

LinkedIn Sues Data Scraping Operation Over Million-Account Bot Army

Fake accounts scraped hundreds of profiles each before detection, as ProAPI kept creating new ones to keep the bots running



Rehmat Alam built a company that sold LinkedIn data to anyone willing to pay up to \$15,000 a month.

The problem with that, according to a lawsuit filed by LinkedIn is that he allegedly stole that data using millions of fake accounts that impersonated real people and then used those accounts to scrape your public and non-public data including post and comments.

LinkedIn filed the lawsuit against Alam and two companies he cofounded, ProAPIs Inc. and Netswift (SMC-Private) which was based on Pakistan for a breach of contract and a host of other claims.

The complaint describes his "industrial-scale fake account mill" that creates hundreds to thousands of new bogus profiles every day to harvest information from the professional networking site's one billion members.

Automated Scrapers, Fake Profiles And Stock Photos

According to the lawsuit, ProAPI use automated tools to create or take over thousands of email addresses, then use those to register LinkedIn accounts under false names with stock photo profile pictures.

Each fake account usually gets detected and restricted within hours by LinkedIn's security systems. But during that time a single fake profile can sometimes scrape hundreds of legitimate member profiles, extracting names, job histories, skills, education, awards and even posts and comments.

"These fake accounts generally are detected by LinkedIn's technical defenses and restricted within a few hours," the complaint says. "But in that brief period, they are sometimes able to scrape hundreds of LinkedIn profiles each, if not more."

The defendants don't appeal when their accounts get shut down, the lawsuit says. They simply create new ones as fast as LinkedIn can detect them, maintaining what the complaint describes as a continuous cycle of account creation and data extraction.

A \$15,000 Monthly Service

ProAPIs marketed its iScraper API tool openly on its website until recently, advertising it as a way to "scrape LinkedIn data efficiently in real-time and at scale." The company's pricing allowed customers to pay up to \$15,000 monthly for five million API calls at 150 requests per second.

The defendants promoted their ability to extract "comprehensive, up-to-the-second profile information" from LinkedIn. In marketing materials cited in the lawsuit, Alam wrote that customers could scrape "name, education history, position groups, languages, location, certifications, volunteer experience, patents and all other data that's public on personal profiles."

But LinkedIn says that ProAPI scraped non public information too. The fake accounts allowed ProAPIs to access information that members had chosen to make visible only to other logged-in LinkedIn users, according to the complaint.

Trust And Safety Are Overloaded By Fake Accounts

LinkedIn says that they had to spend hundreds of hours of employee time and resources trying to stop the fake accounts.

The company employs teams of engineers whose full-time job involves detecting fake accounts and preventing scraping through rate limiters, IP blocks, artificial intelligence models and proprietary algorithms.

The bots place a huge burden on their services and make substantially more request than a normal user would so it places strain on the system

"To maintain normal performance and limit service degradation for legitimate users, LinkedIn must continue to allocate additional capacity, resources, and security measures," the complaint states.

And...Founder Got Premium For Free

In an unusual part of the lawsuit LinkedIn accuses Alam of personal fraud for subscribing to LinkedIn Premium and Sales Navigator services multiple times using credit cards that were declined for payment. He obtained those services without ever paying for them.

LinkedIn Is Seeking A Shutdown

LinkedIn is asking the court for a permanent injunction that would bar the ProAPI from accessing its platform entirely. The company also wants an order requiring destruction of all scraped data and the code used to obtain it, plus notification to all customers who purchased the allegedly stolen information.

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 CORDELL A. BROWN (State Bar No. 356447)
Cordell.Brown@mto.com

4 MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty-Seventh Floor
5 San Francisco, California 94105-2907
Telephone: (415) 512-4000
6 Facsimile: (415) 512-4077

7 Attorneys for LinkedIn Corporation

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA

10
11 LinkedIn Corporation,

12 Plaintiff,

13 vs.

14 ProAPIs Inc., Netswift (SMC-Private)
15 Limited, Rehmat Alam,

16 Defendants.
17
18
19
20
21
22
23
24
25
26
27
28

Case No. 3:25-cv-8393

COMPLAINT FOR:

- (1) BREACH OF CONTRACT;
(2) FRAUD AND DECEIT (CAL. CIV.
CODE §§ 1572, 1710);
(3) BREACH OF THE COMPUTER
FRAUD AND ABUSE ACT, 18 U.S.C.
§ 1030;
(4) BREACH OF THE CALIFORNIA
COMPREHENSIVE DATA ACCESS
AND FRAUD ACT (CAL. PENAL CODE
§ 502);
(5) UNLAWFUL, UNFAIR OR
FRAUDULENT BUSINESS PRACTICES
(CAL. BUS. & PROF. CODE § 17200 ET
SEQ.);
(6) VIOLATION OF THE LANHAM
ACT, 15 U.S.C. § 1125(C);
(7) MISAPPROPRIATION;
(8) TRESPASS TO CHATTELS.**

DEMAND FOR JURY TRIAL

1 Plaintiff LinkedIn Corporation (“LinkedIn” or “Plaintiff”), by and through its attorneys,
2 brings this Complaint against ProAPIs Inc. (“ProAPIs”), Netswift (SMC-Private) Limited
3 (“Netswift”), and Rehmat Alam (collectively, “Defendants”) for injunctive relief and damages.
4 LinkedIn alleges as follows:

5 1. Defendants operate a vast network of continuously-created fake accounts—
6 numbering in the millions—that they use to log into LinkedIn and scrape LinkedIn member,
7 company, and school data, as well as member posts, reactions, and comments. LinkedIn’s
8 technical defenses regularly detect and restrict Defendants’ fake accounts within hours of their
9 creation. But in that time, each such fake account can sometimes scrape hundreds of profiles, if
10 not more. And despite LinkedIn restricting a very high percentage of these fake accounts,
11 Defendants persist in registering hundreds if not thousands of new accounts *per day*.

12 2. Although Defendants conceal how they obtain LinkedIn data, they freely
13 acknowledge that they offer “real-time, detailed data for individual and company LinkedIn
14 profiles” that is “comprehensive” and “up-to-the-second.”¹ They rent out their scraping services
15 to customers who pay up to \$15,000 per month to scrape LinkedIn. Defendants’ industrial-scale
16 fake account mill scrapes member information that real people have posted on LinkedIn, including
17 data that is only available behind LinkedIn’s password wall and that Defendants’ customers may
18 not otherwise be allowed to access, and certainly are not allowed to copy and keep in perpetuity.

19 3. Defendants conduct this illicit activity while including LinkedIn’s trademarks in
20 materials on their website without authorization. Doing so provides the false sense that LinkedIn
21 is somehow associated with or endorses Defendants’ unlawful business. To be clear: there is no
22 association or endorsement. What Defendants are doing is unlawful and must stop.

23 4. LinkedIn brings this action to curb Defendants’ unlawful behavior, preserve the
24 integrity of its platform, and protect and retain the trust of its members, who are at the heart of
25 LinkedIn’s platform. Members create profiles on LinkedIn’s platform to serve as their
26 professional online identities. Members share their information on LinkedIn in order to network
27

28 ¹ ProAPIs, *iScraper API v4.0*, <https://docs.proapis.com/iscraper-docs#tag/profiles-details> (last visited Oct. 1, 2025).

1 with, and to be found by, real people—other professionals on LinkedIn—not fake accounts
2 operated by bots whose only mission is to expropriate member data for profit.

3 5. In order to protect the data that LinkedIn’s members entrust to it, LinkedIn’s User
4 Agreement prohibits data “scraping”: the accessing, extraction, and copying of data by automated
5 bots. It also prohibits impersonating others or creating fake accounts—accounts that are not
6 backed by real people. LinkedIn has invested significant technical and human resources to detect,
7 limit, and block data scraping and fake accounts. These measures are designed to ensure that
8 LinkedIn’s website is used for its intended purpose of facilitating meaningful professional
9 connections between real people.

10 6. LinkedIn’s anti-scraping measures similarly help ensure that LinkedIn’s members
11 retain control over the information that they choose to publish about themselves on LinkedIn.
12 People and their careers evolve, and the information and vocabulary that people use to describe
13 themselves and their experiences evolve as well. It is important for members to be able to control
14 their information and how they describe themselves. That is why when members delete
15 information from LinkedIn, LinkedIn deletes it too.

16 7. Defendants’ scraping activities undermine LinkedIn’s members’ privacy and
17 control over their information. Once Defendants have scraped LinkedIn members’ data, that data
18 can end up in any number of databases and end up used for any purpose, without LinkedIn’s or its
19 members’ awareness. Indeed, on information and belief, Defendants’ business is built on selling
20 its scraping services to others. Neither LinkedIn nor its members can then prevent Defendants or
21 their customers from using that scraped data to send spam, from selling or exposing member data
22 to scammers, or from combining LinkedIn member data with other data to create extensive private
23 databases, among other activities.²

24 8. Defendants’ conduct, as alleged herein, constitutes unlawful acts of breach of
25 contract, fraud and deceit, misappropriation, and trespass to chattels, and violates the Lanham

26
27 ² See, e.g., DataVisor, *Web Scraping*, <https://www.datavisor.com/wiki/web-scraping/> (last visited
28 Oct. 1, 2025) (describing various fraudulent activities individuals in possession of scraped data
can engage in).

1 Act's prohibitions of trademark dilution by disparagement (15 U.S.C. § 1125(c)), the Computer
2 Fraud and Abuse Act (18 U.S.C. § 1030), California's Unfair Competition Law (Bus. & Prof.
3 Code § 17200 *et seq.*), and the Comprehensive Computer Data Access and Fraud Act (Cal. Penal
4 Code § 502).

5 9. Defendants' unlawful conduct has harmed and continues to threaten the LinkedIn
6 platform in multiple ways. It undermines the confidence that LinkedIn members place in the
7 company to protect their information. Defendants sell LinkedIn members' personal data to third
8 parties for profit, depriving members of control over their personal data, and magnifying the harms
9 that LinkedIn has suffered. Defendants' unauthorized scraping has also forced LinkedIn to expend
10 time and technical resources investigating and responding to their scraping, fake accounts, and
11 other misconduct. Their fake accounts pollute the LinkedIn platform which is designed to be used
12 by real people. Defendants' association of its scraping activities with LinkedIn's trademarks in its
13 marketing materials tarnishes LinkedIn's brand, falsely associating it with Defendants, when there
14 is no legitimate association.

15 10. Defendants recently appear to have substantially increased the rate at which they
16 generate fake accounts. Responding to such fraudulent activity will require a considerable
17 increase in the already marked expenditure of LinkedIn's time and technical resources.

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

23 **JURISDICTION AND VENUE**

24 12. This Court has federal question jurisdiction over this action under 28 U.S.C.
25 §§ 1331 and 1338 because this action alleges violations of the Lanham Act (15 U.S.C. § 1051 *et*
26 *seq.*) and the Computer Fraud and Abuse Act (18 U.S.C. § 1030). The Court has supplemental
27 jurisdiction over LinkedIn's state law claims under 28 U.S.C. § 1367, because they arise out of the
28 same nucleus of operative facts as the claims based on federal law.

13. Venue is proper in this Court because Defendants contractually consented to venue in this District. Defendants have consented to the User Agreement,³ which contains a forum selection clause selecting this judicial district for resolution of all disputes between the parties.

14. Venue is also proper because Defendant Netswift has consented to LinkedIn's terms for Pages (the "Pages Agreement"⁴), which apply to all members and organizations who maintain a Company Page on LinkedIn's website. The Pages Agreement also contains a forum selection clause selecting this judicial district for resolution of all disputes between the parties.

15. During all relevant times, Defendants have repeatedly, knowingly, and intentionally targeted their wrongful acts at LinkedIn, which is headquartered in this judicial district. In addition, Defendants have consented to personal jurisdiction in this judicial district by consenting to the forum selection clauses in the User Agreement and Pages Agreement.

INTRADISTRICT ASSIGNMENT

16. This case is an intellectual property action, to be assigned on a districtwide basis per Civil Local Rule 3-2(c).

THE PARTIES

17. LinkedIn Corporation is a Delaware corporation with its principal place of business in Sunnyvale, California.

18. Defendant ProAPIs Inc. is a Delaware corporation with its principal place of business in Middletown, Delaware.

19. Defendant Netswift (SMC-Private) Limited is a company incorporated under the laws of Pakistan in 2022. Netswift's principal place of business is in Pakistan.

20. Defendant Rehmat Alam is the cofounder and Chief Technology Officer of ProAPIs and Netswift. On information and belief, he is a national of Pakistan, where he resides. Alam registered his LinkedIn account on August 18, 2012. He is responsible in whole or in part for the wrongdoing alleged herein.

³ LinkedIn, *User Agreement* (Nov. 20, 2024), <https://www.linkedin.com/legal/user-agreement> (the "User Agreement").

⁴ LinkedIn, *LinkedIn Pages Terms*, <https://legal.linkedin.com/linkedin-pages-terms> (last visited Oct. 1, 2025) (the "Pages Agreement").

1 at all in public search engine results.⁵ Some information is not subject to these settings and can
 2 only be viewed by people who have logged into LinkedIn.

3 27. The privacy choices that LinkedIn offers its members are critical to their decisions
 4 to entrust information to LinkedIn and to LinkedIn's platform. In its Privacy Policy, LinkedIn sets
 5 limits regarding what LinkedIn can and cannot do with member data. The Privacy Policy also
 6 states that if a member decides that he or she wants to delete his or her profile, LinkedIn will
 7 permanently delete the account and all of the data that the member posted to LinkedIn within 30
 8 days. LinkedIn thus ensures that members have ultimate control over their information, by giving
 9 members the ability to customize how much information may be viewable and by whom, and the
 10 ability to remove their information entirely from LinkedIn's platform if they so decide.


11 28. LinkedIn has invested and plans to continue to invest substantial time, labor, skill,
 12 and financial resources into the development and maintenance of the LinkedIn site and platform.


13 **LinkedIn's Marks**


14 29. LinkedIn is the owner of several registered trademarks in graphic logos that it uses
 15 to advertise, market, and promote the LinkedIn brand.

16 30. LinkedIn is the owner of the following marks in International Class 9:

17 U.S. Registration No. 4,023,512 for LINKEDIN

18 U.S. Registration No. 3,971,642 for  19

20 U.S. Registration No. 4,023,511 for  21

22 U.S. Registration No. 4,023,513 for  23

24 (collectively, the "Class 9 Marks") in connection with "Computer software for the collection,
 25 editing, organizing, modifying, bookmarking, transmission, storage and sharing of data and
 26


27
 28 ⁵ See LinkedIn, *LinkedIn Public Profile Visibility*, <https://www.linkedin.com/help/linkedin/answer/a518980/> (last visited Oct. 1, 2025).


1 information in the fields of business and social networking, employment, careers and recruiting;
 2 downloadable electronic publications in the nature of newsletters, research reports, articles and
 3 white papers on topics of professional interest, all in the fields of business and social networking,
 4 recruiting and employment, and personal and career development; computer software
 5 development tools for business and social networking; computer software that provides web-based
 6 access to applications and services through a web-operating system or portal interface” in
 7 International Class 9.


8 31. LinkedIn has used the Class 9 Marks in interstate commerce in connection with the
 9 registered goods continuously since at least as early as April 30, 2007. Copies of the Certificates
 10 of Registration for the Class 9 Marks are attached as Exhibit A. The registrations for the Class 9
 11 Marks are valid, subsisting and incontestable pursuant to section 15 of the Lanham Act, 15 U.S.C.
 12 § 1065. LinkedIn’s use and registration of the Class 9 Marks predate Defendants’ unauthorized
 13 use of LinkedIn’s mark. Accordingly, LinkedIn has priority of rights in the Class 9 Marks.

14 32. LinkedIn is the owner of the following marks in International Class 35:

15 U.S. Registration No. 3,963,244 for LINKEDIN

16 U.S. Registration No. 3,959,413 for  **LinkedIn**

17
 18 U.S. Registration No. 3,959,419 for  **in**

19
 20 U.S. Registration No. 3,959,420 for  **in**


21
 22 (collectively, the “Class 35 Marks”) in connection with “Advertising and marketing services,
 23 namely, promoting goods and services for businesses; providing an online searchable database
 24 featuring employment and career opportunities and business, employment and professional queries
 25 and answers; job placement services, human resources consulting services; business research and
 26 survey services; promoting the goods and services of others via a global computer network;
 27 advertising, marketing and promotional services related to all industries for the purpose of
 28


1 facilitating networking and socializing opportunities for business purposes; charitable services,
 2 namely, promoting public awareness about community service; providing online career
 3 networking services and information in the fields of employment, recruitment, job resources, and
 4 job listings; personnel recruitment and placement services; electronic commerce services, namely,
 5 providing information about products and services via telecommunication networks for
 6 advertising and sales purposes; providing networking opportunities for individuals seeking
 7 employment; on-line professional networking opportunities; providing online computer databases
 8 and online searchable databases in the fields of business and professional networking” in
 9 International Class 35.


10 33. LinkedIn has used the Class 35 Marks in interstate commerce in connection with
 11 the registered services continuously since at least as early as July 31, 2008. Copies of the
 12 Certificates of Registration for the Class 35 Marks are attached as Exhibit B. The registrations for
 13 the Class 35 Marks are valid, subsisting and incontestable pursuant to section 15 of the Lanham
 14 Act, 15 U.S.C. § 1065. LinkedIn’s use and registration of the Class 35 Marks predates
 15 Defendants’ unauthorized use of LinkedIn’s mark. Accordingly, LinkedIn has priority of rights in
 16 the Class 35 Marks.

17 34. LinkedIn is the owner of the following marks in International Class 42:

18 U.S. Registration No. 3,967,561 for LINKEDIN

19 U.S. Registration No. 3,979,174 for 

20 U.S. Registration No. 3,971,641 for 

21 U.S. Registration No. 3,971,640 for 

22 (collectively, the “Class 42 Marks”) in connection with “Computer services, namely, hosting
 23 electronic facilities for others for organizing and conducting meetings, events and interactive
 24 discussions via the Internet; computer services, namely, creating an on-line community for
 25
 26
 27
 28

1 registered users to organize groups, events, participate in discussions, share information and
2 resources, and engage in social, business and community networking; providing temporary use of
3 on-line non-downloadable software for allowing web site users to communicate information of
4 general interest for purposes of social, business and community networking, marketing,
5 recruitment and employment; providing a website featuring temporary use of non-downloadable
6 software enabling users to search, locate and communicate with others via electronic
7 communications networks to network, conduct surveys, track online reference to job opportunities
8 and business topics; computer services in the nature of customized web pages featuring user-
9 defined information, personal profiles, and images; scientific and industrial research in the fields
10 of business and online social networking; providing a web site featuring temporary use of non-
11 downloadable software allowing web site users to post and display online videos and photos for
12 sharing with others for entertainment purposes; computer services, namely, creating an on-line
13 community for registered users to participate in discussions, get feedback from their peers, form
14 virtual communities, and engage in social networking featuring social media including photos,
15 audio and video content on general topics of social interest” (or a substantially similar description)
16 in International Class 42.

17 35. LinkedIn has used the Class 42 Marks in interstate commerce in connection with
18 the registered services continuously since at least as early as July 31, 2008. Copies of the
19 Certificates of Registration for the Class 42 Marks are attached as Exhibit C. The registrations for
20 the Class 42 Marks are valid, subsisting and incontestable pursuant to section 15 of the Lanham
21 Act, 15 U.S.C. § 1065. LinkedIn’s use and registration of the Class 42 Marks predates
22 Defendants’ unauthorized use of LinkedIn’s mark. Accordingly, LinkedIn has priority of rights in
23 the Class 42 Marks.

24 36. Collectively, the marks asserted in paragraphs 29 through 35 of this Complaint,
25 which are representative examples of LinkedIn’s trademark registrations, are referred to as the
26 “LinkedIn Marks.”

27 37. As a result of LinkedIn’s substantial expenditure of time, labor, skill, and financial
28 resources into its platform, the LinkedIn Marks and LinkedIn’s goods and services have developed

1 substantial goodwill.

2 38. The LinkedIn Marks have been distinctive and famous in the United States long
3 before Defendants engaged in the illicit activity described below.

4 **LinkedIn’s Prohibitions on Data Scraping, Fake Accounts,**
5 **and Other Harmful Conduct**

6 39. LinkedIn’s User Agreement (the “User Agreement”) prohibits scraping member
7 data from LinkedIn’s website through any means.⁶

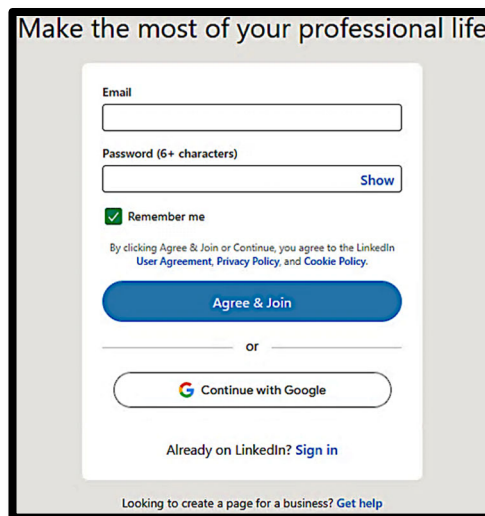
8 40. The User Agreement explains that members, users, and visitors to the LinkedIn
9 website must abide by certain restrictions in accessing and using the website. The current version
10 of the User Agreement, effective November 20, 2024, states that “By creating a LinkedIn account
11 or accessing or using our Services ..., you are agreeing to enter into a legally binding contract with
12 LinkedIn (even if you are using third party credentials or using our Services on behalf of a
13 company).”⁷ Each Defendant has either consented to this current version of the User Agreement
14 or has consented to a prior version of the User Agreement containing substantively identical
15 language.

16 41. Defendants Alam and Whitman bound themselves to the User Agreement when
17 they created their individual member profiles on LinkedIn. As demonstrated by the screenshot
18 below, a prospective member registers for an account by providing an email address and
19 password. By clicking “Agree & Join,” the prospective member “agree[s] to the LinkedIn User
20 Agreement, Privacy Policy, and Cookie Policy,” all of which are hyperlinked on the page.⁸

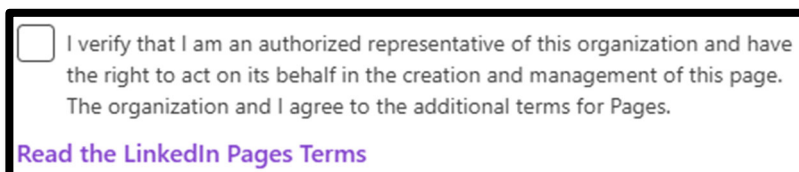
21
22
23
24
25
26
27 ⁶ See User Agreement § 8.2. Defendants also agreed to substantially similar terms at the time they
signed up for their LinkedIn accounts.

28 ⁷ *Id.* § 1.1.

⁸ LinkedIn, *Sign Up*, <https://www.linkedin.com/signup> (last visited Oct. 1, 2025).



42. Defendants ProAPIs and Netswift have also created, and have actively maintained, Company Pages on LinkedIn. An authorized representative of SerpsBot, now owned by Defendant ProAPIs, created a company page for SerpsBot on May 26, 2021.⁹ In so doing, the representative checked a box stating that “I verify that I am an authorized representative of this organization and have the right to act on its behalf in the creation and management of this page. The organization and I agree to the additional terms for Pages.”

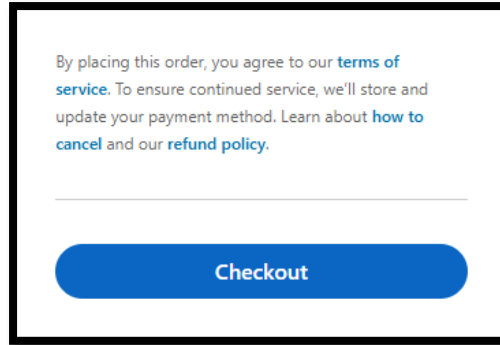


43. Defendant Alam created the Netswift company page on January 1, 2023. In so doing, he checked a box stating that “I verify that I am an authorized representative of this organization and have the right to act on its behalf in the creation and management of this page. The organization and I agree to the additional terms for Pages.”

44. Defendant Alam also agreed to the LinkedIn Subscription Agreement (“LSA”) when he signed up for a Sales Navigator plan, which he did first in May 2023, and again in January and March 2025. When purchasing a Sales Navigator license, prospective customers are

⁹ Only LinkedIn members who have agreed to the LinkedIn User Agreement can create Company Pages.

asked to agree to the Sales Navigator Terms of Service, which are prominently linked above the “checkout” button, as demonstrated in the screenshot below. Clicking on that link takes prospective customers to the LSA. The terms of the User Agreement are incorporated by reference in Section 2.1 of the LSA.



45. The Pages Agreement states that “the LinkedIn User Agreement, Privacy Policy and Cookie Policy apply to any use of our services,” and contains hyperlinks to the pertinent documents.¹⁰

46. Section 2.1 of the User Agreement prohibits users from “creating an account with false information.” The section states, in relevant part:

To use the Services, you agree that: (1) you must be the “Minimum Age”(described below) or older; (2) you will only have one LinkedIn account, which must be in your real name; and (3) you are not already restricted by LinkedIn from using the Services. **Creating an account with false information is a violation of our terms**, including accounts registered on behalf of others or persons under the age of 16.¹¹

47. Section 8.2 of the User Agreement prohibits those who are bound by the agreement from engaging in any of the following activities:

- “Creat[ing] a false identity on LinkedIn, misrepresent[ing] your identity, creat[ing] a Member profile for anyone other than yourself (a real person), or us[ing] or attempt[ing] to use another’s account (such as sharing log-in credentials or copying cookies)”;

¹⁰ Pages Agreement § 1.

¹¹ User Agreement § 2.1 (emphasis added).

- 1 • “Develop[ing], support[ing] or us[ing] software, devices, scripts, robots or any
- 2 other means or processes ... to scrape or copy the Services, including profiles and
- 3 other data from the Services”;
- 4 • Overrid[ing] any security feature or bypass[ing] or circumvent[ing] any access
- 5 controls or use limits of the Services (such as search results, profiles, or videos)
- 6 • “Copy[ing], us[ing], display[ing] or distribut[ing] any information (including
- 7 content) obtained from the Services ... without the consent of the content owner
- 8 (such as LinkedIn for content it owns)”;
- 9 • “Disclos[ing] information that you do not have the consent to disclose”;
- 10 • “Violat[ing] the intellectual property or other rights of LinkedIn”;
- 11 • “Rent[ing], leas[ing], loan[ing], trad[ing], sell[ing]/re-sell[ing] or otherwise
- 12 monetiz[ing] the Services or related data or access to the same, without LinkedIn’s
- 13 consent”;
- 14 • “Us[ing] bots or other unauthorized automated methods to access the Services, add
- 15 or download contacts, send or redirect messages, create, comment on, like, share, or
- 16 re-share posts, or otherwise drive inauthentic engagement”;
- 17 • “Interfer[ing] with the operation of, or plac[ing] an unreasonable load on, the
- 18 Services.”¹²

19 48. Section 8.2(17) of User Agreement also prohibits members from “viola[ting] the
 20 Professional Community Policies.” The Professional Community Policies provide, in relevant
 21 part:

22 **Do not create a fake profile or falsify information about yourself:** We don’t
 23 allow fake profiles or entities. Do not post misleading or deceptive information
 24 about yourself, your business ... [d]o not use or attempt to use another person’s
 25 LinkedIn account or create a member profile for anyone other than yourself.¹³

27 ¹² *Id.* § 8.2.

28 ¹³ LinkedIn, *LinkedIn Professional Community Policies*, <https://www.linkedin.com/legal/professional-community-policies> (last visited Oct. 1, 2025).

49. LinkedIn also maintains a branding policy (“Brand Guidelines”), which users agree to abide by in accepting the terms of the User Agreement.¹⁴ The branding policy instructs users not to use the LinkedIn “Brand, including our name, logos, or any elements that are identical to, incorporate, or closely resemble our Brand, in any way that could cause confusion about the source, sponsorship, or affiliation of your product, service, or account.” The branding policy further states that “LinkedIn does not allow anyone to use the LinkedIn Logo, unless they already have an existing relationship with LinkedIn and a Brand or Trademark License.”¹⁵

50. For years, Defendants have been on notice of and agreed to abide by these and other prohibitions in registering for and using LinkedIn’s services. As demonstrated below, Defendants have engaged in a systematic pattern of conduct that violates and breaches LinkedIn’s terms, including the User Agreement, evidencing their lack of intent to comply with them, and causing harm to LinkedIn.

LinkedIn’s Technical Defenses

51. LinkedIn works hard to protect the integrity and security of its platform. Among other precautions, LinkedIn employs an array of technological safeguards and barriers designed to detect and restrict fake accounts and to prevent data scrapers, bots, and other automated systems from accessing and copying its members’ data. Specifically, LinkedIn has dedicated teams of engineers whose full-time job is to detect and restrict fake accounts, detect and prevent scraping, and to maintain LinkedIn’s technical defenses. It employs many different technical defenses that are constantly operating, including rate limiters, IP address blocks, artificial intelligence models, and proprietary algorithms to detect and block scraping.

52. LinkedIn’s technical measures are important to ensuring that the website is available to and used by legitimate users, and that members feel safe sharing personal information on LinkedIn’s platform. To that end, LinkedIn has used, and will continue to use, commercially reasonable techniques for safeguarding the security of members’ data. In marketing their

¹⁴ LinkedIn, *LinkedIn Brand Guidelines*, <https://brand.linkedin.com/en-us> (last visited Oct. 1, 2025).

¹⁵ LinkedIn, *LinkedIn Logo*, <https://brand.linkedin.com/linkedin-logo> (last visited Oct. 1, 2025).

1 products, Defendants acknowledge that LinkedIn’s technical defenses make it “one of the hardest
2 websites to scrape.”¹⁶

3 **Defendants’ Products Rely on Data Scraped from LinkedIn and Use a Network of Fake**
4 **Accounts to Conduct Logged-In Scraping**

5 53. Defendants offer to their clients the iScraper API—an API that allows users to
6 “scrape LinkedIn data efficiently in real-time and at scale.”¹⁷ It scrapes information that is
7 viewable without logging in, as well as information that cannot be accessed without logging in.
8 Defendants’ logged-in scraping scheme works as follows, on information and belief. Using
9 automated tools, they create and/or take over thousands of email addresses. Defendants then use
10 those email addresses to create accounts on LinkedIn, likely in an automated way, evading
11 LinkedIn’s technical defenses for at least a brief period. These accounts are registered under false
12 names and use stock images as profile photos. Upon information and belief, Defendants have
13 used over a million of these fake accounts as part of their scheme. Defendants continue to create
14 these fake accounts.

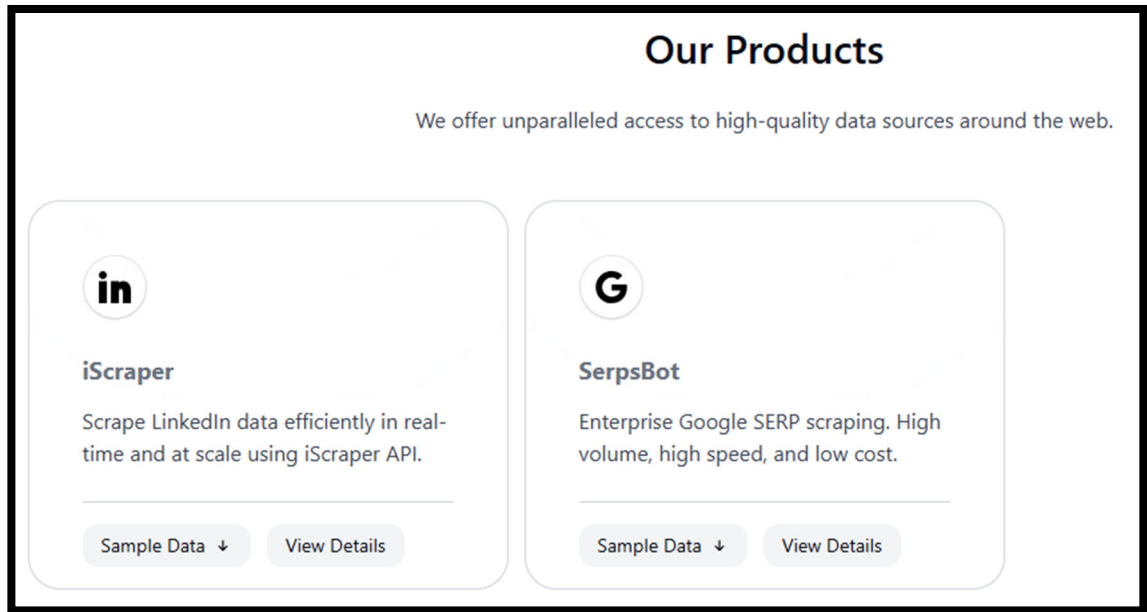
15 54. These fake accounts generally are detected by LinkedIn’s technical defenses and
16 restricted within a few hours. But in that brief period, they are sometimes able to scrape hundreds
17 of LinkedIn profiles each, if not more. Undeterred, Defendants continue their scheme day after
18 day, setting up new accounts as fast as LinkedIn can restrict those that it detects. These fake
19 accounts—registered under false names—appear to exist for the sole reason of scraping member
20 data about real people so that Defendants can sell that data to their customers. It does not appear
21 that Defendants’ fake accounts appeal for reinstatement after LinkedIn restricts them,
22

23 ¹⁶ Rehmat Alam, *Scraping LinkedIn Public Data Without Getting Blocked*, SupportiveHands
24 (Sept. 22, 2021), <https://www.supportivehands.net/how-to-scrape-linkedin-public-data-without-getting-blocked/> (last visited Oct. 1, 2025).

25 ¹⁷ ProAPIs, *Enterprise-Grade APIs for Data-Centric Projects*, <https://proapis.com/> (when visited
26 on August 18, 2025). This text appears to have been removed on or around September 30, 2025.
27 See <https://web.archive.org/web/20250930193200/https://proapis.com/>. The developer
28 documentation for iScraper still exists on the ProAPIs website, and that documentation continues
to advertise that iScraper “delivers comprehensive, up-to-the-second profile information.” See
ProAPIs, iScraper API v4.0, <https://docs.proapis.com/iscraper-docs#tag/profiles-details> (last
visited Oct. 1, 2025).

underscoring that they do not belong to real people.

55. Defendants openly admit to scraping LinkedIn members' data. ProAPIs prominently displayed the iScraper API on its website, describing it to prospective customers as a tool to "scrape LinkedIn data efficiently in real-time and at scale":

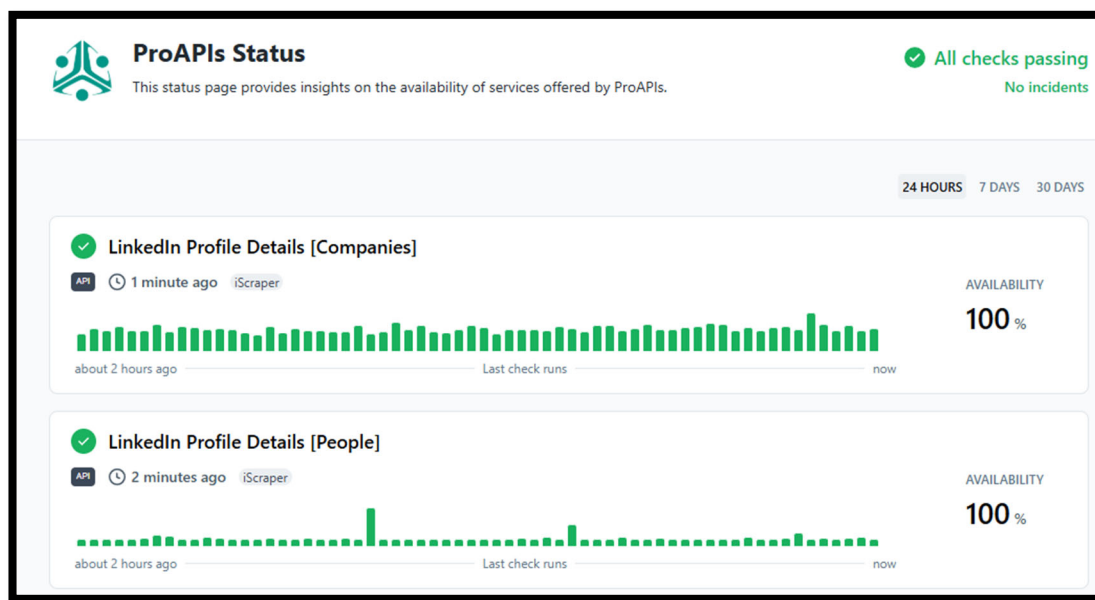


Other marketing material that ProAPIs published promoted the ability of the iScraper API to conduct "[r]eal-time data extraction" of LinkedIn data at a rate of up to "150 requests / second."¹⁸ And Defendants' pricing—which can cost \$15,000 per month for 5,000,000 API calls at 150 requests *per second*—underscores that they are offering industrial-scale scraping abilities.

¹⁸ ProAPIs, *Enterprise-Grade APIs for Data-Centric Projects*, <https://proapis.com/pricing/> (when visited on Aug. 18, 2025). The pricing for and description of iScraper, and the screenshots on this page and the next, appeared on the ProAPIs Pricing page as of August 18, 2025.

\$15000/mo	\$4000/mo	\$2500/mo
iScraper Scale	iScraper Business	iScraper Professional
Scrape LinkedIn data efficiently in real-time and at scale using iScraper API.	Scrape LinkedIn data efficiently in real-time and at scale using iScraper API.	Scrape LinkedIn data efficiently in real-time and at scale using iScraper API.
<ul style="list-style-type: none"> ✓ 5M requests included ✓ \$0.003 per additional API call ✓ 150 requests / second ✓ Real-time data Extraction 	<ul style="list-style-type: none"> ✓ 1M requests included ✓ \$0.004 per additional API call ✓ 100 requests / second ✓ Real-time data Extraction 	<ul style="list-style-type: none"> ✓ 500K requests included ✓ \$0.005 per additional API call ✓ 75 requests / second ✓ Real-time data Extraction
Start now	Start now	Start now

56. Additionally, ProAPIs dedicated a page on its website to updating clients on the status of its iScraper tool, assuring them of its ability to extract details from LinkedIn Company and People Profiles:



57. ProAPIs' website also provides documentation for its application, which includes samples of computer code that ProAPIs' paying customers may use to collect full profile data for LinkedIn members via ProAPIs' service together with samples of the formatted data paying

1 customers can obtain.¹⁹

2 58. In promotional material published by Defendant Alam, he states that “you can
3 scrape both personal and company profiles from LinkedIn using our API service. Now when we
4 talk about the fields that the data contains, then it includes the name, education history, position
5 groups, languages, location, certifications, volunteer experience, patents and all other data that’s
6 public on personal profiles.”²⁰ Alam further instructs individuals to visit the ProAPIs website “and
7 try our service to fulfil your LinkedIn data mining needs.”²¹

8 59. Defendants are scraping while logged in. Defendants not only use logged-in fake
9 accounts to scrape, but they also scrape the profiles of members who have configured their profile
10 settings to restrict the visibility of their entire profile to logged-in members only. This scraping
11 would not be possible without first logging in. This renders Defendants’ statements that they only
12 scrape “data that’s public on personal profiles” false.²²

13 60. To respond to the extensive number of fake accounts created by Defendants,
14 LinkedIn has had to expend substantial human, financial, and technical resources, including
15 hundreds of hours of employee time. LinkedIn’s technical measures quickly detect the majority
16 fake accounts like those Defendants create, but some of these accounts manage to conduct some
17 scraping activity before being disabled. As a result, at scale, Defendants manage to scrape a
18 considerable amount of data.

19 61. Data scraping activity conducted by Defendants consumes LinkedIn’s server
20 capacity in amounts that are abnormal and disproportionate to the capacity used by real human
21 members. Defendants’ scheme results in their fake accounts, in aggregate, making millions of
22 requests more than an individual member would. In addition, because scrapers make requests
23

24 ¹⁹ ProAPIs, *iScraper API v4.0*, <https://docs.proapis.com/iscraper-docs#tag/profiles-details> (last
25 visited Oct. 1, 2025); PROAPIs, *iScraper API v4.0*, [https://docs.proapis.com/iscraper-](https://docs.proapis.com/iscraper-docs#tag/linkedin-search)
[docs#tag/linkedin-search](https://docs.proapis.com/iscraper-docs#tag/linkedin-search) (last visited Oct. 1, 2025).

26 ²⁰ Rehmat Alam, *Scraping LinkedIn Public Data Without Getting Blocked*, SupportiveHands
27 (Sept. 22, 2021), [https://www.supportivehands.net/how-to-scrape-linkedin-public-data-without-](https://www.supportivehands.net/how-to-scrape-linkedin-public-data-without-getting-blocked/)
[getting-blocked/](https://www.supportivehands.net/how-to-scrape-linkedin-public-data-without-getting-blocked/) (last visited Oct. 1, 2025).

28 ²¹ *Id.*

²² *Id.*

1 along certain pathways, in aggregate they task that infrastructure substantially more than even a
2 very active human user. For example, scrapers like Defendants are responsible for the majority of
3 traffic making requests to certain LinkedIn servers that serve member profiles. Although
4 LinkedIn's technical defenses block the majority of such requests, this overconsumption, as well
5 as intentional interference by scrapers with platform operations, places undue strain on LinkedIn's
6 infrastructure, impairing service availability and the ability of LinkedIn's technical defenses to run
7 as intended. This has forced LinkedIn to over-invest in server capacity to mitigate the threat posed
8 by scrapers like Defendants, which otherwise could cause larger failures of LinkedIn's systems.
9 To maintain normal performance and limit service degradation for legitimate users, LinkedIn must
10 continue to allocate additional capacity, resources, and security measures to account for and
11 mitigate interference caused by this unauthorized usage over time.

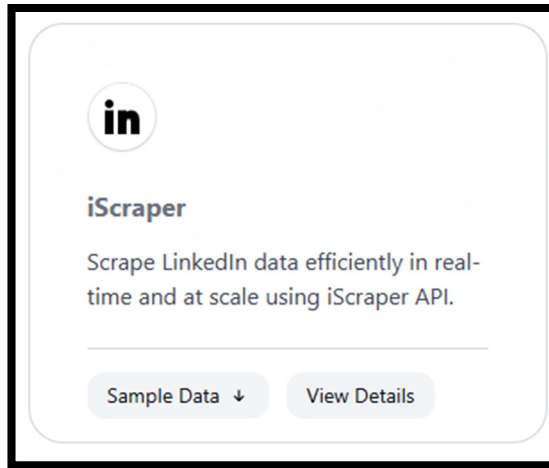
12 62. Defendants then sell the data that they scrape. ProAPIs sells over two dozen fields
13 of LinkedIn member data, including members' names, locations, industries, work experience,
14 education, languages, awards, membership, certifications, posts, reactions, and comments, as well
15 as company and school data. In their efforts to exploit LinkedIn member data for profit,
16 Defendants have scraped millions of members' profiles.

17 63. Defendants' conduct violates the User Agreement and the law. It violates the User
18 Agreement's prohibitions on "scrap[ing] or copy[ing] the Services, including profiles and other
19 data from the Services," among other provisions. Their fake account mill violates the prohibition
20 on "Creat[ing] a false identity on LinkedIn, misrepresent[ing] your identity, or creat[ing] a
21 Member profile for anyone other than yourself (a real person)." Defendants were on notice of
22 these conditions, agreed to them, and knowingly violated them in engaging in their prohibited
23 conduct. Defendants have also circumvented the many technical measures and barriers LinkedIn
24 has in place to prevent such scraping activities, in violation of several state and federal laws
25 prohibiting unauthorized access, as detailed in the causes of action pled below.

26 **Defendants Use LinkedIn's Trademarks To Market Their Scraping Services**

27 64. Defendants have prominently featured the LinkedIn Marks in marketing materials
28 for their scraping services, without LinkedIn's consent and in disregard of LinkedIn's trademark

rights. The following advertisement, once featured on the front page of ProAPIs website, contained LinkedIn's "IN" logo mark:



65. LinkedIn has had no part in the design, marketing, offering for sale, or sale of the data scraping application created by Defendants. Nor is LinkedIn associated, affiliated, or otherwise connected with ProAPIs in any way.

66. Defendants did not have permission or authorization from LinkedIn to use the LinkedIn Marks. Defendants were aware at all relevant times that they did not have permission or authorization, and their use of the LinkedIn Marks was willful.

67. Defendants' use of the LinkedIn Marks causes and is likely to cause an unwanted association between LinkedIn's products and Defendants' illicit scraping activities, tarnishing the LinkedIn Marks. Privacy and member control of personal data are central to LinkedIn's creation of an environment where members feel comfortable sharing their professional identities and engaging with their networks online. In furtherance of that interest, LinkedIn offers members choices about the data that LinkedIn collects, uses, and shares, and maintains a detailed Privacy Policy. Defendants' use of the LinkedIn Marks undermines LinkedIn's reputation for privacy, as well as the substantial goodwill that LinkedIn has accrued, by associating LinkedIn's products with services that scrape data without members' consent and sell it to whomever is willing to pay for it.

68. Defendants' use of the LinkedIn Marks in their marketing materials violates the Lanham Act's prohibitions on trademark dilution. Defendants' conduct also breaches the User

1 Agreement's condition prohibiting users from "[v]iolating the intellectual property or other rights
2 of LinkedIn." Defendants were on notice of both this condition and LinkedIn's branding policy
3 when they agreed to the User Agreement.

4 69. By engaging in the activities described above, Defendants have caused—and, if not
5 halted, will continue to cause—ongoing and irreparable harm to LinkedIn, in a variety of ways,
6 including ongoing and irreparable harm to its consumer goodwill.

7 70. LinkedIn's members entrust to LinkedIn their data, including professional histories,
8 skills and interests on LinkedIn's site, as well as their comments and reactions. LinkedIn will
9 suffer ongoing and irreparable harm to its consumer goodwill and trust, which LinkedIn has
10 worked hard for years to earn and maintain, if Defendants' conduct continues.

11 71. LinkedIn expended significant human, financial, and technical resources, including
12 hundreds of hours of employee time, investigating and responding to Defendants' unlawful
13 activities, including in its efforts to detect the fake accounts that Defendants have created in
14 furtherance of their fraud. Despite these efforts, LinkedIn has not been able to successfully and
15 permanently stop Defendants from continuing their illicit scheme, and thus needs relief from this
16 Court to enjoin Defendants.

17 **Defendants Engage in Fraud to Obtain LinkedIn Products**

18 72. Defendant Alam engaged in fraud on multiple occasions by subscribing to paid
19 LinkedIn products and obtaining their benefits without paying for them, and with no apparent
20 intention to pay for them.

21 73. In February 2023, Alam subscribed to an annual LinkedIn Premium plan, which
22 requires payment of a periodic fee after a free first month. When LinkedIn went to charge the
23 credit card number that Alam supplied, payment was declined. Alam canceled the plan in April
24 2023 without ever paying for the services.

25 74. In January 2025, Alam subscribed to LinkedIn Sales Navigator, another LinkedIn
26 product that requires payment of a periodic fee after a free first month. When LinkedIn went to
27 charge the credit card number that Alam supplied, payment was declined. Alam canceled the plan
28 on March 5, 2025, without ever paying for the services, only to re-subscribe on March 5, 2025,

1 using a different credit card. LinkedIn immediately attempted to charge that new credit card, and
2 attempted repeatedly for approximately two weeks, but the transactions never went through.

3 **FIRST CLAIM FOR RELIEF**

4 **Against all Defendants for Breach of Contract**

5 75. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

6 76. Use of the LinkedIn website and use of LinkedIn services are governed by and
7 subject to the User Agreement.

8 77. LinkedIn members are presented with the User Agreement and must affirmatively
9 accept and agree to the User Agreement to register for a LinkedIn account.

10 78. At all relevant times, LinkedIn also prominently displayed a link to the User
11 Agreement on LinkedIn's homepage.

12 79. Defendants were on notice of and agreed to the User Agreement when Alam
13 created his member profile on LinkedIn and extensively used the LinkedIn website, including
14 through the creation and maintenance of (i) the SerpsBot and Netswift Company Pages, and (ii)
15 their extensive network of fake accounts.

16 80. The User Agreement is incorporated into or incorporates other agreements, such as
17 the Pages Agreement and Brand Guidelines, respectively, to which Defendants agreed.

18 81. The User Agreement is enforceable and binding on Defendants.

19 82. Defendants repeatedly accessed the LinkedIn website with knowledge of the User
20 Agreement and all of its prohibitions. Despite their knowledge of the User Agreement and its
21 prohibitions, Defendants accessed and continue to access the LinkedIn website to, among other
22 things, scrape the LinkedIn website in violation of the User Agreement and without the consent of
23 LinkedIn or its members.

24 83. Defendants' actions, as described above, have willfully, repeatedly, and
25 systematically breached the User Agreement.

26 84. LinkedIn has performed all conditions, covenants, and promises required of it in
27 accordance with the User Agreement.

28 85. Defendants' conduct has damaged LinkedIn, and caused and continues to cause

1 irreparable and incalculable harm and injury to LinkedIn.

2 86. LinkedIn is entitled to injunctive relief, compensatory damages, and/or other
3 equitable relief.

4 **SECOND CLAIM FOR RELIEF**

5 **Against all Defendants for Fraud and Deceit (Common Law, Cal. Civ. Code §§ 1572, 1710)**

6 87. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

7 88. Defendants' acts, as alleged, constitute fraud on LinkedIn. By creating fake
8 accounts, Defendants misrepresented their identities, accepted LinkedIn's User Agreement
9 without any intent to comply, and deceived LinkedIn into activating their fake accounts and
10 granting them access to the platform. They then use these fraudulently obtained accounts to
11 access and scrape member data that they otherwise would not have been able to access.

12 89. Defendants are aware that their representations are false. They know that they are
13 posing as others or as people who are not real, and they know that LinkedIn has relied on these
14 false representations to extend access to its platform to Defendants.

15 90. Defendants specifically intended that LinkedIn would rely on their false
16 representations, granting Defendants' access to its platform and LinkedIn's engagement services.

17 91. In addition, LinkedIn relies on members to accurately portray themselves on
18 LinkedIn's platform in order to maintain an environment where members feel safe sharing
19 personal and career information. Reliance on accurate representations by its members is critical to
20 the trust and goodwill that LinkedIn has worked hard to create. LinkedIn's reliance is justifiable.

21 92. As detailed above, Defendants' behavior has damaged and threatens ongoing injury
22 to LinkedIn if not enjoined. LinkedIn's reliance on Defendants' false representations is a
23 substantial factor in causing LinkedIn's harm.

24 93. Moreover, Defendant Alam submitted false financial information to LinkedIn in
25 order to gain access to LinkedIn products that he otherwise would have to purchase. Alam knows
26 that the credit card information he provided to gain access to LinkedIn Premium and Sales
27 Navigator is not capable of payment, and that payment will not be processed when LinkedIn
28 attempts to charge the credit card information he submits. Alam specifically intended that

1 LinkedIn would rely on this false financial information in order to obtain access to LinkedIn
 2 products, but had no intention of actually paying for those products. LinkedIn relied on the credit
 3 card information that Alam provided being valid and, based on that reliance, provided him access
 4 to LinkedIn products that he otherwise would not have had, absent his fraud.

5 **THIRD CLAIM FOR RELIEF**

6 **Against all Defendants for Breach of the Computer Fraud and Abuse Act (18 U.S.C. § 1030)**

7 94. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

8 95. LinkedIn brings this action under 18 U.S.C. § 1030 (the “CFAA”) allowing any
 9 injured person to maintain a civil action against the violator of 18 U.S.C. § 1030(g).

10 96. Defendants have violated the CFAA by knowingly accessing a protected computer,
 11 without authorization in violation of § 1030(a)(2)(C). Defendants have also violated § 1030(a)(4)
 12 by knowingly and with the intent to defraud accessing a protected computer without authorization,
 13 and by means of such conduct obtaining one or more things of value (namely, data stored on
 14 LinkedIn).

15 97. LinkedIn members have provided data to LinkedIn. That data was then stored on
 16 LinkedIn’s servers, which are protected computers under 18 U.S.C. § 1030(e)(2)(B) as they are
 17 used in or affect interstate commerce. The data was accessible to only those who made accounts
 18 with LinkedIn in accordance with the User Agreement.

19 98. Defendants were never validly given authorization to access the data provided to
 20 LinkedIn that is behind LinkedIn’s password wall. Instead, Defendants obtained authorization
 21 fraudulently, through the creation of an extensive network of fake accounts that then scrape behind
 22 LinkedIn’s password wall. These accounts are created through misrepresentations. Defendants
 23 then accessed that data without authorization, knowing the data was accessible only according to
 24 the User Agreement, and that Defendants did not have valid authorization to access it. Defendants
 25 used the personal data they obtained in furtherance of their unlawful scraping operations, and have
 26 continued to make such data available to third-parties for purchase.

27 99. LinkedIn has suffered losses as a result of these violations amounting to well over
 28 \$5,000 aggregated over a one-year period, including, without limitation:

1 computer networks in violation of California Penal Code § 502(c)(2).

2 105. Defendants knowingly and without permission used or caused to be used
3 LinkedIn's computer services in violation of California Penal Code § 502(c)(3).

4 106. Defendants knowingly and without permission accessed or caused to be accessed
5 LinkedIn's computers, computer systems, and/or computer networks in violation of California
6 Penal Code § 502(c)(7).

7 107. Defendants willfully violated the CDAFA in disregard and derogation of
8 LinkedIn's rights.

9 108. All of Defendants' unlawful conduct in violation of the CDAFA continues to this
10 day.

11 109. LinkedIn has suffered losses as a result of these violations, including, without
12 limitation:

13 a. amounts expended attempting to conduct internal technical investigations in
14 efforts to ascertain the nature and scope of Defendants' unauthorized access to the data; and

15 b. significant employee resources and time to participate and assist in those
16 investigations; and

17 c. substantial human, financial, and technical resources to disable Defendants'
18 network of fake accounts and attempt to prevent Defendants' further access to LinkedIn's website;
19 and

20 d. attorneys' fees in aid of those investigations and in enforcing the relevant
21 User Agreements.

22 110. Pursuant to California Penal Code § 502(e), LinkedIn is entitled to recover its
23 losses and obtain injunctive relief prohibiting Defendants from further violations of the CDAFA
24 and to prohibit Defendants from using the data they obtained by accessing the data without
25 authorization.

FIFTH CLAIM FOR RELIEF

Against all Defendants for Unlawful, Unfair or Fraudulent Business Practices

(Cal. Bus. & Prof. Code § 17200 *et seq.*)

111. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

112. Defendants' actions described above constitute unlawful, unfair, or fraudulent acts or practices in the conduct of a business, in violation of California's Business and Professions Code § 17200 *et seq.*, including because Defendants deceived LinkedIn into providing it access to, and information from, the personal data of LinkedIn members.

113. Defendants' data collection technology and its data scraping tools deliberately misrepresented requests sent to the LinkedIn website. Specifically, Defendants created accounts using email addresses they created and/or took over and fake names in order to pose as legitimate LinkedIn users to send queries to LinkedIn's servers. Defendants did this in order to evade LinkedIn's technical defenses, which are designed to prevent unauthorized access of its computer servers. Defendants conducted these harmful scraping activities while logged in through an extensive network of fake accounts they have registered and maintained.

114. This fraudulent scheme has allowed Defendants to conduct their illicit scraping and further their scheme in a way that they otherwise would not have been able to accomplish had they accessed LinkedIn using non-fraudulent means. Defendants are on notice that their scheme is fraudulent as when their fake accounts are restricted, they cease using them (as they are unable to do so) and not a single one of their fake accounts has applied for reinstatement. Defendants simply create more accounts.

115. Scraping data, creating fake accounts, and circumventing LinkedIn's ability to police its own platform has caused substantial injury to LinkedIn, in the form of costs to investigate, remediate, and prevent Defendants' wrongful conduct. This misconduct also undermines the confidence that LinkedIn members place in the company to protect their information, tarnishing LinkedIn's brand and reputation.

116. As a result of Defendants' various acts and omissions, LinkedIn has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will

1 continue unless Defendants' actions are enjoined.

2 **SIXTH CLAIM FOR RELIEF**

3 **Against all Defendants for Dilution by Tarnishment (15 U.S.C. § 1125(c))**

4 117. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

5 118. The LinkedIn Marks are famous and distinctive. The Marks were famous and
6 distinctive before Defendants began to use them in commerce.

7 119. Defendants' commercial use of the LinkedIn Marks in their marketing materials is
8 likely to cause an unwarranted association between Defendants' illicit activities and the LinkedIn
9 Marks that creates negative associations with LinkedIn and tarnishes the LinkedIn Marks. As
10 noted above, LinkedIn's transparent information about how members' data is collected and used,
11 as well as members' choices regarding their data, is central to LinkedIn's business. Defendants'
12 products, developed through violation of Defendants' contractual obligations, threaten members'
13 privacy and autonomy, and interfere with members' reasonable expectations that LinkedIn will
14 continue to protect their data privacy choices. Defendants distribute code their customers may use
15 to obtain full profile data for LinkedIn members—including information that members have
16 chosen to make available for viewing only by other legitimate, logged-in members—undermining
17 LinkedIn's Privacy Policy and members' choices and user settings, which give members ultimate
18 control over their information, and Defendants promote such code with the unauthorized use of the
19 LinkedIn Marks. This association of privacy violations with the LinkedIn Marks harms
20 LinkedIn's reputation and tarnishes its marks.

21 120. Defendants' conduct has caused and will continue to cause immediate and
22 irreparable injury to LinkedIn, including its business, reputation, and goodwill.

23 121. LinkedIn is entitled to injunctive relief pursuant to 15 U.S.C. § 1125(c)(5).

24 122. Because Defendants willfully intended to trade on LinkedIn's reputation and
25 goodwill, LinkedIn is entitled to damages, enhanced damages, fees, and costs pursuant to 15
26 U.S.C. § 1117(a).

SEVENTH CLAIM FOR RELIEF

Against all Defendants for Misappropriation

123. LinkedIn realleges and incorporates by reference all of the preceding paragraphs.

124. LinkedIn has invested substantial time, labor, skill, and financial resources into the creation and maintenance of LinkedIn, its computer systems and servers, including system and server capacity, as well as the content on the LinkedIn website, which is time sensitive. Defendants have invested none of their own time and resources into developing and building the LinkedIn website and platform.

125. Disregarding the prohibitions set forth in the User Agreement of which they have been on notice and to which they have expressly consented, and in circumvention of various technical barriers, Defendants, without authorization, have wrongfully accessed LinkedIn's website, computer systems and servers, and obtained data from the LinkedIn site. The data that Defendants took included time-sensitive updates to member profiles.

126. Defendants' appropriation and use of this data was at little or no cost to Defendants, without them having to make the substantial investment in time, labor, skill, and financial resources made by LinkedIn in developing the LinkedIn website and platform. In other words, Defendants have reaped what they have not sown. Defendants' use of LinkedIn's computer systems and servers, including member data from the LinkedIn site and system and server capacity, constitutes free-riding on LinkedIn's substantial investment of time, effort, and expense.

127. As a result of this misappropriation, LinkedIn has been forced to expend additional time and resources, including but not limited to, investigating and responding to Defendants' activities.

128. LinkedIn has been and will continue to be damaged as the result of Defendants' acts of misappropriation.

129. LinkedIn has suffered and will continue to suffer irreparable injury, and its remedy at law is not itself adequate to compensate it for injuries inflicted by Defendants.

EIGHTH CLAIM FOR RELIEF

Against all Defendants for Trespass to Chattels

123. LinkedIn realleges and incorporates all preceding paragraphs herein.

124. The LinkedIn platform and all underlying technological infrastructure are the personal property of LinkedIn.

125. Defendants intentionally entered into, and made use of, LinkedIn's technological infrastructure, including its software and servers, to obtain information for their own economic benefit.

126. Using a network of fake accounts, Defendants knowingly exceeded any permission granted by LinkedIn to access its personal property, including its technological infrastructure and servers.

127. Data scraping activity conducted by Defendants consumes LinkedIn's server capacity in amounts that are abnormal and disproportionate to the capacity used by real human members, resulting in their fake accounts making millions of requests more than an individual member would.

128. Defendants' acts place an exceedingly burdensome load on LinkedIn's servers, diminishing the ability of LinkedIn's technical defenses to run as intended, and diminishing the server capacity that LinkedIn can devote to its legitimate users. It has required LinkedIn to invest in additional server capacity to mitigate the threat posed by Defendants and other scrapers, which otherwise could cause larger failures of LinkedIn's systems. These acts thereby injure LinkedIn by depriving it of the ability to use its personal property and requiring it to invest substantial resources to avoid the complete degradation of its servers.

129. LinkedIn has never consented to Defendants' conduct.

130. Defendants' conduct constitutes trespass to LinkedIn's chattels.

131. Defendants' acts have caused injury to LinkedIn and, if continued or expanded, will continue to cause damage in the form of impaired condition, quality, and value of its technical defenses, and requiring LinkedIn to invest in additional server capacity beyond that which it otherwise would without Defendants' scraping.

PRAYER FOR RELIEF

WHEREFORE, LinkedIn prays that judgment be entered in its favor and against Defendants, as follows:

132. A permanent injunction enjoining and restraining all Defendants, their employees, representatives, agents, and all persons or entities acting in concert with them during the pendency of this action and thereafter perpetually from

a. accessing or using LinkedIn's website, servers, systems, and any data displayed or stored therein, including through scraping and crawling technologies or through creating fake accounts, for any purpose whatsoever; and

b. extracting and copying data appearing on LinkedIn's website to their own servers or systems or those controlled by them; and

c. using the LinkedIn Marks in commerce.

133. An order requiring Defendants to destroy all documents, data, and other items, electronic or otherwise, in their possession, custody, or control, that were wrongfully extracted and copied from LinkedIn's website, along with any data that Defendants have inferred, aggregated, or synthesized as a result of data wrongfully extracted and copied from LinkedIn's website;

134. An order requiring Defendants to destroy all software code and other instrumentalities for scraping LinkedIn's platform;

135. An order requiring Defendants to notify all customers that purchased or otherwise acquired access to scraped data from LinkedIn of any decision or award against Defendants;

136. An award to LinkedIn of damages, including, but not limited to, compensatory, statutory, enhanced damages, profits of Defendants, and/or punitive damages, as permitted by law;

137. An award to LinkedIn of its costs of suit, including, but not limited to, reasonable attorney's fees, as permitted by law; and

138. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

LinkedIn hereby demands a jury trial of all issues in the above-captioned action that are

1 triable to a jury.

2 DATED: October 2, 2025

MUNGER, TOLLES & OLSON LLP

3
4 By: /s/ Nicholas D. Fram
5 NICHOLAS D. FRAM
6 Attorney for LinkedIn Corporation
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28