THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY
TRENTON VICINAGE

MAIA PHARMACEUTICALS, INC., Plaintiff, v. SASANK C. KUNADHARAJU, Defendant.	CIVIL ACTION NO.

VERIFIED COMPLAINT IN SUPPORT OF PLAINTIFF'S APPLICATION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTIVE RELIEF

Plaintiff MAIA Pharmaceuticals, Inc. ("MAIA" or the "Company") through its undersigned counsel, Porzio, Bromberg & Newman, PC and Law Office of David R. Lurie PLLC, by way of Verified Complaint against defendant Sasank C. Kunadharaju ("Kunadharaju"), alleges and says:

INTRODUCTION

1. This is a proceeding seeking, among other things, to address the Defendant's misappropriation – and likely theft – of MAIA's most competitively valuable confidential information,

2. MAIA is a New Jersey pharmaceutical company that has spent millions of dollars, and countless hours of research and development, to develop trade-secrets, including respecting manufacturing know how, that are among the Company's most valuable assets.

3. Until January 14, 2022, Defendant was MAIA's Senior Director, Product Development.

4. In that capacity, Defendant had responsibilities related to three of the Company's products. By virtue of his seniority, however, Defendant had the ability to access files containing virtually all of the Company's trade secrets and other confidential information, including access to a password protected secure cloud server, on which MAIA maintains its most sensitive documents containing its trade secrets and other competitively sensitive and confidential information.

5. Defendant entered into two comprehensive confidentiality and non-disclosure agreements with the Company whereby he agreed, among other things, to access – and use – MAIA's confidential information solely for work-related purposes, and to maintain their confidentiality.

6. On January 14, 2022, Defendant informed the Company of his intention to resign, and later agreed to a February 4, 2022 departure date. Defendant later admitted to the Company that he had resolved to resign at the beginning of December 2021, but chose to wait to provide his notice about 45 days later.

7. On January 20, 2022, the Company presented Defendant with a normal course termination agreement, which – if executed – would have entitled him to receive a severance payment. The draft agreement, among other things, included an affirmation of Defendant's existing contractual non-disclosure, confidentiality, as well as non-competition, obligations to the Company.

8. The document also listed the several Company projects on which Defendant had worked accurately stating that they fell within Defendant's existing confidentiality and restrictive covenant and non-competition obligations.

9. Defendant, however refused to execute the draft termination agreement, and stated that he preferred to be bound only by his existing confidentiality and non-competition agreements with the Company which he (falsely) described as "vague."

10. Recognizing that Defendant's statements were suspicious, the Company immediately conducted a review of Defendant's history of accessing the Company's secure server. The review disclosed that, during the months preceding his notice of resignation, Defendant had systematically downloaded 30,000 Company documents from the secure server.

11. The documents at issue contain much of the Company's most competitively sensitive materials, including pharmaceutical formulae, laboratory procedures, manufacturing processes, business agreements and price information.

12. Many of the documents Defendant downloaded were entirely unrelated to the three MAIA products he worked on; accordingly, he accessed and downloaded such materials in express violation of his NDAs with the Company.

13. Additionally, Defendant downloaded approximately 10,000 of the documents at issue between during and after December 2021, after (on his own account) Defendant had decided to leave the Company and was, apparently, preparing for his departure.

14. On January 21, 2022, Defendant informed the Company that he had decided to leave the Company effective retroactively on January 14, 2022, not February 4, 2022, as previously agreed. On that date, he also sent an electronic message reiterating his rejection of the draft termination agreement.

15. Also on January 21, 2021, MAIA's consultant retrieved Defendant's Company laptop from Defendant at his residence, and later delivered it to a forensic computer specialist for examination, who reviewed the laptop in conjunction with a log that recording every time that the

Defendant accessed, and downloaded data from, MAIA's secure sever. The forensic specialist's examination established among other things:

16. First, that Defendant had deleted virtually all of the MAIA related work product that previously resided on the hard drive of the device, including all of the documents containing MAIA's confidential information that he had downloaded from the secure server.

17. Second, that, during or around the time that Defendant been downloading huge volumes of documents containing MAIA's trade secrets and other confidential information from the Company's secure server, Defendant attached a host of devices to the computer's USB ports, including a number of mass storage devices and other devices that may be used to download or copy files. It is not only possible, but likely that some or all of the documents that Defendant downloaded from MAIA's secure server were downloaded directly to – or were transferred to – one or more of these devices; but a forensic review of each of these storage devices will be required to determine what data Defendant transferred to them.

18. Third, also during and around time periods in which he was downloading Company confidential information from the MAIA secure server, Defendant used his Company computer to access a personal "Google Drive" account – an Internet based service that may be utilized to store large volumes of data. Once again, it is not only possible, but likely that some or all of the documents that Defendant downloaded from MAIA's secure server were downloaded directly to – or were transferred to – Defendant's Google Drive account. As in the case of the mass storage devices, it is necessary for MAIA's forensic investigator to obtain access to the Google Drive account to determine what MAIA data Defendant transferred to that account.

19. Finally, while Defendant deleted virtually all of his work-related files from his Company laptop, he did not delete the "browser history" records, reflecting the websites the

Defendant used the laptop to visit, including the website used to access MAIA's secure server. Those and certain other records establish that Defendant used another, non-Company, computer to download and purloin MAIA's documents containing MAIA's trade secrets.

20. The log that recorded all of Defendant's visits to MAIA's secure server indicates that on December 10 and 17, 2021, Defendant used his password to access the secure server and to download approximately 6,500 containing some of MAIA's most competitively sensitive and valuable trade secrets.

21. The laptop's browser history, however, shows that the Defendant did not visit the secure server from that Company device on those two days. Accordingly, the forensic examiner concluded that Defendant employed another computer, in addition to his MAIA-issued Company computer, to access the secure server, download and purloin MAIA's trade secrets and other confidential information.

22. On January 24, 2022, MAIA sent Defendant a cease a desist letter reciting the volume and nature of the MAIA materials he had misappropriated from MAIA's secure server, and demanding that Defendant, among other things, list all Company confidential information he downloaded, state where all copies of such information was located, and identify every person or entity to which he had transferred such materials

23. On January 25, 2022, Defendant sent a responsive letter effectively conceding that he had the downloaded the materials, but offering no account of what he had done with them.

24. Accordingly, on January 26, 2022, the Company sent Defendant a second letter stating that Defendant's initial response was "unsatisfactory," and demanding a certification, under penalty of perjury, identifying, among other things. any "device, location, person or entity" (other than the Company laptop) to which MAIA documents were copied or transferred, via email, server,

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.