

1 JONATHAN H. BLAVIN (State Bar No. 230269)
jonathan.blavin@mto.com

2 NICHOLAS D. FRAM (State Bar No. 288293)
Nicholas.Fram@mto.com

3 MICA L. MOORE (State Bar No. 321473)
Mica.Moore@mto.com

4 MUNGER, TOLLES & OLSON LLP
560 Mission Street
5 Twenty-Seventh Floor
San Francisco, California 94105-2907

6 Telephone: (415) 512-4000

7 Facsimile: (415) 512-4077

8 Attorneys for LinkedIn Corporation

9 UNITED STATES DISTRICT COURT
10 NORTHERN DISTRICT OF CALIFORNIA

11
12
13
14
15
16
17
18
19
20
21
22
23
24

LinkedIn Corporation,

Plaintiff,

vs.

Mantheos Pte. Ltd., Jeremiah Tang, Yuxi
Chew, and Stan Kosyakov

Defendants.

Case No.

COMPLAINT FOR:

- (1) BREACH OF CONTRACT;**
- (2) FRAUD AND DECEIT (CAL. CIV. CODE §§ 1572, 1710);**
- (3) VIOLATION OF THE LANHAM ACT, 15 U.S.C. § 1125(C);**
- (4) MISAPPROPRIATION**

DEMAND FOR JURY TRIAL

1 Plaintiff LinkedIn Corporation (“LinkedIn” or “Plaintiff”), by and through its attorneys,
2 brings this Complaint against Mantheos Pte. Ltd. (“Mantheos”), Jeremiah Tang, Yuxi Chew, and
3 Stan Kosyakov (collectively, “Defendants”) for injunctive relief and damages. LinkedIn alleges as
4 follows:

5 1. LinkedIn is a global online social network with a professional focus. LinkedIn has
6 nearly 800 million members in over 200 countries and territories around the globe. Its mission is
7 to connect the world’s professionals to make them more productive and successful. Through its
8 proprietary platform, LinkedIn allows its members to create, manage, and share their professional
9 histories and interests online.

10 2. At the heart of LinkedIn’s platform are its members. Members create profiles on
11 LinkedIn’s platform, which serve as their professional online identities. Members share their
12 information on LinkedIn’s platform in order to network with, and to be found by, other
13 professionals on LinkedIn. When a member posts an educational experience on her profile, crafts
14 a narrative description of her skills, or makes a new connection, the member does so for these
15 particular purposes.

16 3. In order to protect the data that LinkedIn’s members entrust to it, LinkedIn’s User
17 Agreement prohibits data “scraping”: the accessing, extraction, and copying of data by automated
18 bots on a large scale. LinkedIn also has invested significant technical and human resources to
19 detect, limit, and block data scraping. These measures are designed to ensure that LinkedIn’s
20 website is used for its intended purpose of facilitating meaningful professional connections and to
21 protect members’ expectations that their data will be used specifically for that purpose.

22 4. It is important that LinkedIn members have control over the information that they
23 choose to publish about themselves. People and careers evolve, and the information and
24 vocabulary that people use to describe themselves and their experiences evolve as well. It is

1 therefore critical that members are able to control their information and how they describe
2 themselves. That is why when members delete information from LinkedIn, LinkedIn deletes it too.

3 5. Defendants' entire business model is premised on scraping data from LinkedIn's
4 website. Notwithstanding the conditions in LinkedIn's User Agreement prohibiting data scraping,
5 to which Defendants consented on multiple occasions, Defendants use an extensive network of
6 fake LinkedIn accounts to gain access to areas of LinkedIn's platform that are accessible only to
7 real, logged-in LinkedIn members. Defendants have then used those fake accounts to scrape
8 millions of member profiles in automated fashion, including profile data that is only available for
9 viewing by other LinkedIn members who have logged in to their accounts. Defendants sell to their
10 customers on-demand scraping of more than two dozen LinkedIn member data fields, including
11 members' work experience, education, skills, titles, posts, comments, and reactions to the posts of
12 others.

13 6. Defendants are not shy about their illegal conduct. Defendants advertise their data
14 scraping service extensively on their website, and openly refer to LinkedIn's website as a "Gold
15 Mine" for personal information. Indeed, it appears the *only* service Defendants provide is scraping
16 LinkedIn members' data. Defendants sell that service to all who are willing to pay for it,
17 undermining LinkedIn's members' privacy and control over their information. Defendants have
18 also included LinkedIn's trademarks in materials marketing Mantheos's scraping service to the
19 public, without LinkedIn's consent, thereby associating LinkedIn's services with their illicit
20 activity.

21 7. Once Defendants have scraped LinkedIn members' data, the data can end up in any
22 number of databases and may be used for any purpose. Further, once scraped, neither LinkedIn
23 nor its members can prevent Defendants or their customers from using that data to send spam,
24

1 from selling or inadvertently exposing member data to scammers, or from combining data with
2 other data to create extensive private databases, among other activities.¹

3 8. Defendants have also defrauded LinkedIn by hundreds of thousands of dollars
4 through their fake accounts. As part of their scheme, Defendants use fake accounts to enroll in
5 subscriptions for LinkedIn's Sales Navigator. Sales Navigator is a paid subscription service that
6 provides sales professionals with services that promote quick identification and creation of new
7 customer leads and sales opportunities, in addition to helping professionals stay current about their
8 existing connections and key accounts. These services include advanced search capabilities.
9 LinkedIn offers legitimate members one month of free Sales Navigator service prior to the
10 commencement of a paid subscription. Defendants circumvent this limitation by signing up for
11 Sales Navigator subscriptions, typically through fake accounts using prepaid virtual debit card
12 numbers, and then using Sales Navigator to scrape members' profile data during the free period.
13 When LinkedIn attempts to charge the accounts for the following month of Sales Navigator service
14 after the conclusion of the free month, the associated cards are declined, and LinkedIn is never
15 paid. Defendants then continue using Sales Navigator to scrape members' data, without paying,
16 until LinkedIn cuts off access, at which point Defendants sign up for new Sales Navigator
17 subscriptions through different fake accounts.

18 9. Defendants have committed unlawful acts of breach of contract, fraud and deceit,
19 and misappropriation, and their conduct violates the Lanham Act's prohibitions of trademark
20 dilution by disparagement, 15 U.S.C. § 1125(c) et seq.

21 10. Defendants' unlawful conduct has harmed and threatens the LinkedIn platform in
22 several ways. First, their actions violate the trust that LinkedIn members place in the company to
23

24 ¹ See, e.g., <https://www.wired.com/story/clearview-ai-new-tools-identify-you-photos/> (noting that Clearview AI "has scraped 10 billion photos" from websites) (last accessed Feb. 1, 2022).

1 protect their information. Defendants sell LinkedIn members' personal data to third parties for
2 profit, depriving members of control over their personal data, and magnifying the harms that
3 LinkedIn has suffered. Defendants have also defrauded LinkedIn out of hundreds of thousands of
4 dollars in revenue that they were properly charged for after their free trials concluded, but that they
5 did not pay. Defendants' unauthorized scraping has also forced LinkedIn to expend time and
6 resources investigating and responding to their misconduct, including by locating and investigating
7 the unauthorized activities of the hundreds of fake accounts that Defendants have used on
8 LinkedIn's platform. Finally, Defendants' association of its scraping activities with LinkedIn's
9 trademarks in its marketing materials tarnishes LinkedIn's brand.

10 11. Defendants' activities, if not enjoined, threaten ongoing and irreparable harm to
11 LinkedIn, including to its reputation and substantial consumer goodwill. LinkedIn brings this
12 lawsuit to stop Defendants' conduct, which harms LinkedIn's members and harms LinkedIn by
13 eroding the trust that lies at the core of LinkedIn's relationship with its members. LinkedIn is also
14 entitled to actual damages and exemplary damages as a result of Defendants' misconduct.

15 **JURISDICTION AND VENUE**

16 12. This Court has federal question jurisdiction over this action under 28 U.S.C.
17 §§ 1331 and 1338 because this action alleges violations of the Lanham Act, 15 U.S.C. § 1051 et
18 seq. The Court has supplemental jurisdiction over LinkedIn's state law claims under 28 U.S.C.
19 § 1367, because they arise out of the same nucleus of operative facts as the claims based on federal
20 law.

21 13. This Court also has diversity jurisdiction over this action under 28 U.S.C. § 1332.
22 Plaintiff is a citizen of Delaware and California. Upon information and belief, Defendants are
23 citizens of Singapore and Germany. The amount in controversy exceeds \$75,000.

24

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.