Region of China;

c. Sungjin Cho – 681 S. Norton Avenue, Apt. 116, Los Angeles, CA 90005;

d. David Kwon – 3223 W. 6th Street, Unit 406, Los Angeles, CA 90020;

e. Igor Sabodakha – PR. Geroev Stalingrada 12D, app. 81, Kiev, 04210, Ukraine;

f. Victoria Vorochek – ul. Vilesova 6B, app. 57, Severodonetsk, Luhans'ka Oblast, 93400, Ukraine;

g. Ivan Olefir – Staritskogo 16, Chaika, Kiev Oblast, 08130, Ukraine;

h. Capyield Systems, Ltd. – #1 Mapp Street, Belize City, Belize;

i. Andrey Sarafanov – Nogina, 2-15, Dedovsk, Moskva, 143530, Russian Federation;

j. Kyungja Cho – 56 Neungpyeong-ro 156beon-gil, Opo-eup, Gwangju-si Gyeonggi-do, 12773, Republic of Korea;

k. Lyudmila Kalinkina – Poliny Osipenko 14/1 – 98, Moscow, 123007, Russian Federation;

l. Andrey Meleynikov – The Taras Shevchenko embankment 1/2, 190, Moscow, 121248, Russian Federation; and

m. Ivan Solovev – ul. Sklizkova d 116 korp 1, kv 106, Tver', 170028, Russian Federation.

SUMMARY

1. This action arises from a fraudulent scheme to hack into the SEC's online Electronic Data Gathering, Analysis, and Retrieval ("EDGAR") system to obtain nonpublic documents containing earnings announcements of publicly-traded companies, and to then use that information to profit by trading in advance of the information becoming public. The scheme was the second part of a long-term effort, the first phase of which targeted at least three newswire services.

2. Starting in at least May 2016 and continuing into at least October 2016, Defendant Ieremenko and others working with him used a variety of deceptive means to obtain thousands of nonpublic "test filings" from the SEC's EDGAR system's servers. In some instances, these test filings included submissions by public companies that contained earnings results and other material

information that the companies had not yet released to the public. The hacked material nonpublic information was then transmitted to traders who, in connection with approximately 157 earnings announcements, used it to place profitable securities trades before the information was made public.

3. Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems, Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov (collectively, the "Trader Defendants") served as part of a network of securities traders located in the United States, Ukraine, and Russia, who received the hacked material nonpublic information, directly or indirectly, from Ieremenko. The Trader Defendants then monetized the information by purchasing or selling short the relevant securities and profiting from the market reaction once the information was disseminated to the public. The Trader Defendants then, directly or indirectly, kicked back a portion of the resulting trading profits to Ieremenko.

4. Defendants' scheme reaped over $4.1 million in gross ill-gotten gains from trading based on nonpublic EDGAR filings.

5. These illicit gains are in addition to gains generated during an earlier phase of the scheme in which Ieremenko and others hacked material nonpublic information from at least three newswire services. Most of the Trader Defendants previously traded nonpublic information hacked from newswire services during the previous phase of the scheme, including Sungjin Cho, Capyield, Olefir, Vorochek, Sabodakha, and Sarafanov. An individual with control over Spirit Trade also previously traded on information hacked from newswire services.

6. By engaging in the conduct described herein with the requisite scienter, Defendants violated, and unless enjoined, will continue to violate the securities laws.

NATURE OF PROCEEDING AND RELIEF SOUGHT

7. The SEC brings this action against Defendants pursuant to Section 20(b) of the Securities Act of 1933 ("Securities Act") [*15 U.S.C. § 77t(b)*] and Sections 21 and 21A of the

Securities Exchange Act of 1934 ("Exchange Act") [*15 U.S.C. §§ 78u and 78u-1*] to enjoin the transactions, acts, practices, and courses of business alleged in this Complaint and to seek orders of disgorgement, along with prejudgment interest, civil penalties, and such further relief that the Court may deem appropriate.

JURISDICTION AND VENUE

8. 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), 21(e), 21A, and 27 of the Exchange Act [*15 U.S.C. §§ 78u(d), 78u(e), 78u-1, and 78aa*].

9. Venue in this district is proper 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 purchases and sales of securities and acts, practices, transactions, and courses of business constituting the violations alleged in this Complaint occurred within the District of New Jersey, and were effected, directly or indirectly, by making use of the means, instruments, or instrumentalities of transportation or communication in interstate commerce, or of the mails, or the facilities of national securities exchanges. Specifically, the servers from which the material nonpublic information at issue was obtained through deceptive means were located in Middlesex County, New Jersey. Many of the illegal securities transactions were also conducted using various national securities exchanges, many of which handle orders using servers located in Middlesex County, New Jersey.

DEFENDANTS

The Hacker Defendant

10. **Oleksandr Ieremenko (a.k.a. Eremenko, Alex Boesky, Lamarez, Sergey Komarov, Anton Petrov, and Uladzimir Aleinikau)**, age 27, is a computer hacker who resides in Kiev, Ukraine. He was previously charged by the SEC and Department of Justice with securities fraud in connection with the deceptive acquisition of material nonpublic information via hacking

during the newswire phase of this scheme in *SEC v. Dubovoy, et al.*, District of New Jersey Case No. 15-cv-06076-MCA-MAH; and *United States v. Turchynov, et al.*, District of New Jersey Case No. 2:15-cr-00390. Ieremenko has not appeared in either case, and both remain pending against him.

The Trader Defendants

11. **Spirit Trade, Ltd.** is a company ostensibly headquartered in Hong Kong and controlled by a Ukrainian citizen residing in Kiev, Ukraine ("Individual 1"). On approximately 18 occasions in May 2016, a brokerage account in the name of Spirit Trade traded based on material nonpublic information hacked from EDGAR. Individual 1 previously traded based on material nonpublic information obtained through the hack of at least one newswire service during the first phase of this scheme.

12. **Sungjin Cho**, age 38, resides in Los Angeles, California and was co-founder and co-owner of CYGS, LLC, a proprietary securities trading firm charged by the SEC in March 2017 for acting as an unregistered broker-dealer. On approximately 66 occasions during the period, from May through October 2016, Sungjin Cho traded based on material nonpublic information hacked from EDGAR. Sungjin Cho traded using brokerage accounts in his name, the name of CYGS, and in the names of Relief Defendant Kyungja Cho and at least one other nominee ("Individual 3"). Sungjin Cho also previously traded based on material nonpublic information obtained through the hack of at least two newswire services during the first phase of this scheme.

13. **David Kwon**, age 44, resides in Los Angeles, California. On approximately 18 occasions during the period from July through October 2016, Kwon traded based on material nonpublic information hacked from EDGAR.

14. **Igor Sabodakha**, age 33, is a Ukrainian citizen residing in Kiev, Ukraine. On approximately 49 occasions during the period from May through October 2016, Sabodakha traded based on material nonpublic information hacked from EDGAR. He also previously traded based

on material nonpublic information obtained through the hack of at least two newswire services during the first phase of this scheme.

15. **Victoria Vorochek**, age 33, is a Ukrainian citizen residing in Severodonetsk, Ukraine. On approximately 39 occasions during the period from May to October 2016, she traded based on material nonpublic information hacked from EDGAR. She also previously traded based on material nonpublic information obtained through the hack of at least two newswire services during the first phase of this scheme.

16. **Ivan Olefir (a.k.a. Ifan Ifanov)**, age 34, is a Ukrainian citizen residing in the Kiev region of Ukraine. On approximately 95 occasions during the period from May through October 2016, Olefir traded based on material nonpublic information hacked from EDGAR. Olefir previously traded based on material nonpublic information obtained through the hack of at least one newswire service during the first phase of this scheme.

17. **Capyield Systems, Ltd.** is a proprietary securities trading firm supposedly headquartered in Belize and beneficially owned by Olefir in Ukraine. On approximately 102 occasions during the period from May 2016 through October 2016, Capyield traded based on material nonpublic information hacked from EDGAR. Based on the IP addresses used to access Capyield's brokerage accounts, the trading by Capyield appears to have been directed from Ukraine. Capyield also previously traded based on material nonpublic information obtained through the hack of at least two newswire services during the first phase of this scheme.

18. **Andrey Sarafanov**, age 36, is a Russian citizen residing in Dedovsk, Russia. On approximately 121 occasions during the period from July through October 2016, Sarafanov traded based on material nonpublic information hacked from EDGAR using accounts in his own name and in the names of Relief Defendants Kalinkina, Meleynikov, and Solovev. In account opening documents, Sarafanov is identified as the "investment advisor" for accounts held in the names of

Kalinkina, Meleynikov, and Solovev and had exclusive trading authority for those accounts. He also previously traded in his own account based on material nonpublic information obtained through the hack of at least one of the newswire services during the first phase of this scheme.

RELIEF DEFENDANTS

19. **Kyungja Cho**, age 64, is Sungjin Cho's mother and resides in Korea. On approximately four occasions during August 2016, Sungjin Cho and/or others acting at his direction placed trades based on material nonpublic information hacked from EDGAR using accounts in Kyungja Cho's name.

20. **Lyudmila Kalinkina**, age 64, is a Russian citizen residing in Moscow, Russia. On approximately 80 occasions during the period from July to October 2016, Sarafanov placed trades based on material nonpublic information hacked from EDGAR using an account held in Kalinkina's name.

21. **Andrey Meleynikov**, age 46, is a Russian citizen residing in Moscow, Russia. On approximately 10 occasions during October 2016, Sarafanov placed trades based on material nonpublic information hacked from EDGAR using an account held in Meleynikov's name.

22. **Ivan Solovev**, age 43, is a Russian citizen residing in Moscow, Russia. On approximately 10 occasions during October 2016, Sarafanov placed trades based on material nonpublic information hacked from EDGAR using an account held in Solovev's name.

OTHER RELEVANT PERSONS AND ENTITIES

23. **Individual 1**, age 42, is a Ukrainian citizen residing in Kiev, Ukraine. Individual 1 controls Spirit Trade, Ltd. He also previously traded based on material nonpublic information obtained through the hack of at least one of the newswire services during the first phase of this scheme.

24. **CYGS, LLC** was, during the relevant period, a proprietary securities trading firm, co-founded and co-owned by Sungjin Cho. CYGS was charged by the SEC in March 2017 for acting as an unregistered broker-dealer. *See In the Matter of CYGS, LLC*, Exchange Act Release No. 80356. Sungjin Cho traded on the basis of material nonpublic information hacked from EDGAR using an account in the name of CYGS. Kwon also had a trading account with CYGS. During the relevant time period, CYGS had an office in Ukraine. An account in the name of CYGS was also used previously to trade based on material nonpublic information obtained through the hack of at least one of the newswire services during the first phase of this scheme.

25. **Individual 2**, age 26, is a Ukrainian citizen residing in Kiev, Ukraine. Before and during the period of the EDGAR hack, he was a friend and business associate of Ieremenko. A cryptocurrency account associated with Individual 2 paid for access to a server (the below-described "Exfiltration Machine") that was used to hack and exfiltrate test filings from the EDGAR system.

26. **Individual 3**, age 37, resides in Las Vegas, Nevada. During the period from July through October 2016, Sungjin Cho and/or others at his direction placed approximately 29 trades based on material nonpublic information hacked from EDGAR using accounts in Individual 3's name. An account in Individual 3's name was also used previously to trade based on material nonpublic information obtained through the hack of at least one of the newswire services during the first phase of this scheme.

27. **Individual 4**, age 33, is a Ukrainian citizen residing in Kiev, Ukraine. He is an associate of Ieremenko and several of the other Defendants, including Sungjin Cho and Sabodakha. Individual 4 also participated in the newswire phase of the scheme.

TERMS USED IN THIS COMPLAINT

Options

28. A stock option, commonly referred to as an "option," gives its purchaser-holder the right to buy or sell shares of an underlying stock at a specified price prior to the expiration date. Options are generally sold in "contracts," which give the option holder the opportunity to buy or sell 100 shares of an underlying stock.

29. A "call" option gives the purchaser-holder of the option the right, but not the obligation, to purchase a specified amount of an underlying security at a specified price within a specific time period. Generally, the buyer of a call option anticipates that the price of the underlying security will increase during a specified period of time.

30. A "put" option gives the purchaser-holder of the option the right, but not the obligation, to sell a specified amount of an underlying security at a specified price within a specific time period. Generally, the buyer of a put option anticipates that the price of the underlying security will decrease during a specified period of time.

Short-Selling

31. 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 price. 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, a profit results; if, however, the price rises, a loss results.

Contracts for Differences

32. A contract for difference ("CFD") is a stock derivative that is an agreement between two parties to exchange the difference in value of an underlying stock between the time the contract is opened and the time it is closed. If the share price increases for the underlying security, the seller pays this difference to the buyer. If, however, the underlying share price declines, the buyer must

pay the seller the difference. Generally speaking, an investor anticipating a rise in the price of the referenced security will buy a CFD, and an investor anticipating a decrease in the price of the referenced security will sell a CFD.

33. 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.

34. Generally, the investor in a CFD position benefits by acquiring the future price movement of the underlying common stock without having to pay for or take formal ownership of the underlying shares.

35. Generally, the investor in a CFD is not required to pay for the underlying shares of the security. Instead the CFD investor pays only the transaction fees charged by the CFD provider. Thus, a CFD, like a stock option, allows an investor to recognize significant value from an underlying security's price movement without having to pay for the underlying shares.

36. The counterparty to a CFD transaction often hedges the risk by buying or selling on a national securities exchange the reference security underlying the CFD or a related stock option in an amount and at a price that matches the risk position taken by the CFD seller.

Malware, Spoofing, and Phishing

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

38. "Spoofing" is the deceptive act of creating an email or other electronic communication that falsely appears to have been sent by or originate from a known or trusted source.

39. "Phishing" is the deceptive practice of sending a spoofed communication in order to induce individuals to reveal personal information, such as passwords or other credentials, or to deliver malware designed to compromise the recipient's computer.

IP Address

40. 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.

41. Often, IP addresses can be used to identify the geographical location of the server through which a computer accessed the Internet. Thus, in simple terms, it is like a return address on a letter.

42. An individual can hide the IP address from which he or she is accessing the Internet by a number of different techniques and tools. Such means allow individuals to assume and use IP addresses different than their own in a deceptive manner, including IP addresses identified with different geographical regions.

User Agent String

43. A "user agent string" is a line of text sent to each website accessed by a user, which identifies the name and version of the web browser being used. Each version of each web browser has its own distinctive user agent string, and Internet domains often maintain a log containing the user agent string of each web browser that has accessed the website.

Domain

44. 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.

FACTS

The Newswire Hacking Scheme

45. Each of the Defendants, other than Spirit Trade and Kwon, was involved in an earlier phase of the instant scheme, which similarly involved the exfiltration through hacking of material nonpublic information used for illegal securities trading.

46. Specifically, Ieremenko, a Ukrainian hacker, was involved in the hacking of at least three newswire services, one after another. And Defendants Sungjin Cho, Sabodakha, Olefir, Capyield, Vorochek, and Sarafanov each traded on information hacked from one or more of the newswire services.

47. Newswire services edit and disseminate press releases for publicly-traded companies in the United States. Until the newswire services publish a press release to the general public, often at a specific pre-announced time, the sensitive financial information in the press release constitutes nonpublic information that may be material.

48. Issuers routinely provide draft press releases to the newswire services. These often contain material nonpublic information to be included in the final public version of the press release. Consequently, for each press release, there is a window of time between when the company provides a draft press release to a newswire service and when the newswire service publishes the release to the public (the "trading window"). These trading windows vary between a few minutes and a few days.

49. From 2010 until 2015, Ieremenko and others hacked multiple newswire services' computer systems and accessed over 100,000 draft press releases before they were published. Once Ieremenko and others obtained the material nonpublic information from the newswire services, they monetized the information by providing the not-yet-published press releases to a network of traders. The traders, often using nominees, quickly placed trades based on the hacked information. The

traders compensated the hackers, including Ieremenko, for the information by either paying regular fees for access to the hacked press releases or by kicking back a portion of their trading profits.

50. In 2015, Ieremenko's illegal access to the newswire services was disrupted, and he and others were charged for their roles in the newswire hacking scheme. *See SEC v. Dubovoy, et al.*, District of New Jersey Case No. 2:15-cv-06076; *United States v. Turchynov, et al.*, District of New Jersey Case No. 2:15-cr-00390; *United States v. Korchevsky, et al.*, Eastern District of New York Case No. 1:15-cr-00381. These cases remain pending and unresolved as to Ieremenko, and, upon information and belief, he remains at large in Ukraine.

The EDGAR Hacking Scheme

Overview

51. In early 2016, Ieremenko and others working with him focused on a new source of material nonpublic information that could be used for securities trading: the SEC's Electronic Data Gathering, Analysis, and Retrieval system, known as "EDGAR."

52. Public companies and others who are required or elect to file forms with the SEC may file those forms using EDGAR. Many of those forms are intended to become public, and the filers use EDGAR as a means of quickly and efficiently distributing information to the investing public. For example, companies often file material information about their financial performance via EDGAR, such as Forms 8-K that contain quarterly earnings or other market-moving information.

53. Prior to making information public through an EDGAR filing, filers may also elect to submit "test filings" to EDGAR. Test filings are draft versions of EDGAR filings that are meant to ensure that an EDGAR filing is in the correct format, free from errors, and will be accepted for filing by EDGAR. Test filings are not meant for public dissemination and are not publicly available.

Test filers also sometimes elected to include material nonpublic information – *e.g.*, drafts of forthcoming Forms 8-K – that had not yet been publicly released.

54. An EDGAR filer submitting a test filing could request a "return copy," which was a version of the test filing that the filer was able to view after submitting it to EDGAR. During the time period of the conduct described in this Complaint, return copies of test filings were maintained on SEC computer servers located in Middlesex County, New Jersey, but were not publicly available.

55. In the spring of 2016, Ieremenko and others working with him launched several concurrent efforts to surreptitiously exfiltrate material nonpublic information located on the SEC's EDGAR servers.

56. Ieremenko simultaneously employed a variety of deceptive techniques as part of his coordinated effort to hack EDGAR in order to attempt to access material nonpublic information that could be used to profitably trade securities, including (a) using hacking techniques to circumvent pages of the EDGAR system that required users to login with their credentials to access user identification information; (b) misrepresenting himself as an authorized EDGAR filer and accessing nonpublic test filings within the EDGAR system; (c) using numerous aliases to conceal his control of an IP address used in the EDGAR hack and a related domain used in previous hacks of newswire services; and (d) inducing SEC computer users to open documents containing malware sent via spoofed, phishing emails that falsely represented they had been sent by SEC security personnel. Some of these efforts were successful in accessing material nonpublic information for trading.

57. Ieremenko's deceptive acts created the false appearance that he was an authorized user of the EDGAR system and ultimately allowed him to penetrate the EDGAR computer network to access certain nonpublic return copies of EDGAR test filings. Beginning on or about May 3, 2016, and continuing until at least October 20, 2016, Ieremenko and others working with him used deception to hack and download thousands of then-unpublished return copies of test filings. Some,

but not all, of those return copies contained material nonpublic information that could be used to trade securities.

58. Some of the hacked test filings included corporate earnings results. It is common for financial analysis firms to estimate or predict a given issuer's quarterly or annual earnings. The "market" reaches a consensus expectation based in part on these different predictions. When an issuer releases its earnings, the share price for that issuer often increases if its earnings exceed the market expectation and often decreases if its earnings fall short.

59. The period of time between the filing of a test filing and creation of a return copy, and the subsequent publication of the information contained in the test filing, created a trading window, which allowed Ieremenko to pass, directly or indirectly, the fraudulently obtained information to the Trader Defendants before the information was released to the market. As a result, the Trader Defendants had an improper trading advantage over other market participants, because they had material information from hacked EDGAR test filings before that information was publicly disseminated.

60. The Trader Defendants capitalized on this advantage by initiating trades before the information was released to the market. The Trader Defendants profited on both positive and negative earnings news by either buying securities or selling them short depending on their anticipation of how the market would respond to the information in the hacked EDGAR test filings.

61. The Trader Defendants concealed their access to the hacked information and their trading activities through the use of multiple brokerage accounts and entities, often using accounts in the name of nominees.

62. On information and belief, the Trader Defendants also furthered and substantially assisted the scheme by making payments, directly or indirectly, to Ieremenko. In November 2016, Sungjin Cho sent an email to an individual who had taken part in the scheme to trade on

information hacked from EDGAR and attached an "accounting for the 2nd quarter that u traded."

In a subsequent email two days later, Sungjin Cho wrote again to the same trader:

> Just emailed u when I was going over the accounting w[ith] my group over q2 and q3. I know I probably didn't explain and that would naturally make you have questions so I apologize if I didn't explain how the trading strategy fund worked. This straetgy [sic] we been working on for over 5 years now and the reason why we were able to keep our team toegher [sic] for this long (without 1 person stealing it and run outside money) was agreement to disclose all activity and outside money. Any outside account (like yours at [U.S. Broker-Dealer]) we disclose the prices and has[sic] to pay a cut to the coding team (it ended up being 45% so I actually take a loss on yours, but I told u a third is the cut so I'm gonna honor that and your [U.S. Broker-Dealer] account was small so all good . . . .

On information and belief, Sungjin Cho's reference to a 45% cut of the traders' profits to the "coding team" referred to compensation to Ieremenko and others working with him. Such a payment method is consistent with the manner in which Ieremenko and others were compensated during the newswire phase of the scheme.

63. After the relevant earnings information was publicly issued, the price of the securities often changed as the market learned the previously undisclosed information. The Trader Defendants then closed out the securities positions and reaped substantial profits, a portion of which they kicked back, directly or indirectly, to Ieremenko.

64. Collectively, the Trader Defendants used the information hacked from EDGAR to realize over $4.1 million in gross illicit gains.

The Proof of Concept Period – May 3, 2016 to May 19, 2016

65. In the spring of 2016, Ieremenko and others working with him began efforts to hack the EDGAR System, using common hacking techniques to hunt for access to material nonpublic information. For example, Ieremenko circumvented EDGAR controls that required user authentication and then obtained access to nonpublic EDGAR logs that contained user and document identification information associated with test filings made by authorized EDGAR users.

Ieremenko then employed the information he obtained from these nonpublic logs to access certain return copies of test filings.

66. When accessing EDGAR, Ieremenko was expressly warned, *inter alia*, that "[The EDGAR] system is Federal property and is to be used only for authorized government purposes by users who have been granted access rights by the Office of Information Technology. Misuse of this computer system is a violation of Federal law (Pub. L.99-474)." He was also notified that only authorized filers were permitted to access EDGAR:

> Notice: Before you can electronically file with the SEC on EDGAR, you must become an EDGAR filer with authorized access codes. This website will allow you to create a Form ID and submit it for authorization to the SEC. Upon acceptance, you will receive a unique CIK via e-mail. You will then return to this site and use your CIK and a passphrase to create your EDGAR access codes. Once you have your access codes, you may use EDGAR to begin electronically filing. This website may also be used to regenerate your access codes.

67. When Ieremenko and others working with him accessed EDGAR test filings, they misrepresented themselves as authorized EDGAR filers and as using EDGAR for an authorized government purpose.

68. In the spring of 2016, Ieremenko or others working with him also sent a series of malicious emails to sec.gov email addresses in an effort to obtain material nonpublic information from SEC systems. The emails were spoofed to appear as if they were being sent by SEC security personnel. The spoofed emails contained malware-infected documents, and this phishing successfully infected several SEC computer workstations in an attempt to obtain material nonpublic information.

69. Ieremenko accessed the SEC's EDGAR system using a Romanian IP address he had previously used to send emails between two email accounts he controlled. During the EDGAR hack, he used this IP address to access a key EDGAR directory and test filings. Ieremenko had previously used a domain associated with that same Romanian IP address in connection with two of

the earlier newswire hacks. Ieremenko used a series of aliases to conceal his control of this domain and the Romanian IP address. Additionally, Ieremenko's newswire hacks and his EDGAR intrusions involved an identical user agent string, which indicates that the same web browser was used in both attacks.

70. Ieremenko first successfully accessed a test filing on or about May 3, 2016. On that same day, Ieremenko began manually exfiltrating electronic copies of test filings.

71. Starting the next day, May 4, 2016, Ieremenko put into action his scheme to monetize the information he obtained through deception. He did this by using third-party traders, in yet another significant effort to mislead and insulate himself from detection by separating his hacking from the resulting illegal trading.

72. Specifically, at 1:09 PM ET, Ieremenko, using deceptive hacking techniques, accessed and exfiltrated from EDGAR a test filing for Issuer 1, a public company whose securities trade on the New York Stock Exchange. The hacked test filing contained negative material nonpublic information about Issuer 1's soon-to-be-announced first quarter 2016 financial results and had been uploaded to EDGAR less than an hour earlier.

73. After downloading the information, on information and belief, Ieremenko, directly or indirectly, passed the information to one or more individuals at Spirit Trade, which, between 2:57 PM and 3:59 PM ET, sold short 5,500 shares of Issuer 1 stock using a U.S.-based brokerage account. As discussed above, Spirit Trade is controlled by Individual 1. Individual 1 also engaged in illegal trading in connection with the earlier period of the hacking scheme that targeted the newswire services.

74. On May 4, 2016, after the close of the market and just minutes after Spirit Trade's last shorting transaction, Issuer 1 issued its earnings report for the quarter ending March 31, 2016, and announced a decline in revenue from the prior period and lower than expected earnings and

revenue guidance for the following quarter. During the next day of trading, Issuer 1's stock price dipped 9% on the news.

75. On May 5, 2016, within the first 35 minutes of the opening of the market, Spirit Trade had closed out its short position in Issuer 1 stock, making approximately $9,185 in gross illegal profits.

76. Ieremenko and Spirit Trade repeated this pattern several times during the month of May 2016, illegally profiting from both positive and negative financial news contained in hacked test filings.

77. Another example involved a test filing submitted to EDGAR on behalf of Issuer 2, a public company whose stock trades on the Nasdaq. On May 6, 2016, Issuer 2 announced that it would hold a webcast to discuss its second quarter 2016 financial results after market close on May 19, 2016.

78. At approximately 3:32 PM ET on May 19, 2016, a test filing containing positive material nonpublic information about Issuer 2's not-yet-released second quarter 2016 financial results was uploaded to EDGAR. Ieremenko deceptively accessed and extracted Issuer 2's test filing only six minutes later. From approximately 3:42 PM to 3:59 PM ET, Spirit Trade purchased Issuer 2 stock. After market close on May 19, 2016, Issuer 2 publicly released its second quarter earnings report and announced that it expected to deliver record earnings in fiscal 2016. During the next day of trading, Issuer 2's stock price rose 14% on the news. By 10:46 AM ET on May 20, 2016, Spirit Trade had closed out its position in Issuer 2, making approximately $274,663 in gross illegal profits.

79. In all, during the month of May 2016, Spirit Trade made $496,740 in gross illegal profits from its trading on the information obtained through Ieremenko's deceptive extraction of approximately 17 companies' test filings.

80. Spirit Trade's last trade was May 20, 2016. Less than two months later, Spirit Trade's account was closed, and the proceeds of its illegal trading were transferred out.

The Automated Exfiltration Period – May 18, 2016 to October 2016

81. After confirming that the material nonpublic information obtained by hacking EDGAR could be used to trade profitably, Ieremenko increased the scale of the fraudulent scheme.

82. On May 18, 2016, Ieremenko, or others working in concert with him, deployed a server (the "Exfiltration Machine") using a program to perform on an automated basis the deceptive conduct he performed manually earlier in the month. A few days earlier, a cryptocurrency account associated with Individual 2 paid for access to this server. Ieremenko's Exfiltration Machine employed the same deceptive techniques to misrepresent itself as an authorized EDGAR filer and access return copies of test filings. Ieremenko's Exfiltration Machine then periodically downloaded electronic return copies of test filings on a regular schedule.

83. During this period of the scheme, Ieremenko's Exfiltration Machine accessed EDGAR through an IP address and domain ostensibly located in Lithuania. This IP address used by Ieremenko's Exfiltration Machine had not been used in the previous manual exfiltration period. During this time period, Ieremenko also used two other IP addresses ostensibly located in Switzerland and Luxembourg to download a small number of test filings. On information and belief, Ieremenko used various tools and techniques to make it appear that the IP addresses from which he was accessing the Internet were located in different geographical regions. Ieremenko's use of numerous IP addresses identified with disparate parts of Europe was yet another effort to conceal the hack, his identity, and his physical location.

84. Ieremenko's Exfiltration Machine enabled Ieremenko to obtain hacked test filings on a greater scale. At the same time that Ieremenko employed his Exfiltration Machine, more traders began to monetize the information. Again, he used third-party traders as part of his fraudulent

scheme in an effort to deceptively insulate himself from detection and liability. And again, both the Trader Defendants and Ieremenko were essential participants in this fraudulent scheme; neither could profit without the other.

85. During this period, which ran from at least May 18, 2016, until at least October 20, 2016, Ieremenko worked with traders located in the United States, Ukraine, and Russia to monetize his illegal conduct, one group operating together from California and Ukraine (the "California and Ukraine Trading Group"), and, on information and belief, another trader operating in Russia. Each of the Trader Defendants knew, were reckless in not knowing, should have known, or consciously avoided knowing that they were each trading upon hacked information and participating, assisting, and acting in furtherance of a scheme to defraud.

86. With the exception of Kwon, each member of the California and Ukraine Trading Group also traded in connection with the earlier phase of the fraudulent scheme on the basis of hacked information obtained from newswire services. Moreover, as alleged below, Sungjin Cho and Sabodakha are also connected to Ieremenko through mutual connections to Individual 4, who also traded in the newswire phase of the scheme. Between May 18, 2016, and October 20, 2016, members of the California and Ukraine Trading Group traded approximately 369 times in the trading window between the time a test filing was exfiltrated from EDGAR and a press release announcing the substance of the filing was thereafter publicly released.

87. By July 2016, Sarafanov, a Russian trader who had participated in the newswire phase of the scheme, also began to trade on hacked EDGAR test filings. During February to July 2015, a period when Ieremenko and others working with him were exfiltrating press releases from a specific newswire service, Sarafanov traded ahead of approximately 19 earnings announcements. Of these 19 trades by Sarafanov, approximately 16 were trades in advance of announcements by issuers who used the hacked newswire service.

88. On or about July 18, 2016, Sarafanov began placing his first trades based on material nonpublic information in EDGAR test filings that had been exfiltrated by Ieremenko. Sarafanov traded in an account in his own name as well as in accounts that he controlled in the names of at least three other persons residing in Russia, Relief Defendants Kalinkina, Meleynikov, and Solovev. Between approximately July 18, 2016, and October 25, 2016, accounts controlled by Sarafanov traded approximately 121 times in the period between the time a test filing was exfiltrated from EDGAR and the time that a press release announcing the substance of the filing was publicly released.

89. Together, the California and Ukraine Trading Group and Sarafanov traded approximately 490 times on material nonpublic information deceptively obtained from EDGAR for total gross profits of over $3.6 million. The following are examples that illustrate their trading based on hacked EDGAR test filings:

Issuer 3 - Second Quarter 2016 Announcement

90. On July 7, 2016, Issuer 3, a public company whose stock trades on the New York Stock Exchange, announced that it planned to release its second quarter 2016 financial results before market open on July 26, 2016.

91. At approximately 11:39 AM ET on July 22, 2016, a test filing containing negative material nonpublic information about Issuer 3's second quarter financial results was uploaded to EDGAR. At approximately 2:33 PM ET on July 22, 2016, Ieremenko's Exfiltration Machine fraudulently obtained Issuer 3's test filing containing the not-yet-released financial results.

92. On July 25, 2016, the day before Issuer 3 was expected to publicly release its second quarter results, Sungjin Cho (using an account in Individual 3's name), Sarafanov, Olefir, and Capyield all began shorting the stock of Issuer 3; Sungjin Cho and Sarafanov also began buying Issuer 3 put options; and Sabodakha and Vorochek began selling Issuer 3 CFDs.

93. At approximately 2:24 PM ET on July 25, 2016, Sabodakha began selling Issuer 3 CFDs. Approximately 23 minutes later, at 2:47 PM ET, Vorochek also began selling Issuer 3 CFDs. Approximately 27 minutes later, at 3:14 PM ET on July 25, 2016, Capyield began selling short Issuer 3 stock. Approximately 15 minutes later, at 3:29 PM ET, Sungjin Cho, using an account in the name of Individual 3, also began selling short Issuer 3 stock. Approximately nine minutes later, at 3:38 PM ET, Olefir also began selling short Issuer 3 stock. Approximately three minutes later, at 3:41 PM ET, Sungjin Cho began purchasing Issuer 3 put options in an account in his own name, and Sarafanov began purchasing Issuer 3 put options in an account in his own name. At approximately 3:59 PM ET, Sungjin Cho began purchasing Issuer 3 put options and selling short Issuer 3 stock using the CYGS account. At approximately 4:06 PM ET, Sarafanov, using an account in the name of Relief Defendant Kalinkina, began selling short Issuer 3 stock. Also at 4:33 PM ET, Sarafanov began selling short Issuer 3 stock in his own brokerage account. All of these trades would be expected to result in immediate profits if the company issued negative news and the stock price declined.

94. Before market open on July 26, 2016, Issuer 3 issued a press release announcing second quarter financial results that were largely below analysts' estimates. On July 26, 2016, Issuer 3 stock closed down approximately 4% from the previous day's closing price.

95. By the end of that day, July 26, 2016, Sungjin Cho, Sarafanov, Olefir, Capyield, Sabodakha, and Vorochek had closed out their trading positions in Issuer 3, except for Sarafanov's and Sungjin Cho's put option positions, which were closed out on July 27, 2016, and July 28, 2016, respectively. In all, these Defendants made gross illegal profits of approximately $96,000 by trading on the basis of Issuer 3's hacked EDGAR test filing.

Issuer 4 - Second Quarter 2016 Announcement

96. On July 12, 2016, Issuer 4, a public company whose stock trades on the Nasdaq, announced that it would release its financial results for the second quarter of 2016 after market close on August 4, 2016.

97. At approximately 2:19 PM ET on August 4, 2016, a test filing containing negative material nonpublic information about Issuer 4's second quarter 2016 results was uploaded to EDGAR. Approximately eight minutes later, at 2:27 PM ET, Ieremenko's Exfiltration Machine fraudulently obtained Issuer 4's test filing.

98. Shortly thereafter, seven of the Trader Defendants began taking short positions in Issuer 4. At approximately 3:19 PM ET on August 4, 2016, Capyield and Sarafanov (using Relief Defendant Kalinkina's account) began selling short stock of Issuer 4. At 3:27 PM ET, Olefir began buying Issuer 4 put options. At 3:28 PM ET, Sarafanov began selling short stock of Issuer 4 in an account in his own name, and at 3:40 PM ET, Sarafanov began buying Issuer 4 put options in an account in his own name. At 3:33 and 3:36 PM ET, respectively, Sabodakha and Vorochek each began selling Issuer 4 CFDs. At 3:38 PM ET, Sungjin Cho began buying Issuer 4 put options in an account in his own name, and at 3:40 PM ET and 3:46 PM ET, respectively, Sungjin Cho began selling short Issuer 4 stock using accounts in the names of Individual 3 and CYGS. At 3:54 PM ET, Kwon began buying Issuer 4 put options. All of these trades would be expected to result in immediate profits if the company issued negative news and the stock price declined.

99. At 4:01 PM ET on August 4, 2016, Issuer 4 issued a press release announcing that its total billings and revenue for the quarter were below expectations.

100. The next trading day, August 5, 2016, the market reacted, and Issuer 4's stock closed down approximately 12% from the previous day's closing price.

101. By the end of the same day, August 5, 2016, Kwon, Capyield, Olefir, Sabodakha, Vorochek, Sungjin Cho, and Sarafanov had closed out their trading positions in Issuer 4, except for Sungjin Cho's short positions held in CYGS's account, which were closed out on August 9, 2016. In all, these defendants made gross illegal profits of approximately $307,000 by trading on the basis of Issuer 4's hacked EDGAR test filing.

Issuer 5 - Second Quarter 2016 Announcement

102. On July 20, 2016, Issuer 5, a public company whose stock trades on the Nasdaq, announced that it would report its second quarter 2016 financial results after market close on August 3, 2016.

103. At 9:22 PM ET on July 29, 2016, a test filing containing positive material nonpublic information about Issuer 5's second quarter 2016 financial results was uploaded to EDGAR. At 9:58 PM ET, Ieremenko's Exfiltration Machine fraudulently obtained Issuer 5's test filing.

104. On August 3, 2016, at 3:13 PM ET, Capyield began purchasing stock of Issuer 5. At 3:15 PM ET, Sarafanov began purchasing stock of Issuer 5 in an account in the name of Relief Defendant Kalinkina. At 3:25 PM ET, Sarafanov began purchasing stock of Issuer 5 in an account in his name. At 3:35 PM ET, Olefir began purchasing stock of Issuer 5. At 3:38 PM ET, Sabodakha began purchasing Issuer 5 CFDs. At 3:46 PM ET, Sungjin Cho began purchasing stock of Issuer 5 in an account in the name of Individual 3. At 3:57 PM ET, Vorochek began purchasing Issuer 5 CFDs. At 3:58 PM ET, Sungjin Cho began purchasing stock of Issuer 5 in a CYGS account. All of these trades would be expected to result in immediate profits if the company issued positive news and the stock price increased.

105. After market close on August 3, 2016, Issuer 5 issued a press release announcing stronger than anticipated fiscal second quarter sales growth, higher than projected gross profit

margins, better than expected operating income, and that Issuer 5 was increasing its full year 2016 financial guidance.

106. On August 4, 2016, stock of Issuer 5 closed approximately 8% higher than the previous day's closing price. By the end of that day, August 4, 2016, Sungjin Cho, Sabodakha, Vorochek, Capyield, Olefir, and Sarafanov had closed their positions, reaping gross illegal profits of over $61,000.

Issuer 2 - Third Quarter 2016 Earnings Announcement

107. On August 5, 2016, Issuer 2 announced that it would release its third quarter 2016 financial results after market close on August 18, 2016.

108. At approximately 6:04 PM ET on August 17, 2016, a test filing containing positive material nonpublic information about Issuer 2's third quarter 2016 earnings was uploaded to EDGAR. Approximately 13 minutes later, at 6:17 PM ET, Ieremenko's Exfiltration Machine fraudulently obtained Issuer 2's test filing.

109. The following trading day, August 18, 2016, at approximately 2:45 PM ET, Sarafanov began buying Issuer 2 call options in an account in his own name. At 2:48 PM ET, Sarafanov began purchasing Issuer 2 stock in an account in the name of Relief Defendant Kalinkina. At approximately 3:05 and 3:07 PM ET, respectively, Vorochek and Sabodakha began purchasing Issuer 2 CFDs. At 3:06 PM ET, Sarafanov began purchasing Issuer 2 stock. At 3:29 PM ET, Sungjin Cho began purchasing Issuer 2 stock in an account in his own name. At 3:38 PM ET, Sungjin Cho began purchasing Issuer 2 stock in the CYGS account. At 3:41 PM ET, Olefir began purchasing Issuer 2 stock, and Sungjin Cho began purchasing Issuer 2 stock using an account in the name of Individual 3. At approximately 3:44 PM ET, Sungjin Cho also began purchasing Issuer 2 call options using an account in his mother Relief Defendant Kyungja Cho's name. At 3:46 PM ET, Olefir began purchasing Issuer 2 CFDs. At 3:49 PM ET, Capyield began purchasing Issuer 2 stock.

And at 3:51 PM ET, Kwon began purchasing Issuer 2 stock. All of these trades would be expected to result in immediate profits if the company issued positive news and the stock price increased.

110. After market close on August 18, 2016, Issuer 2 announced record results for third quarter 2016, including record earnings per share and an all-time high for new orders.

111. On August 19, 2016, Issuer 2 stock closed approximately 7% higher than the previous day's closing price. By the end of that day, August 19, 2016, Sarafanov, Vorochek, Sabodakha, Capyield, Sungjin Cho, Olefir, and Kwon had closed out their trading positions, except for Kalinkina's and CYGS's positions in Issuer 2 stock, which were closed out on August 22, 2016. These Defendants made gross illegal profits of approximately $285,000 by trading on the basis of Issuer 2's hacked EDGAR test filing.

Issuer 6 - Second Quarter 2016 Announcement

112. On July 18, 2016, Issuer 6, a public company whose securities trade on the Nasdaq, announced that it would release its second quarter 2016 financial results after market close on August 8, 2016.

113. At approximately 8:25 AM ET on August 8, 2016, a test filing containing positive material nonpublic information about Issuer 6's second quarter 2016 earnings was uploaded to EDGAR. At approximately 1:19 PM ET, Ieremenko's Exfiltration Machine fraudulently obtained Issuer 6's test filing.

114. At 3:37 PM ET on August 8, 2016, Vorochek began purchasing Issuer 6 CFDs. At 3:41 PM ET, Sabodakha began purchasing Issuer 6 CFDs. At approximately 3:42 PM ET, Capyield began purchasing Issuer 6 stock. At 3:48 PM ET, Sungjin Cho began purchasing Issuer 6 stock in a CYGS account. At 3:49 PM ET, Sungjin Cho began purchasing Issuer 6 call options in an account in his own name. At 3:50 PM ET, Sungjin Cho began purchasing Issuer 6 stock in Individual 3's account. At 3:55 PM ET, Kwon began purchasing Issuer 6 call options. At 3:56 PM ET, Sungjin

Cho began purchasing Issuer 6 call options in Relief Defendant Kyungja Cho's account. On this day, Sungjin Cho purchased Issuer 6 stock or call options in at least four different accounts, including those in the names of CYGS, Individual 3, and Kyungja Cho. All of these trades would be expected to result in immediate profits if the company issued positive news and the stock price increased.

115. After market close on August 8, 2016, Issuer 6 announced its second quarter 2016 financial results and that they were on-track or ahead of Issuer 6's expectations for the quarter.

116. On August 9, 2016, Issuer 6 stock closed approximately 22% higher than the previous day's closing price. By the end of that day, August 9, 2016, Capyield, Vorochek, Sabodakha, Sungjin Cho, and Kwon had all closed out their trading positions, making gross illegal profits of approximately $82,300.

Ieremenko Loses Access to EDGAR

117. In October 2016, SEC IT personnel patched EDGAR software in response to a detected attack on the system, which also had the effect of preventing Ieremenko from accessing test filings.

118. After Ieremenko's access to EDGAR was blocked, some Trader Defendants' continued to trade for a short time based on material nonpublic information that had been previously hacked but not yet publicly released. Shortly thereafter, however, with Ieremenko's access to new test filings cut off, their illegal trading ahead of the release of EDGAR test filings ceased entirely.

119. Efforts to compromise EDGAR continued into early 2017. For example, at approximately the same time that Ieremenko lost access to EDGAR test filings in October 2016, he returned to his previous efforts to compromise SEC computer workstations through malware, which he had delivered through phishing emails, spoofed to appear to have been sent by SEC

security personnel. Other efforts also continued, including by other people, though none of the post-October 2016 efforts appear to have led to access to test filings containing material nonpublic information or to trading.

120. During the summer of 2018, Ieremenko, using the alias "Lamarez," appeared to take credit for the hacks of both the newswire services and EDGAR. Specifically, in response to an online communication regarding hacking, Ieremenko boasted about his successful hack of several specific newswire companies and "sec.gov" and provided links to English- and Russian-language news coverage of the newswire hacks.

Connections Between Defendants

121. Defendants' participation in a common scheme is demonstrated through (a) their parallel trading, often during very brief trading windows, in the securities of issuers whose test filings were exfiltrated from EDGAR by Ieremenko; (b) for many of them, the pattern of trading in both the newswire and EDGAR phases of the scheme; and (c) an extensive web of connections among them.

122. To begin, nearly all of the Defendants involved in the EDGAR hack were also involved in the previous hack of the newswire services. Specifically, during the period from 2013 through 2015, Sungjin Cho, Sabodakha, Olefir, Capyield, Vorochek, Sarafanov, and an individual who controlled Spirit Trade each traded on information that Ieremenko and others hacked from the newswire services.

123. Generally, the Trader Defendants' trading profits soared during periods when they had access to hacked information and plummeted when they did not.

124. For example, considered collectively, the California and Ukraine Trading Group made hundreds of thousands of dollars trading on hacked earnings announcements in 2013. The following year, when they did not have access to hacked information from any newswire service

because the hack had been disrupted, their trading profits were a small fraction of what they had been when they had access to hacked information.

125. In 2015, during another period of newswire hacking, trading by the California and Ukraine Trading Group was again very profitable. But after Ieremenko's hacking of the newswire services was disrupted again in mid-2015, these same Defendants' trading dwindled and was much less profitable.

126. Later, during the six months of the EDGAR hacking scheme, these same Defendants' trading again was extremely profitable.

127. In addition, many of the Trader Defendants often traded on the same hacked earnings announcements, taking trading positions that indicated that they had a common belief about the market's reaction to an upcoming announcement. This uniformity is significant because corporate earnings announcements may contain a mix of positive and negative news such that anticipated market reaction may not be readily determinable.

128. Defendants are also connected by a web of business affiliations and relationships, often spanning years. These connections are evidenced through, among other things, electronic communications and shared use of specific IP addresses, the latter indicating that they accessed the Internet from the same network access point. On information and belief, Defendants are also in possession of additional relevant evidence of their connections to each other and the fraudulent scheme alleged herein to which the SEC does not currently have access.

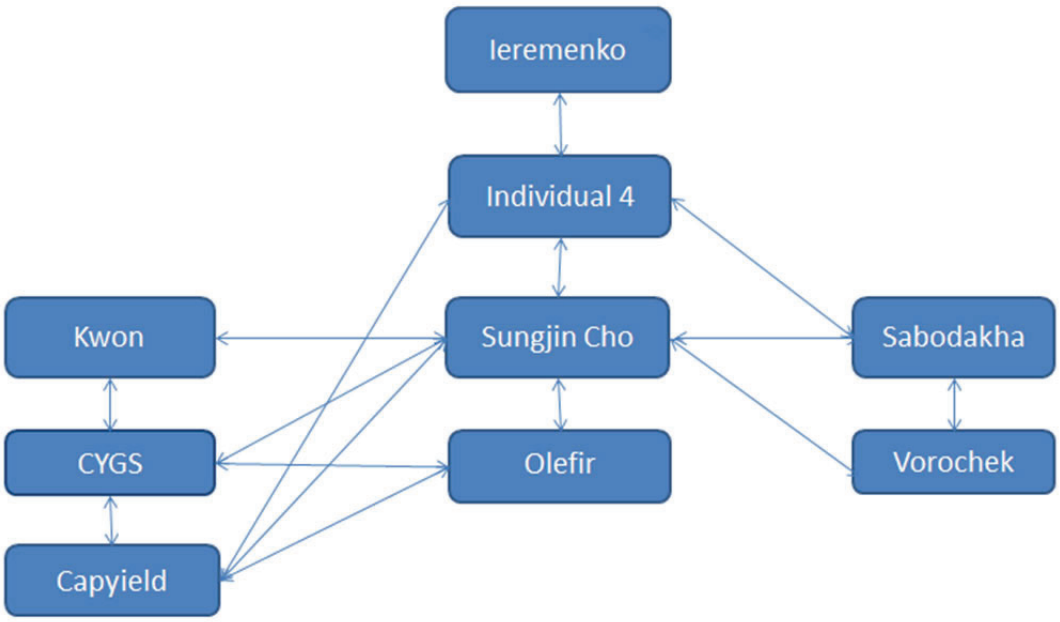
Connections Between Ieremenko and Spirit Trade

129. As alleged above, in May 2016, Ieremenko first tested his ability to monetize material nonpublic information he obtained through hacking the EDGAR system by, directly or indirectly, passing the information to one or more individuals at Spirit Trade. Spirit Trade then used that hacked material nonpublic information to trade before earnings announcements.

130. Ieremenko and Spirit Trade are connected through Individual 1 and Individual 2. Prior to May 2016, Ieremenko and Individual 2 were friends and business associates, and on information and belief, Individual 2 worked with Ieremenko on the EDGAR hack. A cryptocurrency account associated with Individual 2 was used to pay for Ieremenko's Exfiltration Machine. Likewise, prior to May 2016, Individual 1, who had control over Spirit Trade, and Individual 2 were associates. In or about April and May of 2016, on information and belief, Individual 1 and Individual 2 were in contact with one another.

Connections Between Ieremenko and the California and Ukraine Trading Group

131. The connections between Ieremenko and the California and Ukraine Trading Group are illustrated below:



132. Individual 4 is a Ukrainian citizen through whom many of the Trader Defendants are connected to Ieremenko. Individual 4, like Ieremenko, Sabodakha, and other Defendants, lives in Kiev and traded during the newswire phase of the scheme. Prior to the EDGAR hack, Individual 4 and Ieremenko were in contact through email, including an email exchange in which Individual 4

requested business advice from Ieremenko regarding a potential cryptocurrency business Individual 4 was exploring.

133. Individual 4, in turn, is associated with Sungjin Cho, Sabodakha, and Capyield. For example, on May 24, 2013, during the newswire phase of the scheme, an email account associated with Capyield set up a trading account for Individual 4, and trades were contemporaneously placed in both Sungjin Cho's and Individual 4's accounts at two different broker-dealers using the same IP address. Based on emails exchanged between the two, Individual 4 has been an associate of Sabodakha since at least 2013, and in 2018, Individual 4 and Sabodakha also served as CEO and COO, respectively, of a cryptocurrency company.

134. Sungjin Cho is also a long-time associate of Sabodakha, Olefir, Vorochek, Capyield, and other Ukrainian traders. Sungjin Cho and Olefir have also been working together as securities traders for at least a decade. In 2010, Sungjin Cho co-founded CYGS, a proprietary securities trading firm. After its founding, CYGS opened additional offices, including an office in Ukraine.

135. Capyield is another proprietary securities trading firm affiliated with Sungjin Cho and Olefir. In September 2014, Olefir became the beneficial owner of Capyield. Prior to that, in January 2012, Capyield made a $200,000 loan to Sungjin Cho's trading firm, CYGS.

136. Sungjin Cho is also a long-time associate of Sabodakha and Vorochek. In August 2012, Sungjin Cho emailed to Sabodakha a photograph of himself with others who appear to include Sabodakha and Vorochek. Sabodakha then forwarded the photograph to Vorochek.

137. Sungjin Cho is also connected to Kwon, who described himself as Sungjin Cho's "uncle" in a September 2017 document describing a $236,000 "gift" from Kwon to Sungjin Cho.

138. In November 2016, after the conclusion of the trading on information hacked from EDGAR, Kwon sent Sungjin Cho a summary of trading in Kwon's brokerage account from August through October 2016. This summary included Kwon's trading in issuers whose test filings had

been exfiltrated by Ieremenko. In subsequent emails, Kwon sent Sungjin Cho invitations to edit a shared spreadsheet calculating trading gains and losses. Kwon advised Sungjin Cho to "use this spreadsheet to get the accurate figures and tell you [sic] other traders to do the same . . . ."

Defendants' Use of Nominee Accounts

139. Several of the Trader Defendants also conducted illegal trading using accounts held in the names of others, including, but not limited to, Kyungja Cho, Kalinkina, Meleynikov, Solovev, and Individual 3.

140. Specifically, Sungjin Cho controlled and directed the trading that occurred in the account ostensibly owned by his mother, Kyungja Cho. During the time period of the EDGAR hack, Sungjin Cho placed four trades using this account and made approximately $21,000 in gross illegal profits.

141. Sungjin Cho also controlled an account ostensibly owned by Individual 3. During the time period of the EDGAR hack, Sungjin Cho or someone at his direction placed approximately 29 trades using this account and made approximately $134,000 in gross illegal profits.

142. Sarafanov also had exclusive trading authority for accounts ostensibly owned by Relief Defendants Kalinkina, Meleynikov, and Solovev. During the time period of the EDGAR hack, Sarafanov placed approximately 100 trades using these accounts and made approximately $413,000 in gross illegal profits.

Overview of Defendants' Trading During the Period of the EDGAR Hack

143. During the period from May through October 2016, when Defendants had access to hacked return copies of EDGAR test filings as a result of Ieremenko's deceptive conduct, the Trader Defendants' trading in securities of issuers whose information was contained in hacked EDGAR test filings was remarkably more successful than trading in securities of issuers whose information was not obtained by the EDGAR hack. Put another way, when the Trader Defendants

traded in the securities of issuers whose test filings had recently been exfiltrated through Ieremenko's hack of EDGAR, they had a much higher win rate.

144. The table below illustrates the comparison of the Trader Defendants' non-hacked trading activity to their hacked trading activity:

	Trading Episodes Not Related to an EDGAR Hack			Trading Episodes Related to an EDGAR Hack			
Trader	Trading Episodes	Net Profit / Loss	Win Rate*	Trading Episodes	Net Profit / Loss	Win Rate*	Gross Profit / Loss
Spirit Trade	1	-$79	0%	18	$477,799	96%	$496,740
Sungjin Cho	150	-$17,813	39%	66	$650,192	89%	$679,862
David Kwon	63	$33,061	48%	18	$401,474	78%	$404,243
Igor Sabodakha	44	-$1,440	21%	49	$57,712	74%	$69,120
Victoria Vorochek	8	-$646	17%	39	$91,092	72%	$108,637
Ivan Olefir	111	-$21,217	37%	95	$338,164	70%	$449,010
Capyield	397	-$22,756	39%	102	$670,147	68%	$832,967
Andrey Sarafanov	63	-$7,667	58%	121	$901,604	76%	$1,094,435
Total	**837**	**-$38,559**	**45%**	**508**	**$3,588,184**	**77%**	**$4,135,015**

*Win Rate is the dollar-weighted fraction of a Trader Defendant's trading episodes that resulted in positive net profits. The outcome of each trading episode (either 0 for an episode with net losses or 1 for an episode with net gains) is multiplied by dollars invested for the episode. This quantity is summed across all the Trader Defendant's trading episodes and then divided by the Trader Defendant's aggregate dollars invested.

145. The Trader Defendants' success rates when they had access to hacked earnings information are particularly notable because earnings announcements may reflect positive or negative news. The ability of these defendants to profit consistently, regardless of the direction of the price change, indicates that they had the benefit of deceptively-acquired, material nonpublic information. Despite this illegal advantage, it is not surprising that the Trading Defendants did not trade successfully based on this information 100% of the time. This is so because, unlike some other corporate announcements, it is not always predictable how the market will react to a given earnings announcement. For example, an earnings release may contain a combination of positive and negative news, may match analysts' preexisting expectations, or the market may focus on a

particular aspect of a release at the exclusion of other information that points to a contrary conclusion.

146. During the period when the Trader Defendants had access to hacked EDGAR filings, they were also much more likely to trade ahead of corporate earnings events that were the subject of hacked EDGAR test filings than earnings events that were not.

147. Each of the Trader Defendants traded significantly more heavily in hacked events than would be expected if their trading were uncorrelated with the EDGAR hacks: from 4 times as many hacked events as would be expected by random chance for Sungjin Cho, Kwon, and Vorochek to 14 times as many hacked events as would be expected by random chance for Spirit Trade's trades.

148. It is virtually impossible that the Trader Defendants' disproportionate trading in hacked events, as opposed to thousands of other earnings events during the same time period, could have occurred by random chance. Statistical analysis shows that for each of the Trader Defendants, the odds of that trader trading so disproportionately in hacked events by random chance ranged from less than 7 in 10 million to less than 1 in 1 trillion. This means that for each of the Trader Defendants, it is nearly impossible that their trading is uncorrelated with the hack of the EDGAR system.

CONCLUSION

149. At all relevant times, Ieremenko, Spirit Trade, Sungjin Cho, Kwon, Capyield, Olefir, Sabodakha, Vorochek, and Sarafanov participated in a scheme to defraud. The fraudulent scheme required all of the Defendants' participation in order to succeed.

150. Ieremenko obtained, through deception, material nonpublic information from the SEC's EDGAR system and provided it, directly or indirectly, to the other Defendants. The other

Defendants monetized the material nonpublic information by making profitable securities trades and then compensated Ieremenko for his deceptive conduct.

151. In perpetrating the fraud, Ieremenko made a series of material misrepresentations, including his use of spoofed phishing emails, malware, and representations that he was an authorized EDGAR filer.

152. Spirit Trade, Sungjin Cho, Kwon, Capyield, Olefir, Sabodakha, Vorochek, and Sarafanov provided substantial assistance to Ieremenko's hack of the EDGAR system by monetizing the hacked information through securities trading.

153. Spirit Trade, Sungjin Cho, Kwon, Capyield, Olefir, Sabodakha, Vorochek, and Sarafanov concealed their access to the hacked information and their trading activities through the use of multiple brokerage accounts and entities, often using accounts in the name of nominees. Ieremenko's decision to utilize other members of the scheme to monetize the hacked information was itself a deceptive act. Defendants also used domains and IP addresses indicating locations in several different countries to facilitate and further conceal their fraud.

154. The information hacked from EDGAR included material nonpublic information.

155. Hacked information was used to place securities trades on numerous national securities exchanges through numerous U.S.-based broker dealers, in a manner that utilized the instrumentalities of interstate commerce.

156. Ieremenko knew, was reckless in not knowing, or should have known that his material misstatements and omissions were false or materially misleading and that he was participating, assisting, and acting in furtherance of a scheme to defraud.

157. Spirit Trade, Sungjin Cho, Kwon, Capyield, Olefir, Sabodakha, Vorochek, and Sarafanov knew, were reckless in not knowing, should have known, or consciously avoided knowing that the material nonpublic information they received, directly or indirectly, from Ieremenko was

obtained through a scheme to defraud and through material misstatements and omissions. Indeed, Spirit Trade, Sungjin Cho, Kwon, Capyield, Olefir, Sabodakha, Vorochek, and Sarafanov knew, were reckless in not knowing, should have known, or consciously avoided knowing that they were each participating, assisting, and acting in furtherance of a scheme to defraud.

158. Relief Defendants Kyungja Cho, Kalinkina, Meleynikov, and Solovev and others have obtained funds as part, and in furtherance, of violations of the securities laws, and, as a consequence, these Relief Defendants have been unjustly enriched.

FIRST CLAIM FOR RELIEF
Violations of Exchange Act Section 10(b) and Rule 10b-5 Thereunder
(All Defendants)

159. The SEC realleges and incorporates by reference each and every allegation in paragraphs 1 through 158, inclusive, as if they were fully set forth herein.

160. By engaging in the conduct in 2016 that is 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 which operated or would operate as a fraud or deceit upon any person in connection with the purchase or sale of any security.

161. By engaging in the foregoing conduct in 2016, Defendants violated, and unless enjoined will continue 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*].

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

162. The SEC realleges and incorporates by reference each and every allegation in paragraphs 1 through 158, inclusive, as if they were fully set forth herein.

163. By engaging in the conduct in 2016 that is described above, Defendants knowingly, recklessly, or negligently in connection with the offer or sale of securities, by the 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.

164. By engaging in the foregoing conduct in 2016, Defendants violated, and unless enjoined will continue to violate, Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*].

THIRD CLAIM FOR RELIEF
Aiding and Abetting Violations of Exchange Act Section 10(b) and Rule 10b-5 Thereunder
(Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems, Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov)

165. The SEC realleges and incorporates by reference each and every allegation in paragraphs 1 through 158, inclusive, as if they were fully set forth herein.

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

167. Through their illicit trading, payments directly or indirectly to Defendant Ieremenko, and other means alleged above, Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems, Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov knowingly provided substantial assistance to, and thereby aided and abetted, Ieremenko's violations of the securities laws.

168. By engaging in the foregoing conduct in 2016, pursuant to Exchange Act Section 20(e) [*15 U.S.C. § 78t*], Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems, Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov violated, an unless enjoined will continue 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*].

FOURTH CLAIM FOR RELIEF
Aiding and Abetting Violations of Securities Act Section 17(a)
(Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems, Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov)

169. The SEC realleges and incorporates by reference each and every allegation in paragraphs 1 through 158, inclusive, as if they were fully set forth herein.

170. As alleged above, Defendant Ieremenko and others violated Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*].

171. Through their illicit trading, payments directly or indirectly to Defendant Ieremenko, and other means alleged above, Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems, Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov knowingly provided substantial assistance to, and thereby aided and abetted, Defendant Ieremenko's violations of the securities laws.

172. By engaging in the foregoing conduct in 2016, pursuant to Securities Act Section 15(b) [*15 U.S.C. § 77o(b)*], Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems,

Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov violated, and unless enjoined will violate again, Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*].

FIFTH CLAIM FOR RELIEF
Unjust Enrichment Liability
(Relief Defendants Kyungja Cho, Kalinkina, Meleynikov, and Solovev)

173. The SEC realleges and incorporates by reference each and every allegation in paragraphs 1 through 158, inclusive, as if they were fully set forth herein.

174. Relief Defendants Kyungja Cho, Kalinkina, Meleynikov, and Solovev have obtained funds as part, and in furtherance, of the securities violations alleged above, and under circumstances in which it is not just, equitable, or conscionable for these individuals to retain the funds. As a consequence, these Relief Defendants have been unjustly enriched.

PRAYER FOR RELIEF

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

I.

Finding that Defendants violated the provisions of the federal securities laws alleged herein;

II.

Permanently restraining and enjoining each Defendant from, directly or indirectly, engaging in conduct in violation of Exchange Act Section 10(b) [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5], and Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*], and permanently enjoining Defendants Spirit Trade, Ltd., Sungjin Cho, Kwon, Capyield Systems, Ltd., Olefir, Sabodakha, Vorochek, and Sarafanov from aiding and abetting any violation of Exchange Act Section 10(b) [*15 U.S.C. § 78j(b)*] and Rule 10b-5 thereunder [*17 C.F.R. § 240.10b-5*], and Securities Act Section 17(a) [*15 U.S.C. § 77q(a)*];

III.

Ordering Defendants to disgorge, with prejudgment interest, all illicit trading profits, avoided losses, or other ill-gotten gains received by any person or entity as a result of the actions alleged herein;

IV.

Ordering Defendants to pay civil penalties pursuant to Sections 21 and 21A of the Exchange Act [*15 U.S.C. § 78u, 78u-1*]; and

V.

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

JURY DEMAND

Pursuant to Rule 39 of the Federal Rules of Civil Procedure, Plaintiff demands that this case be tried to a jury.

Dated: January 15, 2019

Respectfully submitted,

s/ *Cheryl L. Crumpton*

Cheryl L. Crumpton
Stephan J. Schlegelmilch
Robert A. Cohen
Joseph G. Sansone
Carolyn M. Welshhans

U.S. SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, D.C. 20549
Tel: (202) 551-4459 (Crumpton)
Tel: (202) 551-4935 (Schlegelmilch)
CrumptonC@SEC.gov
SchlegelmilchS@SEC.gov

Of Counsel:

David E. Bennett
Michael C. Baker
Laura K. D'Allaird
Adam B. Gottlieb
Arsen R. Ablaev
Jason J. Burt
James A. Scoggins
David W. Snyder
Jonathan M. Warner
U.S. SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, DC 20549

DESIGNATION OF AGENT FOR SERVICE

Pursuant to Local Rule 101.1(f), because the U.S. Securities and Exchange Commission (the "SEC") does not have an office in this district, the United States Attorney for the District of New Jersey is hereby designated as eligible as an alternative to the SEC to receive service of all notices or papers in the captioned action. Therefore, service upon the United States or its authorized designee, J. Andrew Ryman, Chief, Civil Division, United States Attorney's Office for the District of New Jersey, 402 E. State Street, Room 430, Trenton, NJ 08608 shall constitute service upon the SEC for purposes of this action.

Dated: January 15, 2019

Respectfully submitted,

s/ *Cheryl L. Crumpton*

Cheryl L. Crumpton
Stephan J. Schlegelmilch
U.S. SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, DC 20549
Tel: (202) 551-4459 (Crumpton)
Tel: (202) 551-4935 (Schlegelmilch)
CrumptonC@SEC.gov
SchlegelmilchS@SEC.gov