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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.